KONA2 D2320N ePassport EAC with PACE Security Target Lite

V01.00 (2018.11.07)

R&D Center

Revision History

KONA2 D2320N ePassport EAC with PACE Security Target Lite

No.	Ver.	Date	Description of Change	Chapter	Writer
1	V01.00	2018/11/07	New Publication	All	KONA I

2018. Nov 07, 1st Release

Table of Contents

1. ST Introduction

1.1. ST Reference

Document No:	SP-08-23
Document Title:	KONA2 D2320N ePassport EAC with PACE Security Target Lite
Version:	1
Revision:	00
Release date:	2018-11-07

Table 1. ST Reference

1.2. TOE Reference

Name:	KONA2 D2320N ePassport [EAC with PACE configuration]
Version:	02
Revision:	10
Update (patch)	00

Table 2. TOE Reference

1.3. TOE Overview

The Target of Evaluation (TOE) is a contactless smart card programmed according to ICAO Technical Report “Supplemental Access Control” [ICAO SAC] (which means amongst others according to the Logical Data Structure (LDS) defined in ‘ICAO Doc 9303’) and additionally providing the Extended Access Control according to the ‘ICAO Doc 9303’ [ICAO 9303] and BSI TR-03110-1 [TR-03110-1], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE [PACE-PP].

The TOE is composed of:

- the circuitry of the MRTD’s chip (16-Bit RISC Microcontroller for Smart Cards, S3FT9MG rev 0)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system KONA2 D2320N ePassport V02.10.00),
- the associated guidance documentation.

It provides the security level of EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

The TOE type of the current security target is "the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) and providing Extended Access Control with PACE", compatible with the expected TOE type described in [PACE-PP] and [EAC-PP].

2. TOE Description

The Target of Evaluation (TOE) is a contactless smart card programmed according to ICAO Technical Report "Supplemental Access Control" [ICAO SAC] (which means amongst others according to the Logical Data Structure (LDS) defined in 'ICAO Doc 9303') and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [ICAO 9303] and BSI TR-03110-1 [TR-03110-1], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE [PACE-PP].

The TOE is composed of:

- the circuitry of the MRTD's chip (16-Bit RISC Microcontroller for Smart Cards, S3FT9MG rev 0)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system KONA2 D2320N ePassport V02.10.00),
- the associated guidance documentation.

TOE usage and security features for operational use:

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 protection profile 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 personalised 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 Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation.

For this security target the MRTD is viewed as unit of:

1) 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 passport book,
    b. the printed data in the Machine-Readable Zone (MRZ) and
    c. the printed portrait.
2) 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 contactless integrated circuit. It presents 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 optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
    d. the other data according to LDS (EF.DG5 to EF.DG16) and

e. the Document security object(SOD).

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 Organization and the security features of the travel document's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303, and Password Authenticated Connection Establishment (PACE). The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

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

If BAC is supported by the TOE, the travel document has to be evaluated and certified separately. This is due to the fact that BAC-PP does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

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 SAC, the following steps shall be performed:

1) 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.
2) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
3) 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.
4) Each party generates an authentication token, sends it to the other party and verifies the received token.

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

The security target requires the TOE to implement the Extended Access Control as defined in BSI 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.1 has been successfully executed. The Terminal Authentication Protocol v.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 issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

TOE life cycle:
According to [PACE-PP] and [EAC-PP], the TOE life cycle is described in terms of the four life cycle phases, which are additionally subdivided into 7 steps.

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.

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile programmable memories (FLASH) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase 2 "Manufacturing"

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and the parts of the travel document's chip Embedded Software in the non-volatile non-programmable memories (FLASH). 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 manufacture 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 FLASH).

(Step4) The travel document manufacturer combines the IC with hardware for the contactless interface in the travel document unless the travel document consists of the card only

The MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The software developer of the step 2 also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 "Personalization of the MRTD"

(Step5) the Personalization Agent equips MRTD's chips with pre-personalization Data.

(Step6) The personalization of the MRTD 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 Personalization 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] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Phase 4 "Operational Use"

(Step7) The TOE is used as MRTD 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 Organization and can be used according to the security policy of the issuing State but they can never be modified.

(See the EAC-PP for applicable application notes: 1, 2, 3 and 4)

A matching table between the card lifecycle states and the TOE lifecycle phases is:

Card lifecycle state	TOE lifecycle phase
Creation State	Phase 2. Manufacturing
Initialization State	Phase 3. Personalization of the MRTD
Operation State	Phase 4. Operational Use
Termination State	

2.1. TOE Architecture

The TOE is a composition of IC hardware and embedded software that controls the IC.

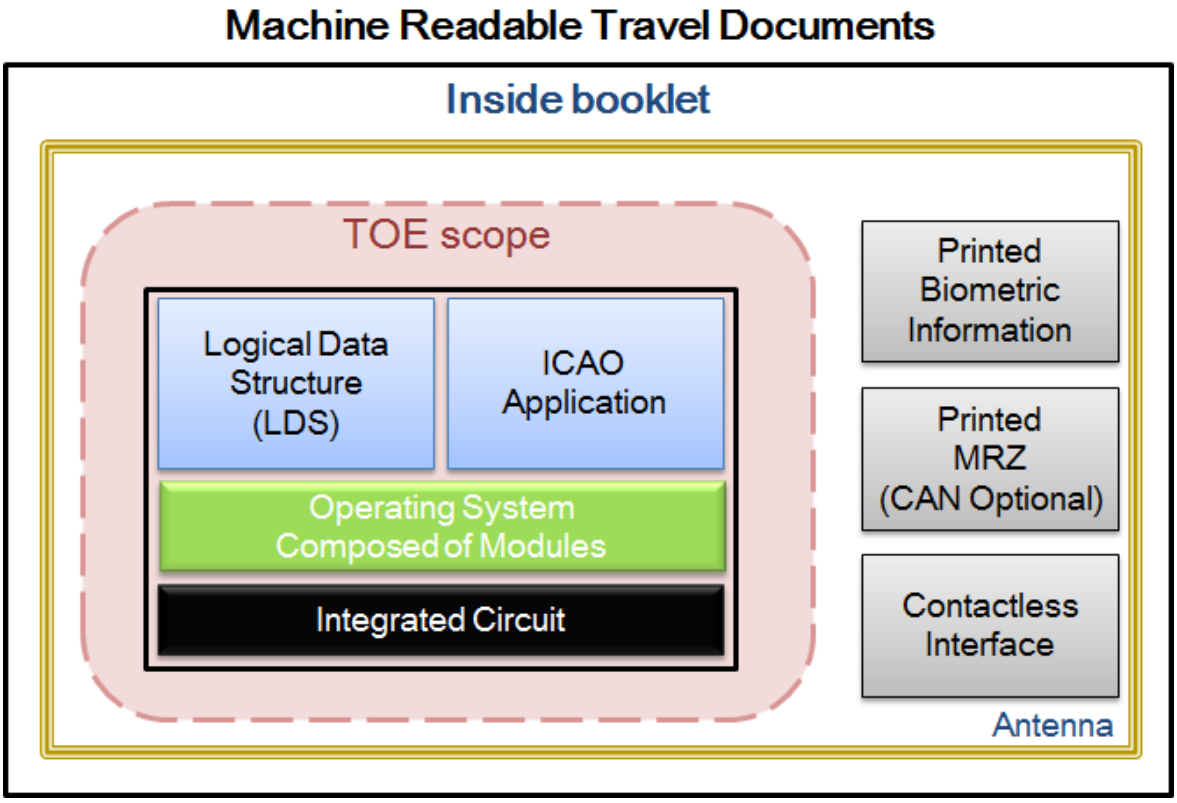

Figure 1. TOE Scope

The TOE is defined to comprise the chip and the hardware abstraction layer and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

2.1.1. TOE guidance

The guidance documentation consists of the:

- [AGD_OPE] this guide is delivered to the card holder (card holder or receiving state)
- [AGD_PRE] this guide is delivered to the personalization agent (issuing state)
- [ALC_DEL] this guide is used by all the entities to deliver the TOE between them.

3. Conformance Claim

This security target claims the following conformance with Common Criteria:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012 conformant.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012 extended conformance with FAU_SAS.1, FCS_RND.1, FMT_LIM.1, FMT_LIM.2, FPT_EMS.1 and FIA_API.1 (defined in the chapter 6. *Extended component definition*).
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 4, September 2012 conformant.

This security target claims the following conformance with protection profiles:

- A strict conformance with Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] version 1.01, 22th July 2014.
- A strict conformance with Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [EAC-PP] version 1.3.2, 5th December 2012.

This security target and the TOE claim conformity with EAL5+, augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis)

3.1. Conformance Claim Rationale

The security target and the TOE are conformant with CC version 3.1 Release 4 and the protection profile with CC version 3.1 Release 3. However, in transition from CC Version 3.1 Revision 3 to CC Version 3.1 Revision 4, there is no modification on SFRs used in the Security Target. Also no modification is made on SARs of the assurance level claimed by the Security Target.

This security target doesn't introduce any additional threat, organization security policy or assumption, objectives for the TOE or environment to [PACE-PP] and [EAC-PP].

