Security Target Lite

for the

IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0

SAC/EAC configuration

a Product of Morpho B.V.

Filename	7301-9301-112 ASE-Lite IDeal Pass v2 - SAC-EAC JC ePassport 4.0.0 (SAC-EAC configuration) v1.0.3.doc
Document version	1.0.3 approved
Date	2013-11-28
Author	Morpho B.V
Certification ID	BSI-DSZ-CC-0866
Classification	Public release

Table of Contents

Document Revision History

Version	Date	Author	Description
1.0.0	2013-11-11	Morpho	Public release based on ASE v1.2.2
1.0.1	2013-11-12	Morpho	Synchronised with ASE v1.2.3
1.0.2	2013-11-18	Morpho	Synchronised with ASE v1.2.4
1.0.3	2013-11-28	Morpho	Synchronised with ASE v1.2.5

Distribution List

Name	v1.0.0	v1.0.1	v1.0.2	v1.0.3
TÜVIT	X	X	X	X
Morpho	X	X	X	X
BSI	X		X	X

1 ST Introduction

The aim of this document is to describe the Security Target Lite for the Machine Readable Travel Document (MRTD) with the ICAO application, Password Authenticated Connection Establishment and Extended Access Control on the NXP J3E120_MP65 (JCOP 2.4.2R3) Java Card Platform.

1.1 ST Reference

Title:	ASE-Lite IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 (SAC/EAC configuration)
Version Number:	1.0.3
Document Reference:	**7301-9301-112** ASE Lite IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 (SAC/EAC configuration)
Document type:	**ASE Lite**
CC version:	3.1 Revision 4
Provided by:	Morpho B.V
Evaluation body:	TÜV Informationstechnik GmbH (TÜViT)
Certification body:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Evaluation assurance level:	EAL5 augmented with ALC_DVS.2 and AVA_VAN.5

1.2 TOE Reference

TOE Name:	IDeal Pass v2 - SAC/EAC JC ePassport
TOE Version:	4.0.0
Developer:	Morpho B.V
TOE identification:	IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0
Certification ID:	BSI-DSZ-CC-0866
Product type / platform	Machine Readable Travel Document (MRTD) with the ICAO application, PACE and Extended Access Control on the NXP J3E120_MP65 (JCOP 2.4.2R3) Secure Smart Card Controller (NSCIB-CC-13-37760)
TOE hardware	NXP P5CD145V0B (certificate BSI-DSZ-CC-0858-2013) and the crypto libraries in the hardware have been certified by BSI (certificate BSI-DSZ-CC-0750)

1.3 TOE Overview

The Security Target Lite (ST-Lite) defines the security objectives and requirements for a contact or contactless based chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) and EU requirements for Extended Access Control v1 with PACE.

The main features and their origin are the following:

- **Password Authenticated Connection Establishment (PACE)**
  according to ICAO Technical Report "Supplemental Access Control" [ICAO-SAC] and strictly conform to BSI-CC-PP-0068-V2 [PACE-PP] for protection of the communication between terminal and chip.
- **Chip Authentication v1**
  according to BSI TR-03110 parts 1 and 3 [TR-03110-1], [TR-03110-3] and strictly conform to BSI-CC-PP-0056-V2-2012 [EAC-PP-V2], authenticates the travel document's chip to the inspection system.
- **Terminal Authentication v1**
  according to BSI TR-03110 parts 1 and 3 [TR-03110-1], [TR-03110-3] and strictly conform to BSI-CC-PP-0056-V2-2012 [EAC-PP-V2], authenticates the inspection system to travel document's chip and protects the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system.

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

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

1.4 TOE Description

1.4.1 TOE Definition

The Target of Evaluation (TOE) addressed by the current security target is an electronic travel document representing a contactless / contact 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-9303]) and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [ICAO-9303], BSI TR-03110 part 1 [TR-03110-1] and part 3 [TR-03110-3] and Active Authentication according to [ICAO-9303]. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 [PACE-PP].