This security target includes SFRs defined in [PACE-PP] and [EAC-PP]. If the SFR is duplicated in PPs, ST uses the SFR of [EAC-PP] and that covers the definition in [PACE-PP], being:

- FIA_UID.1/PACE
- FIA_UAU.1/PACE
- FIA_UAU.4/PACE
- FIA_UAU.5/PACE
- FDP_ACC.1/TRM
- FDP_ACF.1/TRM
- FMT_SMR.1/PACE

- FMT_LIM.1
- FMT_LIM.2
- FMT_MTD.1/KEY_READ
- FPT_EMS.1

[PACE-PP] and [EAC-PP] are conformant with ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition and Supplemental Access Control for Machine Readable Travel Documents, Version 1.00. But ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition and Supplemental Access Control for Machine Readable Travel Documents, Version 1.00 documents were merged into ICAO Doc 9303, Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs, seventh Edition [ICAO part11] with the addition of CAM functionality. The security target and the TOE are conformant with [ICAO part11]. The following statements show CAM functionality:

- CAM is one of PACE mechanism for identification and authentication. The following SFRs for identification and authentication are defined as iteration.
  - 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

- CAM is an integrated function of existing PACE and Chip Authentication. Chip authentication mapping can be used instead of the chip authentication version1. The following SFR for authentication proof of identity is defined as iteration.
  - FIA_API.1/PACE_CAM

- Public key and private key are used for CAM. Private key should be managed. The following SFR for management for CAM Private key is defined as iteration.
  - FMT_MTD.1/PACE_CAMPK

- And access to private keys should be restricted. The following SFR for management for CAM public key is defined as iteration.
  - FMT_MTD.1/PACE_CAM_KEY_READ

- Personalization agent should store the public key in the form of a file called CardScurity in TOE for CAM. The following SFR for management for CAM public key is defined as iteration.
  - FMT_MTD.1/PACE_CAMPA

- Generates key for CAM only through ECDH. And CAM supports only AES secure messaging. The following SFRs for cryptographic operations are defined as iteration.
  - FCS_CKM.1/PACE_CAM
  - FCS_COP.1/PACE_CAM_ENC
  - FCS_COP.1/PACE_CAM_MAC

This security target uses additional iteration over several SFR for differentiate authenticate features, being:

- FIA_AFL.1/TRANS
- FIA_AFL.1/ISSUER

  FIA_AFL.1/PACE

FIA_UID.1/TRANS
- FIA_UID.1/ISSUER
- FIA_UID.1/TRANS
- FIA_UAU.1/ISSUER

Finally, FIA_API.1 is updated using iteration, being:
- FIA_API.1/CA

This security target claims conformity with EAL5 extending the EAL4 from PACE-PP and EAC-PP. The differences in the assurance components do not reduce the EAL, indeed enforce some requirements based on module testing and semiformal description of the development parts

- ADV_FSP.4 passes to ADV_FSP.5 (semiformal description of interfaces)
- ADV_TDS.3 passes to ADV_TDS.4 (modules description)
- ALC_CMS.4 passes to ALC_CMS.5 (including tools in the CM list)
- ALC_TAT.1 passes to ALC_TAT.2 (implementation based on Standards)
- ATE_DPT.1 passes to ADV_DPT.3 (testing at module level)
- Adding the component ADV_INT.2 (well-structure internals description)
- AVA_VAN.3 passes to AVA_VAN.4, however the PP and this ST claims for AVA_VAN.5.

The developer uses the EAL5+ for providing more assurance to their customers.

The TOE type of the current security target is "the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) and providing Extended Access Control with PACE", compatible with the expected TOE type described in [PACE-PP] and [EAC-PP].

4. Security Problem Definition

4.1. Introduction

Assets

The assets to be protected by the TOE include the User Data on the MRTD's chip.

Asset	Definition	Generic security property to be maintained by the current security policy
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 SAC] sense of [ICAO SAC]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [BAC-PP]. This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [BAC-PP].	Confidentiality Integrity Authenticity
user data transferred between the TOE and the terminal connected (i.e. 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 de and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the fined in Technical Report SAC between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of Technical Report SAC). User data can be received and sent (exchange ⇔ {receive, send})	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 recognising the TOE not knowing any PAC E password. TOE tracing data can be provided / gathered.	unavailability
Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	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].	Availability
TOE internal secret	Permanently or temporarily stored secret	Confidentiality

cryptographic keys	cryptographic material used by the TOE in order to enforce its security functionality.	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 **And CardSecurity in [ICAO part11]**) used by the TOE in order to enforce its security functionality	Integrity Authenticity
travel document communication establishment authorisation data	Restricted-revealable authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.	Confidentiality Integrity
Logical travel document sensitive User Data	Sensitive biometric reference data (EF.DG3, EF.DG4)	
Authenticity of the travel document's chip	The authenticity of the travel document's chip personalised by the issuing State or Organisation for the travel document holder is used by the traveller to prove his possession of a genuine travel document.	

Subjects and external entities

This ST considers the following subjects external entities:

Role	Definition
travel document holder	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).
Terminal	A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface.
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
Basic Inspection System with PACE (BISPACE)	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.
Extended Inspection System (EIS)	The Extended Inspection System (EIS) performs the Advanced Inspection Procedure (figure 1) 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.
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (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].
Travel document presenter (traveller)	A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [BAC-PP]. Please note that a travel document presenter can also be an attacker (s. below).
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 Doc 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].
Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the [PACE-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 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.
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 LinkCertificates.
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.

4.2. Assumptions

4.2.1. A.Passive_Auth PKI for Passive Authentication

This assumption is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] Chap 3.4).

4.2.2. A.Insp_Sys Inspection Systems for global interoperability

This assumption is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [EAC-PP], Chap 3.2.

4.2.3. A.Auth_PKI PKI for Inspection Systems

This assumption is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [EAC-PP], Chap 3.2.

4.3. Threats

4.3.1. T.Skimming Skimming travel document / Capturing Card-Terminal Communication

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.2.

4.3.2. T.Eavesdropping Eavesdropping on the communication between the TOE and the PACE terminal

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.2.

4.3.3. T.Tracing Tracing travel document

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.2.

4.3.4. T.Forgery Forgery of Data

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.2.

4.3.5. T.Abuse-Func Abuse of Functionality

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.2.

4.3.6. T.Information_Leakage Information Leakage from travel document

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.2.

4.3.7. T.Phys-Tamper Physical Tampering

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.2.

4.3.8. T.Malfunction Malfunction due to Environmental Stress

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.2.

4.3.9. T.Read_Sensitive_Data Read the sensitive biometric reference data

This threat is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [EAC-PP], Chap 3.3.

4.3.10. T.Counterfeit Counterfeit of travel document chip data

This threat is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [EAC-PP], Chap 3.3.

4.4. Organizational Security Policies

4.4.1. P.Manufact Manufacturing of the travel document's chip

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.3.

4.4.2. P.Pre-Operational Pre-operational handling of the travel document

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.3.

4.4.3. P.Card_PKI PKI for Passive Authentication (issuing branch)

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.3.

4.4.4. P.Trustworthy_PKI Trustworthiness of PKI

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.3.

4.4.5. P.Terminal Abilities and trustworthiness of terminals

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP], Chap 3.3.

4.4.6. P.Sensitive_Data Privacy of sensitive biometric reference data

This security policy is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [EAC-PP], Chap 3.4.

4.4.7. P.Personalisation Personalisation of the travel document by issuing State or Organisation only

This security policy is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [EAC-PP], Chap 3.4.

5. 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.

5.1 Security Objectives for the TOE

5.1.1. OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [EAC-PP] (section 4.1).

5.1.2. OT.Chip_Auth_Proof Proof of the travel document’s chip authenticity

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [EAC-PP] (section 4.1).

5.1.3. OT.Data_Integrity Integrity of Data

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1).

5.1.4. OT.Data_Authenticity Authenticity of Data

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1).

5.1.5. OT.Data_Confidentiality Confidentiality of Data

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1)

5.1.6. OT.Tracing Tracing travel document

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1)

5.1.7. OT.Prot_Abuse-Func Protection against Abuse of Functionality

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1)

5.1.8. OT.Prot_Inf_Leak Protection against Information Leakage

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1)

5.1.9. OT.Prot_Phys-Tamper Protection against Physical Tampering

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1)

5.1.10. OT.Prot_Malfunction Protection against Malfunctions

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1)

5.1.11. OT.Identification Identification of the TOE

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1)

5.1.12. OT.AC_Pers Access Control for Personalisation of logical MRTD

This security objective for the TOE is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.1).

5.2. Security Objectives for the Operational Environment

5.2.1. OE.Auth_Key_Travel_Document Travel document Authentication Key

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [EAC-PP] (section 4.2).

5.2.2. OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [EAC-PP] (section 4.2).

5.2.3. OE.Exam_Travel_Document Examination of the physical part of the travel document

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [EAC-PP] (section 4.2).

5.2.4. OE.Prot_Logical_Travel_Document Protection of data from the logical travel document

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [EAC-PP]

section 4.2).

5.2.5. OE.Ext_Insp_Systems Authorization of Extended Inspection Systems

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [EAC-PP] (section 4.2).

5.2.6. OE.Legislative_Compliance Issuing of the travel document

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.2).

5.2.7. OE.Passive_Auth_Sign Authentication of travel document by Signature

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.2).

5.2.8. OE.Personalisation Personalisation of travel document

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.2).

5.2.9. OE.Terminal Terminal operating

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.2).

5.2.10. OE.Travel_Document_Holder Travel document holder Obligations

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 4.2).

5.3. Security Objective Rationale

The following table provides an overview for security objectives coverage:

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holde	OE.Legislative_Compliance
T.Read_Sensitive_Data	x													x			x					
T.Counterfeit		x											x		x							

T.Skimming				x	x	x													X	
T.Eavesdropping						X														
T.Tracing							X												X	
T.Abuse-Func								x												
T.Information_Leakage									x											
T.Phys-Tamper										X										
T.Malfunction											X									
T.Forgery			x	x	x			x			x			x			x	x	x		
P.Sensitive_Data	x												x			X				
P.Personalization			x							x							X			
P.Manufact										X										
P.Pre-Operational			x							x							x			X
P.Terminal														X					x	
P.Card_PKI																		X		
P.Trustworthy_PKI																		X		
A.Insp_Sys														x	X					
A.Auth_PKI													x			X				
A.Passive_Auth														x				x		

Table 3. Coverage table between SPD and Objectives

A detailed justification required for suitability of the security objectives to coup with the security problem definition is given below.

The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact interface. This threat is countered by the security objectives OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality through the PACE authentication. The objective OE.Travel_Document_Holder ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

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

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

The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective OT.AC_Pers requires the TOE to limit the write access for the travel document to the trustworthy Personalisation Agent (cf. OE.Personalisation). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives OT.Data_Integrity and OT.Data_Authenticity, respectively. The objectives OT.Prot_Phys-Tamper and OT.Prot_Abuse-Func contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to OE.Terminal and performing the Passive Authentication using the Document Security Object as aimed by OE.Passive_Auth_Sign will be able to effectively verify integrity and authenticity of the

data received from the TOE.