The TOE (IDeal Pass v2 - SAC/EAC JC ePassport) comprises of

- the NXP J3E120_MP65 (JCOP 2.4.2R3) Secure Smartcard Controller, comprising of

  - the circuitry of the MRTD's chip (the NXP P5CD145V0B integrated circuit, IC) with hardware for the contact and contactless interface;
  - the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software;
  - the IC Embedded Software (operating system): JCOP2.4.2R3;
- the MRTD application IDeal Pass v2 - SAC/EAC JC ePassport Applet version 1.0.59.300 loaded in ROM or in EEPROM;
- the associated guidance documentation.

For this TOE, only one application will be present on the IC, namely the ICAO MRTD Application. The TOE utilizes the evaluation of the underlying platform, which includes the NXP chip, the IC Dedicated Software and the JCOP2.4.2R3 operating system certified by the Dutch NSCIB Certification Body (NSCIB-CC-13-37760). The hardware platform NXP P5CD145V0B has been certified by BSI (BSI-DSZ-CC-0858-2013) and the crypto libraries in the hardware have been certified by BSI (BSI-DSZ-CC-0750).

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

- The MRTD's chip circuitry and the IC dedicated software forming the Smart Card Platform (Hardware Platform and Hardware Abstraction Layer);
- The IC embedded software running on the Smart Card Platform consisting of
  - Java Card virtual machine, ensuring language-level security;
  - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
  - Java card API, providing access to card's resources for the Applet;
  - Global Platform Card Manager, responsible for management of Applets on the card. For this TOE post issuance loading or deletion of Applets is not allowed;
  - Native Mifare application, for this TOE the Mifare application is disabled.
- The Applet Layer is the IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 Applet.

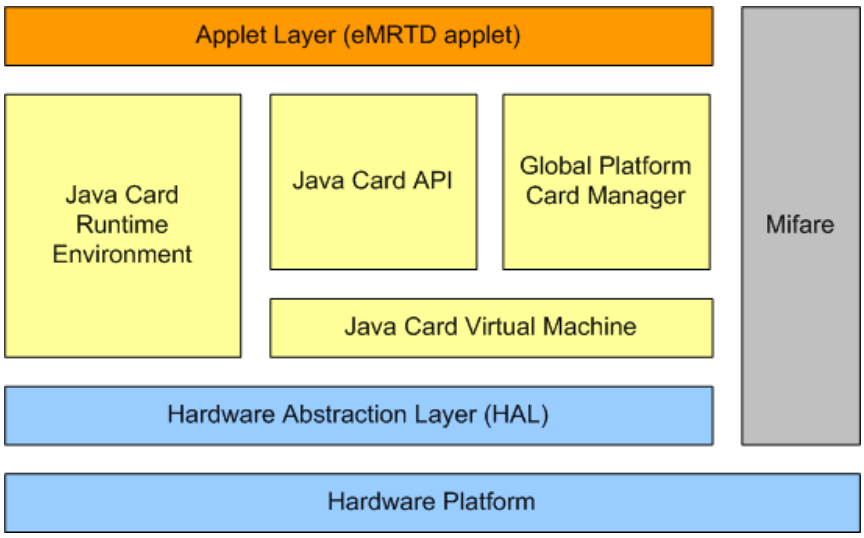


Figure 1: TOE

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

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

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

(ii) the **logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO-9303] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based or contactless readable data including(but not limited to) personal data of the travel document holder
   (a) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(b) the digitized portraits (EF.DG2),
(c) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1],
(d) the other data according to LDS (EF.DG5 to EF.DG16) and
(e) the Document Security Object (SO_D).

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

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

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

The ICAO 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 [ICAO-9303] and Password Authenticated Connection Establishment [ICAO-SAC]. 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 [TR-03110-1] as an alternative to the Active Authentication stated in [ICAO-9303] as well Active Authentication itself.

For Basic Access Control (BAC) supported by the TOE, a separate evaluation and certification is performed with ST [ST-BAC] under Certification ID BSI-DSZ-CC-0867.

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)' [PACE-PP]. Note that [PACE-PP]considers high attack potential.

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

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

(i) the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.
(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
(iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

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

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

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

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

Active Authentication may be optionally configured.