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

The threats **T.Information_Leakage**, **T.Phys-Tamper** and **T.Malfunction** are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is obviously addressed by the directly related security objectives OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper and OT.Prot_Malfunction, respectively.

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

The OSP **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'.

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

The OSP **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).

The OSP **P.Trustworthy_PKI** is enforced by OE.Passive_Auth_Sign (for CSCA, issuing PKI branch).

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

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

Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems”.

The OSP **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]. **E.Exam_Travel_Document** enforces the terminals to perform the terminal part of the PACE protocol.

The threat **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 **or CardSecurity** 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.

The threat **T.Forgery** “Forgery of data” addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. Additionally to the security objectives from [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 examination of the travel document addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objectives for the TOE environment **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” which requires the inspection system to examine physically the travel document, the
Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document’s chip. The security objectives for the TOE environment **OE.Prot_Logical_Travel_Document** “Protection of data from the logical travel document” require the Inspection System to protect the logical travel document data during the transmission and the internal handling.

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] 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”.

The assumption **A.Auth_PKI** “PKI for Inspection Systems” is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** “Authorization for use of sensitive biometric reference data” requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organisations only. The Document Verifier of the receiving State is required

by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems” to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure.

6. Extended Components Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [EAC-PP] and the others are defined in [PACE-PP].

6.1. Definition of Family FIA_API

This family and components (FIA_API.1) of security functional requirements are included and described in the MRTD, “ICAO Application", Extended Access Control with PACE [EAC-PP] (section 5.1).

6.2. Definition of Family FAU_SAS

This family and components (FAU_SAS.1) of security functional requirements are included and described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 5.1)

6.3. Definition of Family FCS_RND

This family and components (FCS_RND.1) of security functional requirements are included and described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 5.2)

6.4. Definition of Family FMT_LIM

This family and components (FMT_LIM.1 and FMT_LIM.2) of security functional requirements are included and described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 5.3).

6.5. Definition of Family FPT_EMS

This family and components (FPT_EMS.1) of security functional requirements are included and described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PACE-PP] (section 5.4).

7. Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 of the CC. Each of these operations is used in [EAC-PP].

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. The added/changed words for the refinement are written in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that ~~were removed~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicized. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized like *this*.

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

The definition of the subjects "Manufacturer", "Personalisation Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and "re-authenticate" are originally taken from [CC part 2]. The operation "load" is synonymous to "import" used in [CC part 2].

Definition of security attributes:

security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR-03], A.5.1); 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-03], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA v.1 1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR-03], A.5.1); Terminal is

		authenticated as foreign Document Verifier after successful CA and TA
	IS	roles defined in the certificate used for authentication (cf. [TR-03], A.5.1); 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-03], A.5.1)
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR-03], A.5.1)
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [TR-03], A.5.1)

Table 4. Security Attributes

The following table provides an overview of the keys and certificates used. Further keys and certificates are listed in [PACE-PP].

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 attributes.
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 11770-3].
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 Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.

	Or The Chip Authentication Public Key (PKICC) is stored in signed CardSecurity Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Mapping 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	Country Signing Certification Authority of the issuing State or Organisation signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organisation (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organisation signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organisation with the Document Signer Public Key.
Chip Authentication Session Keys	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	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.

Table 5. Keys and Certificates

7.1. Security Functional Requirements for the TOE

This section describes the security functional requirements for the TOE.

7.1.1. Class FCS Cryptographic Support

Cryptographic key generation (FCS_CKM.1)

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2).

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

Hierarchical to:	No other components.
Dependencies	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1 /DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to TR-03111*][1] and specified cryptographic key sizes [assignment: *DH 2048 , ECDH 256*] that meet the following: [ICAO SAC][2]

[1] [assignment: *cryptographic key generation algorithm*]
[2] [assignment: *list of standard*]

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

Hierarchical to:	No other components.
Dependencies	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to TR-03111*] and specified cryptographic key sizes [assignment: *DH 2048, ECDH 256*] that meet the following:[selection: *based on the Diffie-Hellman key derivation protocol compliant to PKCS#3 and TR-03110-1 , based on an ECDH protocol compliant to TR-03111*][3]

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

Hierarchical to:	No other components.
Dependencies	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1 /PACE_CAM	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:*ECDH compliant to TR-03111, ICAO part11*] and specified cryptographic key sizes [assignment: *ECDH 256*] that meet the following:[assignment: *based on an ECDH protocol compliant to TR-03111*]

Cryptographic key destruction (FCS_CKM.4)

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (Common Criteria Part 2).

FCS_CKM.4 Cryptographic key destruction – Session key

Hierarchical to:	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *randomisation]* that meets the following: [assignment: *none*].

Cryptographic operation (FCS_COP.1)

The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (Common Criteria Part 2).

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

Hierarchical to:	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1/ PACE_ENC	The TSF shall perform secure messaging – encryption and decryption [4]in accordance with a specified cryptographic algorithm [selection: *AES,*

[3] [assignment: *list of standards*]

[4] [assignment: *list of cryptographic operations*]

3DES] in CBC mode[5] and cryptographic key sizes [selection: *112, 128, 192, 256*] bit[6] that meet the following: compliant to [ICAO SAC][7].

Application note: secure messaging – encryption and decryption operation with Triple-DES CBC mode (112 bits key) or AES CBC mode (128,192,256 bits keys)
The 3DES is supported by the TOE only for compatibility with ICAO9303. According to TR-03110, the 3DES is deprecated for CA and PACE authentication operation, so a user should use AES for CA or PACE authentication.

FCS_COP.1/PACE_MAC Cryptographic operation – MAC

Hierarchical to:	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1/ PACE_MAC	The TSF shall perform secure messaging – message authentication code[8] in accordance with a specified cryptographic algorithm [selection: *CMAC, Retail-MAC*][9] and cryptographic key sizes [selection: *112, 128, 192, 256*] bit[10] that meet the following: compliant to [ICAO SAC][11].

Application note: secure messaging – MAC operation with *Retail-MAC* (112 bits key) or CMAC (128,192,256 bits keys)

FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption

Hierarchical to:	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ CA_ENC	The TSF shall perform secure messaging – encryption and decryption[12] in accordance with a specified cryptographic algorithm [assignment: *AES, 3DES in CBC mode*] and cryptographic key sizes [assignment: *112, 128, 192, 256*] that meet the following: [assignment: *ICAO 9303, TR-03110-1*].

Application note: secure messaging – encryption and decryption operation with Triple-DES CBC mode (112 bits key) or AES CBC mode (128,192,256 bits keys)
The 3DES is supported by the TOE only for compatibility with ICAO9303. According to TR-03110, the 3DES is deprecated for CA and PACE authentication operation, so a user should use AES for CA or PACE authentication.

FCS_COP.1/CA_MAC Cryptographic operation – MAC

[5] [assignment: *cryptographic algorithm*]
[6] [assignment: *cryptographic key sizes*]
[7] [assignment: *list of standards*]
[8] [*assignment: list of cryptographic operations*]
[9] [assignment: *cryptographic algorithm*]
[10] [assignment: *cryptographic key sizes*]
[11] [assignment: *list of standards*]
[12] [*assignment: list of cryptographic operations*]

Hierarchical to:	No other components.
Dependencies	FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ CA_MAC	The TSF shall perform secure messaging – message authentication code[13] in accordance with a specified cryptographic algorithm [assignment: *CMAC, Retail-MAC*] and cryptographic key sizes [assignment: *112, 128, 192, 256*] that meet the following: [assignment: *ICAO 9303, TR-03110-1*].

Application note: secure messaging – MAC operation with *Retail-MAC* (112 bits key) or CMAC (128,192,256 bits keys)

FCS_COP.1/PACE_CAM_ENC Cryptographic operation – Symmetric Encryption / Decryption

Hierarchical to:	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ PACE_CAM _ENC	The TSF shall perform [assignment: secure messaging - *encryption and decryption*] in accordance with a specified cryptographic algorithm [assignment: *AES in CBC mode*] and cryptographic key sizes [assignment: *128, 192, 256*] that meet the following: [assignment: *ICAO part11*].

Application note: secure messaging – encryption and decryption operation with AES CBC mode (128,192,256 bits keys)

FCS_COP.1/PACE_CAM_MAC Cryptographic operation – MAC

Hierarchical to:	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ PACE_CAM _MAC	The TSF shall perform [assignment: secure messaging - *message authentication code*] in accordance with a specified cryptographic algorithm [assignment: *CMAC*] and cryptographic key sizes [assignment: *128, 192, 256*] that meet the following: [assignment: *ICAO part11*].

Application note: secure messaging – MAC operation with *Retail-MAC* (112 bits key) or CMAC (128,192,256 bits keys)

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by travel document

Hierarchical to:	No other components.
Dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

[13] [*assignment: list of cryptographic operations*]

FCS_COP.1.1 /SIG_VER	The TSF shall perform digital signature verification[14] in accordance with a specified cryptographic algorithm [assignment: *ECDSA(SHA-224, SHA-256), RSASSA-PSS(SHA-256)*] and cryptographic key sizes [assignment: *ECDSA(256 key sizes), RSA(2048 key sizes)*] that meet the following: [assignment: *ISO15946-2, PKCS1*].

Subset access control (FCS_RND.1)

The TOE shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

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: 1. *Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.* 2. *The average Shannon entropy per internal random bit exceeds 0.997(7.976 bits per octet)*]

7.1.2. Class FIA Identification and Authentication

Authentication failure handling (FIA_AFL.1)

The TOE shall meet the requirement “Authentication failure handling (FIA_AFL.1)” as specified below (Common Criteria Part 2).

FIA_AFL.1/TRANS Authentication failure handling-Transport key authentication using

Hierarchical to:	No other components.
Dependencies	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1 /TRANS	The TSF shall detect when [selection: *[assignment: 30]]* **consecutive** unsuccessful authentication attempts occur related to [assignment: *failure of a Triple-DES based Transport key authentication*].
FIA_AFL.1.2 /TRANS	When the defined number of unsuccessful authentication attempts has been [selection: *met*], the TSF shall [assignment: *terminate itself or generate security reset*].

Application note: Regarding authentication, the 3DES is adopted by the TOE only for transport key authentication and issuer authentication. So users should use AES for CA or PACE authentication.

FIA_AFL.1/ISSUER Authentication failure handling-Issuer authentication using

Hierarchical to:	No other components.
Dependencies	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1 /ISSUER	The TSF shall detect when [selection: *[assignment: 30]]* **consecutive** unsuccessful authentication attempts occur related to [assignment: *failure of a Triple-DES based issuer authentication*].
FIA_AFL.1.2 /ISSUER	When the defined number of unsuccessful authentication attempts has been [selection: *met*], the TSF shall [assignment: *terminate itself or generate security reset*].

Application note: Regarding authentication, the 3DES is adopted by the TOE only for transport key authentication and issuer authentication. So users should use AES for CA or

[14] [assignment: *list of cryptographic operations*]

PACE authentication.

FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authorisation data

Hierarchical to:	No other components.
Dependencies	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1 /PACE	The TSF shall detect when [assignment: *1*] **consecutive** unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password[15].
FIA_AFL.1.2 /PACE	When the defined number of unsuccessful authentication attempts has been met[16], the TSF shall [assignment: *increase the reaction time of the TOE to the next authentication attempt using PACE password by 0.1 seconds until reaching a maximum of 3 seconds*].

Timing of identification (FIA_UID.1)

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2).

FIA_UID.1/TRANS Timing of identification

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_UID.1.1 /TRANS	The TSF shall allow [assignment: *request of commands which are available in the 'Creation state' of Card lifecycle*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 /TRANS	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1/ISSUER Timing of identification

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_UID.1.1 /ISSUER	The TSF shall allow [assignment: *request of commands which are available in the 'Initialization state' of Card lifecycle, except the dedicated commands for ISSUER key authenticated channel*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 /ISSUER	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1/PACE Timing of identification

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_UID.1.1 /PACE	The TSF shall allow 1.to establish the communication channel, 2.carrying out the PACE Protocol according to [ICAO SAC], 3.to read the Initialization 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][17]

[15] [assignment: *list of authentication events*]
[16] [selection: *met, surpassed*]
[17] [assignment: *list of TSF-mediated actions*]

	6.[assignment: *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_UID.1/PACE_CAM Timing of identification

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_UID.1.1 /PACE_CAM	The TSF shall allow [assignment : *1.to establish the communication channel,* *2.carrying out the CAM with PACE Protocol according to [ICAO 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.

Timing of authentication (FIA_UAU.1)

The TOE shall meet the requirement “Timing of authentication (FIA_UAU.1)” as specified below (Common Criteria Part 2).

Application note: The user of identified after a successfully performed CAM with PACE protocol is a terminal.

FIA_UAU.1/TRANS Timing of authentication

Hierarchical to:	No other components.
Dependencies	FIA_UID.1 Timing of identification.
FIA_UAU.1.1/TRANS	The TSF shall allow [assignment: *request of commands which are available in the ‘Creation state’ of Card lifecycle*] on behalf of the user to be performed before the user is authenticated.
FIA_UAU1.2/TRANS	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/ISSUER Timing of authentication

Hierarchical to:	No other components.
Dependencies	FIA_UID.1 Timing of identification.
FIA_UAU.1.1/ISSUER	The TSF shall allow [assignment: *request of commands which are available in the ‘Initialization state’ of Card lifecycle, except the dedicated commands for ISSUER key authenticated channel*] on behalf of the user to be performed before the user is authenticated.
FIA_UAU1.2/ISSUER	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PACE Timing of authentication

Hierarchical to:	No other components.
Dependencies	FIA_UID.1 Timing of identification.
FIA_UAU.1.1/PACE	The TSF shall allow 1. to establish the communication channel, 2. carrying out the PACE Protocol according to ICAO Technical Report “Supplemental Access Control”,

	3. to read the Initialization 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 Version 1 according to [TR-03110-1] 6. to carry out the Terminal Authentication Protocol Version 1 according to [TR-03110-1][18] 7. [assignment: *none*] on behalf of the user to be performed before the user is authenticated.
FIA_UAU1.2/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.1/PACE_CAM Timing of authentication

Hierarchical to:	No other components.
Dependencies	FIA_UID.1 Timing of identification.
FIA_UAU.1.1/ PACE_CAM	The TSF shall allow [assignment: *1. to establish the communication channel,* *2. carrying out the CAM with PACE Protocol according to [ICAO part 11],* *3. to identify themselves by selection of the authentication key*] 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.

Application note: The user authenticated after a successfully performed CAM with PACE protocol is a terminal.

Single-use authentication mechanisms (FIA_UAU.4)

The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

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

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_UAU.4.1/ PACE	The TSF shall prevent reuse of authentication data related to 1.PACE Protocol according to [ICAO SAC], 2.Authentication Mechanism based on [selection: *AES*] 3.Terminal Authentication Protocol v.1 according to [TR-03110-1][19]

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

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_UAU.4.1/ PACE_CAM	The TSF shall prevent reuse of authentication data related to [assignment: *1.CAM with PACE Protocol according to [ICAO part 11],* *2.Authentication Mechanism based on AES*]

[18] [assignment: *list of TSF-mediation actions*]
[19] [assignment: *identified authentication mechanism(s)*]

Multiple authentication mechanisms (FIA_UAU.5)

The TOE shall meet the requirements of "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2).

FIA_UAU.5/PACE Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies	No dependencies
FIA_UAU.5.1 /PACE	The TSF shall provide 1.PACE Protocol according to [ICAO SAC], 2.Passive Authentication according to [ICAO 9303] 3.Secure messaging in MAC-ENC mode according to [ICAO SAC], 4.Symmetric Authentication Mechanism based on [selection:*AES*] 5.Terminal Authentication Protocol v.1 according to [TR-03110-1][20], 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 as Personalisation Agent by [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]. 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 v.1. 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.[21] 5. [assignment: *none*]

FIA_UAU.5/PACE_CAM Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies	No dependencies
FIA_UAU.5.1/ PACE_CAM	The TSF shall provide [assignment: *1.CAM with PACE Protocol according to [ICAO part11]*] to support user authentication.
FIA_UAU.5.2/ PACE_CAM	The TSF shall authenticate any user's claimed identity according to the [assignment : *following rules:* *1. Having successfully run the CAM with 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. After run of the CAM with PACE the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with CAM.* *3. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the*

[20] [assignment: *list of multiple authentication mechanisms*]
[21] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

public key presented during the CAM and the secure messaging established by the CAM Mechanism].

Application note: The user authenticated after a successfully performed CAM with PACE protocol is a terminal.

Re-authenticating (FIA_UAU.6)

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

FIA_UAU.6/PACE Re-authenticating of Terminal by the TOE

Hierarchical to:	No other components.
Dependencies	No dependencies.
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[22].

FIA_UAU.6/EAC Re-authenticating of Terminal by the TOE

Hierarchical to:	No other components.
Dependencies	No dependencies.
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[23].

FIA_UAU.6/PACE_CAM Re-authenticating of Terminal by the TOE

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_UAU.6.1 /PACE_CAM	The TSF shall re-authenticate the user under the conditions [assignment: *each command sent to the TOE after successful run of the CAM with PACE protocol shall be verified as being sent by the PACE terminal.*]

Application note: The user authenticated after a successfully performed CAM with PACE protocol is a terminal.

Authentication Proof of Identity (FIA_API.1)

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended).

FIA_API.1/CA Authentication Proof of Identity

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_API.1.1/CA	The TSF shall provide a [assignment: *Chip Authentication Protocol Version 1 according to [TR-03110-1]*] to prove the identity of the [assignment: *TOE*].

FIA_API.1/PACE_CAM Authentication Proof of Identity

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_API.1.1	The TSF shall provide a [*assignment: Chip Authentication Mapping*

[22] [assignment: *list of conditions under which re-authentication is required*]
[23] [assignment: *list of conditions under which re-authentication is required*]

/PACE_CAM	*according to [ICAO part11]*] to prove the identity of the [assignment*: TOE*]

7.1.3. Class FDP User Data Protection

Subset access control (FDP_ACC.1)

The TOE shall meet the requirement “Subset access control (FDP_ACC.1)” as specified below (Common Criteria Part 2).

FDP_ACC.1/TRM Subset access control

Hierarchical to:	No other components.
Dependencies	FDP_ACF.1 Security attribute based access control
FDP_ACC /TRM.1.1	The TSF shall enforce the Access Control SFP[24] on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document[25]

Security attribute based access control (FDP_ACF.1)

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (Common Criteria Part 2).

FDP_ACF.1/TRM Security attribute based access control

Hierarchical to:	No other components.
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1 /TRM	The TSF shall enforce the Access Control SFP[26] to objects based on the following: 1. Subjects: a. Terminal, b. BIS-PACE c. Extended Inspection System 2. Objects: a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document , b. data in EF.DG3 of the logical travel document , c. data in EF.DG4 of the logical travel document , d. all TOE intrinsic secret cryptographic keys stored in the travel document, 3. Security attributes a. PACE Authentication b. Terminal Authentication v.1 c. Authorisation of the Terminal[27]
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 SAC] after a successful PACE authentication as required by FIA_UAU.1/PACE[28].

[24] [assignment: *access control SFP*]
[25] [assignment: *list of subjects, objects and operations among subjects and objects covered by the SFP*]
[26] [assignment: *access control SFP*]
[27] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[28] [assignment: rules governing access among controlled subjects and controlled objects using controlled

FDP_ACF.1.3 /TRM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[29].
FDP_ACF.1.4 /TRM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1.Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the 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[30].

Subset residual information protection (FDP_RIP.1)

The TOE shall meet the requirement “Subset residual information protection (FDP_RIP.1)” as specified below (Common Criteria Part 2).

FDP_RIP.1 Subset residual information protection

Hierarchical to:	No other components.
Dependencies	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *deallocation of the resource from*] the following objects: 1.Session Keys (immediately after closing related communication session) , 2.the ephemeral private key ephem - SKpicc- PACE (by having generated a DH shared secret K)[31], 3.[assignment:*none*].

Basic data exchange confidentiality (FDP_UCT.1)

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD

Hierarchical to:	No other components.
Dependencies	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM

operations on controlled objects]

[29] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[30] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[31] [assignment: *list of objects*]

FDP_UCT.1.1 /TRM	The TSF shall enforce the Access Control SFP[32] to be able to transmit and receive[33] user data in a manner protected from unauthorised disclosure.

Data exchange integrity (FDP_UIT.1)

The TOE shall meet the requirement “Data exchange integrity (FDP_UIT.1)” as specified below (Common Criteria Part 2).

FDP_UIT.1/TRM Data exchange integrity

Hierarchical to:	No other components.
Dependencies	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UIT.1.1 /TRM	The TSF shall enforce the Access Control SFP[34] to be able to transmit and receive[35] user data in a manner protected from modification, deletion, insertion and replay[36] errors.
FDP_UIT.1.2 /TRM	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[37] has occurred.

7.1.4. Class FTP Trusted Path/Channels

Inter-TSF trusted channel (FTP_ITC.1)

The TOE shall meet the requirement “Inter-TSF trusted channel (FTP_ITC.1)” as specified below (Common Criteria Part 2).

FTP_ITC.1/PACE Inter-TSF trusted channel after PACE

Hierarchical to:	No other components.
Dependencies	No Dependencies
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	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal[38].

7.1.5. Class FAU Security Audit

Audit storage (FAU_SAS.1)

The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below

[32] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[33] [selection: *transmit, receive*]
[34] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[35] [selection: *transmit, receive*]
[36] [selection: *modification, deletion, insertion, replay*]
[37] [selection: *modification, deletion, insertion, replay*]
[38] [assignment: *list of functions for which a trusted channel is required*]

(Common Criteria Part 2 extended).

FAU_SAS.1 Audit storage

Hierarchical to:	No other components.
Dependencies	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer[39] with the capability to store the Initialisation and Pre-Personalisation Data[40] in the audit records.

7.1.6. Class FMT Security Management

Specification of Management Functions (FMT_SMF.1)

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2 extended).

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1.Initialization, 2.Pre-personalisation , 3.Personalisation 4.Configuration[41].

Security roles (FMT_SMR.1)

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

FMT_SMR.1/PACE Security roles

Hierarchical to:	No other components.
Dependencies	FIA_UID.1 Timing of identification.
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[42]
FMT_SMR.1.2 /PACE	The TSF shall be able to associate users with roles.

Limited capabilities (FMT_LIM.1)

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

[39] [assignment: *authorised users*]
[40] [assignment: *list of audit information*]
[41] [assignment: *list of management functions to be provided by the TSF*]
[42] [assignment: *the authorised identified roles*]

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: 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 User Data (EF.DG3 and EF.DG4) to be disclosed[43],

Limited availability (FMT_LIM.2)

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

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: 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 User Data (EF.DG3 and EF.DG4) to be disclosed[44],

Management of TSF data (FMT_MTD.1)

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2).

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

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1 /INI_ENA	The TSF shall restrict the ability to write[45] the Initialisation Data and Pre-personalisation Data[46] to the Manufacturer[47].

FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data

[43] [assignment: *Limited capability and availability policy*]
[44] [assignment: *Limited capability and availability policy*]
[45] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[46] [assignment: *list of TSF data*]
[47] [assignment: *the authorised identified roles*]

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1 /INI_DIS	The TSF shall restrict the ability to read out[48] the Initialisation Data and the Pre-personalisation Data[49] to the Personalisation Agent[50].

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

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles：fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1 /KEY_READ	The TSF shall restrict the ability to read[51] the 1.PACE passwords, 2.Chip Authentication Private Key, 3.Personalisation Agent Keys[52] to none[53]

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

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1 / PACE_CAM _KEY_READ	The TSF shall restrict the ability to [selection: [assignment: *read*]] the [assignment: *1.Chip Authentication Private Key for CAM*] to [assignment: *none*]

FMT_MTD.1/PA Management of TSF data – Personalisation Agent

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/PA	The TSF shall restrict the ability to write[54] the Document Security Object (SOD)[55] to the Personalisation Agent[56].

FMT_MTD.1/PACE_CAMPA Management of TSF data – Personalisation Agent

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1 /PACE_CAMPA	The TSF shall restrict the ability to [selection: [assignment: *write*]] the [assignment: *file with CAM public key in [ICAO part11]*] to [assignment: *the Personalisation Agent*.]

[48] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[49] [assignment: *list of TSF data*]
[50] [assignment: *the authorised identified roles*]
[51] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[52] [assignment: *list of TSF data*]
[53] [assignment: *the authorized identified roles*]
[54] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[55] [assignment: *list of TSF data*]
[56] [assignment: *the authorized identified roles*]

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

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1 /CVCA_INI	The TSF shall restrict the ability to write[57] the 1.initial Country Verifying Certification Authority Public Key, 2.initial Country Verifying Certification Authority Certificate, 3.initial Current Date, 4.[assignment: *none*][58] to [assignment: *Personalization Agent*].

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

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1 /CVCA_UPD	The TSF shall restrict the ability to update[59] the 1.Country Verifying Certification Authority Public Key, 2.Country Verifying Certification Authority Certificate[60] to Country Verifying Certification Authority[61].

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

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1 /DATE	The TSF shall restrict the ability to modify[62] the Current date[63] to 1.Country Verifying Certification Authority, 2.Document Verifier, 3.Domestic Extended Inspection System[64].

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

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1 /CAPK	The TSF shall restrict the ability to [selection: *load*][65] the Chip Authentication Private Key[66] to [assignment: *Personalization Agent*].

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

Hierarchical to:	No other components.
Dependencies	FMT_SMF.1 Specification of management functions

[57] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[58] [assignment: *list of TSF data*]
[59] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[60] [assignment: *list of TSF data*]
[61] [assignment: *the authorized identified roles*]
[62] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[63] [assignment: *list of TSF data*]
[64] [assignment: *the authorized identified roles*]
[65] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[66] [assignment: *list of TSF data*]

	FMT_SMR.1 Security roles
FMT_MTD.1.1 /PACE_CAMPK	The TSF shall restrict the ability to [selection: [assignment: *load*]] the [assignment: *Chip Authentication Private Key for CAM*] to [assignment: *the Personalization Agent*].

Secure TSF data (FMT_MTD.3)

The TOE shall meet the requirement “Secure TSF data (FMT_MTD.3)” as specified below (Common Criteria Part 2).

FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components.
Dependencies	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1	The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control[67].

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.

7.1.7. Class FPT Protection of the Security Functions

TOE Emanation (FPT_EMS.1)

[67] [assignment: *list of TSF data*]

The TOE shall meet the requirement “TOE Emanation (FPT_EMS.1)” as specified below (Common Criteria Part 2 extended).

FPT_EMS.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies	No Dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *electromagnetic field*] in excess of [assignment*: values that allows deduce sensitive information*] enabling access to 1.Chip Authentication Session Keys 2.PACE session Keys (PACE-K MAC, PACE-KEnc), 3.the ephemeral private key ephem SKpicc-PACE, 4.[assignment: *Transport key, Chip Authentication Key for CAM*], 5.Personalisation Agent Key(s), 6.Chip Authentication Private Key[68] and 7.[assignment: *EF.DG1 to EF.DG16, EF.SOD, EF.COM*].
FPT_EMS.1.2	The TSF shall ensure any users[69] are unable to use the following interface smart card circuit contacts[70] to gain access to 1.Chip Authentication Session Keys 2.PACE session Keys (PACE-K MAC, PACE-KEnc), 3.the ephemeral private key ephem SKpicc-PACE, 4.[assignment: *Transport key, Chip Authentication Key for CAM*], 5.Personalisation Agent Key(s), 6.Chip Authentication Private Key[71] and 7.[assignment: *EF.DG1 to EF.DG16, EF.SOD, EF.COM*].

Failure with preservation of secure state (FPT_FLS.1)

The TOE shall meet the requirement “Failure with preservation of secure state (FPT_FLS.1)” as specified below (Common Criteria Part 2).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies	No Dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1.Exposure to operating conditions causing a TOE malfunction, 2.Failure detected by TSF according to FPT_TST.1[72], 3.[assignment: *none*].

TSF testing (FPT_TST.1)

The TOE shall meet the requirement “TSF testing (FPT_TST.1)” as specified below (Common Criteria Part 2).

FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies	No Dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests [selection: *during initial start-up, at the conditions* [assignment:

[68] [assignment: *list of types of TSF data*]
[69] [assignment: *type of users*]
[70] [assignment: *type of connection*]
[71] [assignment: *list of types of TSF data*]
[72] [assignment: *list of types pf failures in the TSF*]

1.under which FLAG_SELF_TEST should on for initial start up test, 2.before the cryptographic operation is activated, and after the cryptographic operation has been activated]
to demonstrate the correct operation of the TSF[73].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[74].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[75].

Resistance to physical attack (FPT_PHP.3)

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies No Dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[76] to the TSF[77] by responding automatically such that the SFRs are always enforced.

7.2. Security Assurance Requirements for the TOE

The for the evaluation of the TOE and its development and operating environment are those taken from the

- Evaluation Assurance Level 5 (EAL5) and augmented by taking the following component:
- ALC_DVS.2 and AVA_VAN.5

7.3. Security Functional Requirement Rationale

The traceability table and the coverage rationale between SFR and security objectives is provided in [EAC-PP], section 6.3.1. Note that FIA_API.1/CA is the same SFR that FIA_API.1 provided in [EAC-PP].

Rationale for additional SRFs as below

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality
FCS_CKM.1/PACE_CAM	x	x	x	x	x	x
FCS_COP.1/PACE_CAM_ENC	x	x	x			x
FCS_COP.1/PACE_CAM_MAC	x	x	x	x	x	
FIA_AFL.1/TRNAS			X			

[73] [selection: *[assignment: parts of TSF], the TSF*]
[74] [selection: *[assignment: parts of TSF], TSF data*]
[75] [selection: *[assignment: parts of TSF], TSF*]
[76] [assignment: *physical tampering scenarios*]
[77] [assignment: *list of TSF devices/elements*]

FIA_AFL.1/ISSUER			X			
FIA_UID.1/TRANS			X			
FIA_UID.1/ISSUER			X			
FIA_UID.1/PACE_CAM	x		x	x	x	x
FIA_UAU.1/TRANS			X			
FIA_UAU.1/ISSUER			X			
FIA_UAU.1/PACE_CAM	x		x	x	x	x
FIA_UAU.4/PACE_CAM	x		x	x	x	x
FIA_UAU.5/PACE_CAM	x		x	x	x	x
FIA_UAU.6/PACE_CAM	x		x	x	x	x
FIA_API.1/CA (same SFR that FIA_API.1 provided in [EAC-PP])		x				
FIA_API.1/PACE_CAM		x				
FMT_MTD.1/PACE_CAMPK	x	x		x		
FMT_MTD.1/PACE_CAMPA			x	x	x	x
FMT_MTD.1/PACE_CAM_KEY_READ	x	x	x	x	x	x

The iterations for CAM do not make changes in the SFRs of [PACE-PP] and [EAC-PP]. And the iterations for CAM compatible with the SFRs and security objects defined in [PACE-PP] and [EAC-PP] as follows.

The security objective **OT.Data_Integrity** aims that the TOE always ensures integrity of the User- and TSF-data stored and, after the PACE authentication, of these data exchanged (physical manipulation and unauthorised modifying). FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM and FCS_CKM.4 represent some required specific properties of the protocols used.Unauthorised modifying of the exchanged data is addressed, in the first line, by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_CAM_MAC. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM) using FCS_CKM.1/PACE_CAM and possessing the special properties FIA_UAU.5/PACE_CAM, FIA_UAU.6/PACE_COM. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). The SFR FMT_MTD.1./KEY_READ restricts the access to the chip authentication private key for CAM.
FMT_MTD.1/PACE_CAMPA requires that CardScurity containing signature over the chip authentication public key 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.

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_CAM_MAC. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM) using FCS_CKM.1/PACE_CAM and possessing the special properties FIA_UAU.5/PACE_CAM, FIA_UAU.6/PACE_CAM. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). The SFR FMT_MTD.1./KEY_READ restricts the access to the chip authentication private key for CAM. FMT_MTD.1/PACE_CAMPA requires that CardSecurity containing signature over the chip authentication public key 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.FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM and FCS_CKM.4 represent

some required specific properties of the protocols used.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.

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, 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_CAM, FIA_UAU.5/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_CAM_ENC. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE_CAM, FIA_UAU.6/PACE_CAM. FDP_RIP.1 requires erasing the values of session keys (here: for Kenc). The SFR FMT_MTD.1./PACE_CAM_KEY_READ restricts the access to chip authentication private key. FMT_MTD.1/PACE_CAMPA requires that CardSecurity containing signature over the chip authentication public key 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.

The security objective **OT.Chip_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Mapping provided by FIA_API.1/PACE_CAM proving the identity of the TOE. The Chip Authentication Mapping defined by FCS_CKM.1/PACE_CAM is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/PACE_CAMPK and FMT_MTD.1/PACE_CAM_KEY_READ. The Chip Authentication Mapping [ICAO part11] requires additional TSF according to FCS_CKM.1/PACE_CAM (for the derivation of the session keys), FCS_COP.1/PACE_CAM_CA_ENC and FCS_COP.1/PACE_CAM_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 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_CAM and FIA_UAU.1/PACE_CAM require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE_CAM requires the successful Chip Authentication Mapping before any authentication attempt as Extended Inspection System. During the protected communication following the CAM the reuse of authentication data is prevented by FIA_UAU.4/PACE_CAM. The SFR FIA_UAU.6/PACE_CAM and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication Mapping 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/PACE_CAM (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/PACE_CAM_ENC and FCS_COP.1/PACE_CAM_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/PACE_CAMPK and FMT_MTD.1/PACE_CAM_KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

The security objective **OT.AC_Pers** "Access Control for Personalisation of logical travel document" addresses the access control of the writing the logical travel document.
The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data.
The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write chap authentication public key for CAM of the logical travel document only once. Before the PACE authentication, the FIA_AFL.1/TRANS, FIA_AFL.1/ISSUER, FIA_UID.1/TRANS, FIA_UID.1/ISSUER, FIA_UAU.1/TRANS and FIA_UAU.1/ISSUER help providing interim authentication phase for enhanced preventing of unauthorized personalisation tries. FMT_MTD.1/PACE_CAMPA covers the related property of OT.AC_Pers (writing CardSecurity). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1/KEY_READ and FMT_MTD.1/PACE_CAM_KEY_READ and FPT_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.
The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE_CAM and FIA_UAU.5/PACE_CAM. If the Personalisation Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication Mapping) 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/PACE_CAM (for the derivation of the new session keys after Chip Authentication Mapping), and FCS_COP.1/PACE_CAM_ENC and FCS_COP.1/PACE_CAM_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/PACE_CAM (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/PACE_CAM_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

7.4. Dependency Rationale

The dependency analysis for the SFRs is provided in the [PACE-PP] section 6.3.2 and [EAC-PP] section 6.3.2. Note that FIA_API.1/CA is the same SFR that FIA_API.1 provided in [EAC-PP].

Rationale for additional Dependency as below

SFR	Dependencies	Support of the Dependencies
FIA_AFL.1/TRANS	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/TRANS
FIA_AFL.1/ISSUER	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/ISSUER

FCS_CKM.1/PACE_CAM	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/PACE_CAM_ENC, and FCS_COP.1/PACE_CAM_MAC, Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1/DH_PACE and FCS_CKM.1/CA and FCS_CKM.1/PACE_CAM
FCS_COP.1/PACE_CAM_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/ PACE_CAM, Fulfilled by FCS_CKM.4
FCS_COP.1/PACE_CAM_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/ PACE_CAM, Fulfilled by FCS_CKM.4
FIA_UID.1/TRANS	No dependencies	n.a
FIA_UID.1/ISSUER	No dependencies	n.a
FIA_UID.1/PACE_CAM	No dependencies	n.a.
FIA_UAU.1/TRANS	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/TRANS

FIA_UAU.1/ISSUER	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/ISSUER
FIA_UAU.1/PACE_CAM	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE_CAM
FIA_UAU.4/PACE_CAM	No dependencies	n.a.
FIA_UAU.5/PACE_CAM	No dependencies	n.a.
FIA_UAU.6/PACE_CAM	No dependencies	n.a.
FIA_API.1/CA (same SFR that FIA_API.1 provided in [EAC-PP])	No dependencies	n.a.
FIA_API.1/PACE_CAM	No dependencies	n.a.
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE Fulfilled by FIA_UID.1/PACE_CAM
FMT_MTD.1/PACE_CAMPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PACE_CAMPA	FMT_SMF.1 Specification of management functionsFMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PACE_CAM_KEY_READ	FMT_SMF.1 Specification of management functionsFMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE

7.5. Security Assurance Requirement Rationale

This composite ST has a set of assurance requirements at EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 were chosen in order to meet the assurance expectations to this type of TOE which is intended to operate in open environments, where attackers can easily exploit vulnerabilities.
This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices without the need for highly specialized processes and practices. It corresponds to a white box analysis and it can be considered as a reasonable level that can be applied to an existing product line without undue expense and complexity.

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

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

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

The component AVA_VAN.5 has the following dependencies:

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

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

8. TOE summary specification

Access Control
Access Control generates a session key for secure messaging according to the appropriate security procedures. It can also perform authentication according to the life cycle of the TOE.
It ensures that at any time, sensitive data must be Invisible:
It also controls access to the life cycle according to the policy below:
In the personalization phase:
- The authorized user through the key can perform limited control TOE and can perform the personalization of the TOE.

In the operational use:
- No one should be able to change the functions and control of the TOE.
- The TOE shall ensure that the personalization data must not be modified except for migration certification by certificate chaining.

- The terminal can read user data which are prohibited.

PACE mechanism
The TSF ensures securely PACE operation. It supports GM, IM and CAM algorithms and generates session key. The standard domain parameter is basically supported for PACE. For CAM, the Personalization Agent must provide additional CAM key.

EAC mechanism
The TSF ensures securely EAC operation.
The TSF has the following TA algorithm and there is a limitation in the migration between each algorithm.
- ECDSA (SHA-224, SHA-256),
- *RSASSA-PSS* (SHA-256)

Secure Messaging
The TSF ensures the integrity, confidentiality, and authenticity.
After GM, IM with PACE and Chip Authentication, a secure channel is established.
At the end of the session, the session key disappears.

Safety management
The TSF provides the following security measures.
- Low atomic write to correct the problem when Sudden power off
- Sensors and security codes that can detect security attacks. Supports a killing mechanism for protecting the TOE when an attack is continuously detected
- Using the active shield to protect TOE against physical attacks.

Test to verify TSFs:
- The data integrity is checked before data usage
- The Security functions is checked at each power on

This section provides a detail of how the TOE satisfies all the security functional requirements:

- **FCS_CKM.1/DH-PACE Cryptographic key generation – Diffie-Hellman for PACE session keys**
  As PACE is done, a secret seed will be shared between TOE and Terminal using the mapping operations such as GM or IM.
  The TSF generates session keys using the shared secret seed which protect commands and responses exchanged between a terminal and a card.

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

  As chip authentication is done, a secret seed will be shared between TOE and Terminal using the Elliptic curve Diffie-Hellman Private Key. The TSF generates session keys using the shared secret seed which protect commands and responses exchanged between a terminal and a card.

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

  As PACE is done, a secret seed will be shared between TOE and Terminal using the CAM mapping.

  The TSF generates session keys using the shared secret seed which protect commands and responses exchanged between a terminal and a card.

- **FCS_CKM.4 Cryptographic key destruction**

  The TSF destroy session keys by overwriting them with random numbers.

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

  The TOE is capable of performing the secure messaging – encryption and decryption operation with Triple-DES CBC mode (112 bits key) or AES CBC (128,192,256 bits keys) defined in all iterations of this SFR. It also meets each standard as specified

- **FCS_COP.1/PACE_MAC Cryptographic operation – MAC**

  The TOE is capable of performing the MAC operation – generate and compare operation with Retail-MAC(CBC) mode (112 bits key) or CMAC (128,192,256 bits keys) defined in all iterations of this SFR. It also meets each standard as specified

- **FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption**

  The TOE is capable of performing the secure messaging – encryption and decryption operation with Triple-DES CBC mode (112 bits key) or AES CBC (128,192,256 bits keys) defined in all iterations of this SFR. It also meets each standard as specified

- **FCS_COP.1/CA_MAC Cryptographic operation – MAC**

  The TOE is capable of performing the MAC operation – generate and compare operation with Retail-MAC(CBC) mode (112 bits key) or CMAC (128,192,256 bits keys) defined in all iterations of this SFR. It also meets each standard as specified

- **FCS_COP.1/ PACE_CAM_ENC Cryptographic operation – Symmetric Encryption / Decryption**

  The TOE is capable of performing the secure messaging – encryption and decryption operation with AES CBC (128,192,256 bits keys) defined in all iterations of this SFR. It also meets each standard as specified

- **FCS_COP.1/ PACE_CAM_MAC Cryptographic operation – MAC**

  The TOE is capable of performing the MAC operation – generate and compare operation with CMAC (128,192,256 bits key) defined in all iterations of this SFR. It also meets each standard as specified

- **FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by travel document**

The TOE receives CVCA, DV or IS certificates and verifies their signatures prior to importing them during certificate chaining.

- **FCS_RND.1 Quality metric for random numbers**
  The TSF uses random numbers generated by underlying platform which ensures level of entropy specified in [STIC]. The TSF also execute the AIS31 statistical tests(Test Procedure A) of goodness recommended in [AIS31] on the random numbers.
  Moreover, the TOE does not use or output any random numbers in the cases that they do not pass the statistical test or RNG hardware test fails.

- **FIA_AFL.1/TRANS Authentication failure handling-Transport key authentication using**
  The TOE terminates (reset) itself if 30 times unsuccessful Transport key authentication attempts have been occurred. Since the successful authentication with the TRANSPORT KEY causes state transition of the TOE to the Initialization state, the failure counter doesn't have to be initialized. So, the TOE doesn't initialize the failure counter of the TRANSPORT key.

- **FIA_AFL.1/ISSUER Authentication failure handling-Issuer authentication using**
  The TOE terminates (reset) itself if 30 times consecutive unsuccessful Personalization Agent key authentication attempts have been occurred. Once ISSUER Authentication success, the accumulated counter is initialized by 0.

- **FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authorisation data**
  When the PACE authentication fails, the TOE returns state word which indicating PACE authentication failure, and increases its response delay by 0.1 seconds. The response delay can be increased up to 3 seconds, and if the consecutive authentication failure exceeds 30 times, the TOE still returns 3 seconds delayed response. Once PACE authentication success, the accumulated counter is initialized by 0. PACE authentication failure doesn't cause any security reset or card killing mechanism.

- **FIA_UID.1/TRANS Timing of identification**
  Since the 'Creation State' is an irreversible state which allows operations for TRANPORT key authentication, the TOE with the 'Creation State' assumes that an entity who accesses the TOE is a 'Personalization Agent' having the TRANSPORT key. So, by sending GET CHALLENGE command for ISSUER AUTHENTICATE, the user claims his identity as 'Personalization Agent' to the TOE in the 'Creation State'.

- **FIA_UID.1/ISSUER Timing of identification**
  The 'Initialization State' is an irreversible state which allows operations for issuing process, and the TOE with 'Initialization State' is transited state from the 'Creation State' by successful authentication with the TRANPORT key. So, by sending GET CHALLENGE command for the ISSUER AUTHENTICATE, the user claims his identity as 'ISSUER' to the TOE in the 'Initialization State'.

- **FIA_UID.1/PACE Timing of identification**
  The TOE must be authenticated by PACE defined in [ICAO 9303] and Chip Authentication defined in [TR-03110-1] before a user is identified. After PACE protocol, TFS provides data excluding biometric information. And after Terminal Authentication, TFS provides biometric information.

- **FIA_UID.1/PACE_CAM Timing of identification**
  The TOE must be authenticated by CAM with PACE defined in [ICAO part11] and Terminal Authentication defined in [TR-03110-1] before a user is identified. After identification, After Chip Authentication Mapping, TFS provides data excluding biometric information. And after Terminal Authentication, TFS provides biometric information.

- **FIA_UAU.1/TRANS Timing of authentication**
  The TOE must be authenticated by TRANSPORT key for transiting its state to the 'Initialization State'. After successful TRANSPORT key authentication, the TOE allows commands for the 'Initialization State'.

- **FIA_UAU.1/ISSUER Timing of authentication**
  The TOE must be authenticated by ISSUER key for allowing the commands for personalization (pre-personalization).

- **FIA_UAU.1/PACE Timing of authentication**
  The TOE must be authenticated by PACE defined in [ICAO 9303] and Chip Authentication defined in [TR-03110-1] and/or Terminal Authentication defined in [TR-03110-1] before a user is authenticated. After PACE protocol, TFS provides data excluding biometric information. And after Terminal Authentication, TFS provides biometric information.

- **FIA_UAU.1/PACE_CAM Timing of authentication**
  The TOE must be authenticated by CAM with PACE and/or Terminal Authentication defined in [TR-03110-1] before a user is authenticated. After Chip Authentication Mapping, TFS provides data excluding biometric information. And after Terminal Authentication, TFS provides biometric information.

- **FIA_UAU.4/PACE Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**
  The TSF requires using random number to establish secure channel for PACE to [ICAO 9303]. It also requires using challenge to authenticate Personalization Agent keys.

- **FIA_UAU.4/PACE_CAM Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**
  The TSF requires using random number to establish secure channel for CAM with PACE to [ICAO 9303]. It also requires using challenge to authenticate Personalization Agent keys. And it also requires using the ephemeral public key ephem – SKpcd to Terminal authentication. All of the above data are randomly generated and used only once.

- **FIA_UAU.5/PACE Multiple authentication mechanisms**
  The TSF implements Personalization Agent Authentication using Symmetric Authentication Mechanism based on AES algorithm. The TSF provides access control like PACE. And then Chip Authentication is performed, the TOE accepts commands which MAC is correctly verified by the TOE using the key agreed with a terminal. The TOE Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric information during their transmission from the TOE to the inspection system.

- **FIA_UAU.5/PACE_CAM Multiple authentication mechanisms**
  The TSF provides Chip Authentication Mapping, and then the TOE requires Terminal

Authentication to protect the confidentiality and integrity of the sensitive biometric information during their transmission from the TOE to the inspection system.

- **FIA_UAU.6/PACE Re-authenticating of Terminal by the TOE**
  After PACE, the TOE always enforces checking by secure messaging in MAC_ENC mode each command based on MAC whether it was sent by the successfully an authenticated terminal by the PACE. The does not process any commands with incorrect MAC. 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.

- **FIA_UAU.6/EAC Re-authenticating of Terminal by the TOE**
  After Chip Authentication, the TOE always enforces checking by secure messaging in MAC_ENC mode each command based on MAC whether it was sent by the successfully an authenticated terminal by the Chip Authentication. The does not process any commands with incorrect MAC. 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.

- **FIA_UAU.6/PACE_CAM Re-authenticating of Terminal by the TOE**
  After Chip Authentication Mapping, the TOE always enforces checking by secure messaging in MAC_ENC mode each command based on CMAC whether it was sent by the successfully an authenticated terminal by the Chip Authentication Mapping. The does not process any commands with incorrect CMAC. 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.

- **FIA_API.1/CA Authentication Proof of Identity**
  The TSF implements Chip Authentication protocol according to [TR-03110-1] which use private key stored in the TOE. As this private key cannot be read by an external access in any condition, proving possession of this key can be a valid proof of genuine identification.

- **FIA_API.1/PACE_CAM Authentication Proof of Identity**
  The TSF implements Chip Authentication Mapping protocol according to [ICAO part11] which use private key stored in the TOE. As this private key cannot be read by an external access in any condition, proving possession of this key can be a valid proof of genuine identification.

- **FDP_ACC.1/TRM Subset access control**
  The TSF implements the access control Policy over the EF.COM, EF.SOD, EF.DG.1 to EF.DG.16 of the logical MRTD, applying the rules and operations over objects defined in FDP_ACF.1

- **FDP_ACF.1/TRM Security attribute based access control**
  The TSF implements Personalization Agent Authentication using Symmetric Authentication Mechanism based on 3DES algorithm or AES algorithm and the authentication is required for personalization. The TSF allows reading DG3 and DG4 only if a terminal has been successfully authenticated by Terminal Authentication and proves that it has enough effective access right to read those sensitive data during certificate chaining. Also, the TSF does not grant the CVCA and DV extend

access to the sensitive data.

- **FDP_RIP.1 Subset residual information protection**
  After closing secure messaging session, the TSF injects a random value into the session key. And the TSF Initialize ephemeral private key to zero, when a shared secret K is created.

- **FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD**
  The TSF implements PACE according to [ICAO part11], and Extended Access Control mechanism according to [TR-03110-1], which enforces MAC_ENC mode to protect user data from unauthorised disclosure.

- **FDP_UIT.1/TRM Data exchange integrity**
  The TSF implements PACE according to [ICAO part11] and Extended Access Control mechanism according to [TR-03110-1], which enforces MAC_ENC mode to protect user data from modification, deletion, insertion and replay errors. Also The TOE does not process a received command if it detects that modification, deletion, insertion or replay has occurred on the command by verifying MAC and by checking presence of essential tags of secure messaging.

- **FTP_ITC.1/PACE Inter-TSF trusted channel after PACE**
  The trusted channel is established after successful performing the PACE protocol and after successful performing chip authentication. If the channel is successfully created, secure messaging is immediately started using the derived session keys. The TOE is capable of performing the secure messaging – encryption and decryption operation with Triple-DES CBC mode (112 bits key) or AES CBC mode (128,192,256 bits keys) as described in [ICAO SAC]

- **FAU_SAS.1 Audit storage**
  IC Manufacturer writes IC Serial Number during IC manufacturing process. MTRD Manufacturer does not deal with any Pre-personalization data.

- **FMT_SMF.1 Specification of Management Functions**
  The TOE requires Transport Key authentication to initializes (activate) itself. The TOE provides functionality to write Personalization Agent keys (Pre-personalization) after default Personalization Agent keys have been authenticated.
  After Personalization Agent key authentication, the TOE allows to write user data using UPDATE BINARY commands (Personalization).
  For Configuration, the TSF provide command for Manage the configuration of the TOE. This command can be used to set contactless type A config or to perform start-up self test on / off.

- **FMT_SMR.1/PACE Security roles**
  The TSF defines roles of Personalization Agent, Country Verifying Certification Authority, Document Verifier, and Extended Inspection System as specified in [EAC-PP] and associates users with each of those roles.
  The TSF associates a user with role of Personalization Agent, Country Verifying Certification Authority, Document Verifier, and Extended Inspection System by authenticating following keys.
    - Manufacturer: None.
    - Personalization Agent: Personalization Agents keys.
    - Country Verifying Certification Authority : CVCA private key
    - Document Verifier : DV private key
    - domestic Extended Inspection System : IS private key

- foreign Extended Inspection System : IS private key

Manufacturer does not have to be authenticated by key because it does not deal with any sensitive user data. Also the TOE is protected by Transport key before being delivered to Personalization Agent.

- **FMT_LIM.1 Limited capabilities**

  The TSF provides limited capabilities through LDS system and security code.
  The TSF does not have test features after TOE Delivery.

- **FMT_LIM.2 Limited availability**

  The TSF provides limited availability through LDS system and security code.
  The TSF does not have test features after TOE Delivery.

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

  When TOE is delivered from MRTD manufacturer to Personalization Agent, it is protected by Transport Key. After Transport Key authentication, the TSF explicitly requires to identify Personalization Agent itself by authenticating default Personalization Agent keys.
  The TSF allows changing the default Personalization Agent keys to customer's keys only if the default Personalization Agent keys have been successfully authenticated

- **FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data**

  Personalization Agent is able to transfer card life-cycle state from INITIALISATION state to OPERATION state by sending SET LIFECYCLE command. SET LIFECYCLE is a dedicated command to manage card life cycle and it is only allowed to an entity that has been identified as Personalization Agent.
  During "Operational Use" of the TOE, it is not allowed to read IC serial number if Personalization Agent keys are not successfully authenticated.

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

  The TSF does not provide functionality to read Personalization Agent keys to anyone in any life-cycle states, because it is not possible to read the files that store the keys. Also, the PACE keys the Chip Authentication Private Key are generated by Personalization Agent and are stored in a hidden file which encrypts its contents and checks the integrity of the contents whenever it is used.

- **FMT_MTD.1/PACE_CAM_KEY_READ Management of TSF data – Key Read**

  Chip Authentication Mapping keys are generated by Personalization Agent and are stored in a hidden file which encrypts its contents and checks the integrity of the contents whenever it is used.

- **FMT_MTD.1/PA Management of TSF data – Personalisation Agent**

  During INITIALISATION state, SOD written by a Personalization Agent using UPDATE BINARY command. After completion of personalization, the TOE does not support functionality to write SOD again.

- **FMT_MTD.1/ PACE_CAMPA Management of TSF data – Personalisation Agent**

  During INITIALISATION state, CardSecurity written by a Personalization Agent using UPDATE BINARY command. After completion of personalization, the TOE does not support functionality to write CardSecurity again.

- **FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA**

Certificate and Current Date

During INITIALISATION state, the initial CVCA Public Key, initial CVCA Certificate and initial Current Date are written by a Personalization Agent using UPDATE BINARY command. After completion of personalization, the TOE does not support functionality to write the initial CVCA Public Key, initial CVCA Certificate or initial Current Date again.

- **FMT_MTD.1/ CVCA_UPD Management of TSF data – Country Verifying Certification Authority**

  During INITIALISATION state, the initial CVCA Public Key and the initial CVCA Certificate are written by a Personalization Agent, using UPDATE BINARY command. After completion of personalization, the TOE does not support functionality of updating the initial CVCA Public Key and initial CVCA Certificate again.

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

  In OPERATION state, the TSF updates its Current Date if and only if CVCA, DV or IS certificate are verified to be signed with a valid private key during certificate chaining.

- **FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key**

  During INITIALISATION state, the Chip Authentication Private Key is written by a Personalization Agent using UPDATE BINARY command. After completion of personalization, the TOE does not support functionality to read or write the Chip Authentication Private Key.

- **FMT_MTD.1/PACE_CAMPK Management of TSF data – Chip Authentication Private Key for CAM**

  During INITIALISATION state, the Chip Authentication Private Key for CAM is written by a Personalization Agent using UPDATE BINARY command.

- **FMT_MTD.3 Secure TSF data**

  The TSF allows importing a new CVCA certificate if and only if the imported certificate is correctly verified using the current CVCA public key stored in MRTD.

- **FPT_EMS.1 TOE Emanation**

  The IC is designed to avoid disclosing of Personalization Agent Key(s), All Session key(s) and All Authentication private key(s) by means of electromagnetic emanations. Moreover the OS provides measures to balance conditions and variables in critical operations generating same consumption that it is reflected in electromagnetic emanations. Moreover the OS introduces noise when critical data is handled.

- **FPT_FLS.1 Failure with preservation of secure state**

  When the TOE is exposed to out-of-range operating conditions such as extreme temperature, intensive light or abnormal voltage etc., the IC triggers sensor reset and the TSF increases a security counter. When the security counter reaches a specific number, the TOE destroys itself.

  If the TSF detects that one of the self-test fails, it responses a status word to inform which self-test has been failed and reset itself.

- **FPT_TST.1 TSF testing**

  Verification of TSF executable code integrity stored in NVM is done by IC manufacturer during FLASH masking process. Also IC triggers sensor reset automatically when it detects parity error.

The TSF executes self-test (DES, AES, RSA, CRC) of crypto co-processor once after each start-up. Also Random Number Generator is tested (1) each time random numbers are generated before using it, (2) after cryptographic operations are done.

- **FPT_PHP.3 Resistance to physical attack**

  The IC chip has several security detector that detect whether such abnormal condition occur.

  - Voltage detector
  - Frequency detector
  - Active Shield Removal Detector
  - Light and laser detector
  - Temperature detector
  - Voltage Glitch detector

9. Acronyms

BIS	Basic Inspection System
CC	Common Criteria
EAL	Evaluation Assurance Level
EF	Elementary File
EIS	Extended Inspection System
GIS	General Inspection System
ICAO	International Civil Aviation Organization
IT	Information Technology
MRTD	Machine Readable Travel Document
OSP	Organizational security policy
PP	Protection Profile
RNG	Random Number Generator
SAR	Security assurance requirements
SFP	Security Function Policy
SFR	Security functional requirement
ST	Security Target
TOE	Target of evaluation
TSF	TOE Security Functions
PA	Passive Authentication
AA	Active Authentication
BAC	Basic Access Control
EAC	Extended Access Control
PACE	Password Authenticated Connection Establishment
CAM	Chip Authentication Mapping
CA	Chip Authentication
TA	Terminal Authentication
CAN	Card Access Number
SOD	Security object Data
MRZ	Machine readable Zone

10. Bibliography

[BAC-PP]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, Version 1.10, 25th March 2009
[PACE-PP]	Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE-PP) version 1.01, 22th July 2014.
[EAC-PP]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC-PP) version 1.3.2, 5th December 2012
[ICAO 9303]	Doc Series, ICAO Doc 9303, Machine Readable Travel Documents, seventh Edition, 2015
[ICAO part11]	ICAO Doc 9303, Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs, seventh Edition, 2015
[TR-03110-1]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents -Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26. February 2015
[TR-03111]	Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 2.0, Bundesamt fur icherheit in der Informationstechnik (BSI)
[ICAO SAC]	International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010
[ICPP]	Euro smart Security IC Platform Protection Profile with augmentation packages, version 1.0, BSI-CC-PP-0084-2014
[STIC]	S3FT9MH/ S3FT9MV/ S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional specific IC Dedicated Software Version 3.2 27th March 2017
[GDOM]	Security Application Note for S3FT9MD/MC,MF/MT/MS,MH/MK/MG Version 1.9 09th June 2015
[AIS31]	A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators version 3.1 25.09.2001

[DES]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46- 3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S.DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
[FIPS 180-4]	Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2015 August
[PKCS3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PKCS1]	PKCS #1: RSA Cryptographic Standard, An RSA Laboratories Technical Note, Version 2.2, Revised October 27, 2012
[ISO15946-2]	ISO/IEC15946-2. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures, 2002
[ISO 9796-2]	ISO/IEC 9796-2, Information Technology - Security Techniques - Digital Signature Schemes giving message recovery - Part 2: Integer factorisation based mechanisms, 2010 3rd edition
[ISO 11770-3]	Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques, 2015
[AGD_OPE]	KONA2 D2320N ePassport Operational Guidance, Version 1.16
[AGD_PRE]	KONA2 D2320N ePassport Preparative Procedure Guidance, Version 1.16
[ALC_DEL]	KONA2 D2320N ePassport Delivery Procedure, Version 1.14

End of Document