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

1.4.3 TOE life cycle

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

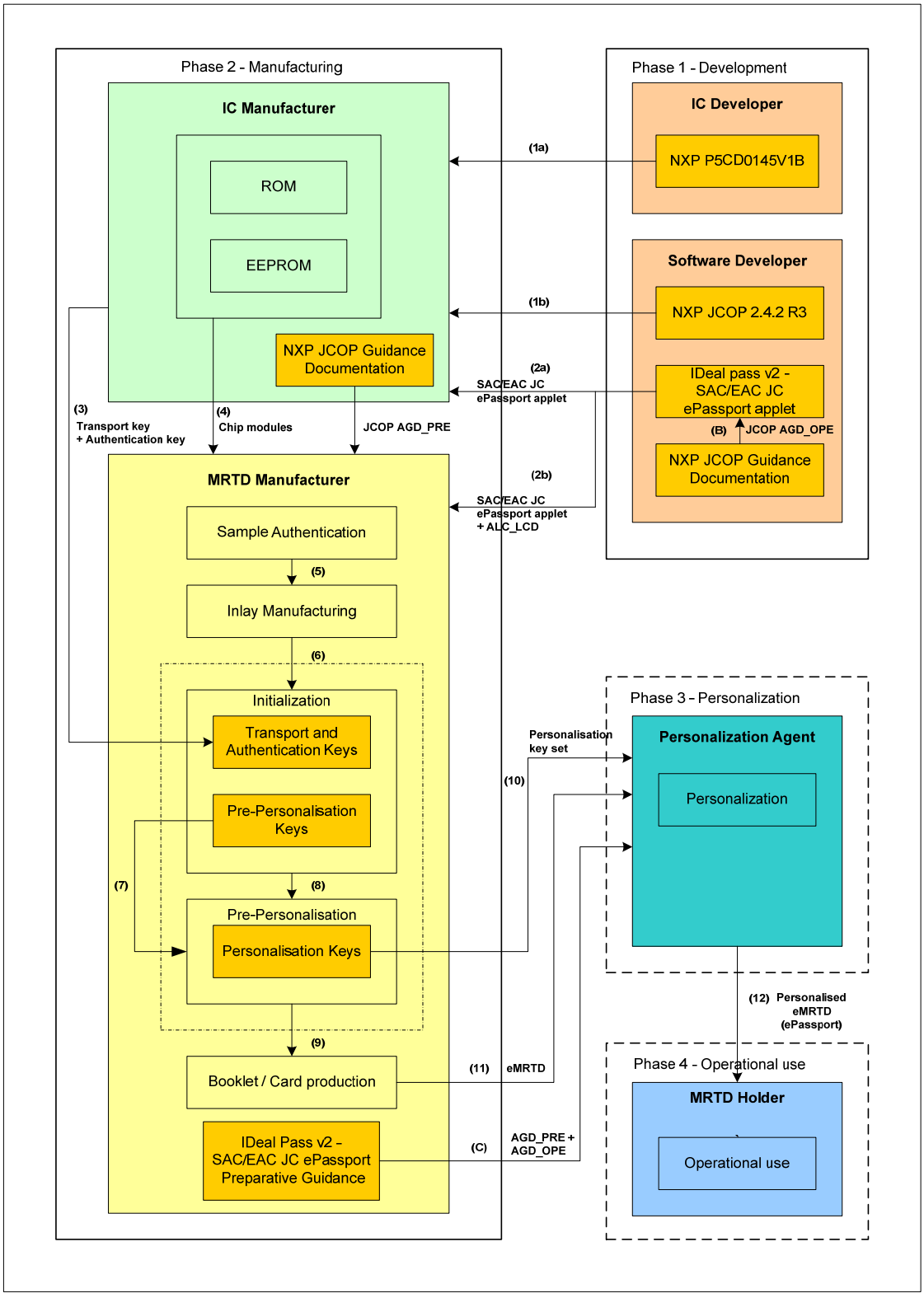


Figure 2: TOE life-cycle

1.4.3.1 Phase 1 “Development”

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components. The IC developer also acts as the developer of the IC Embedded Software (operating system) which is the JCOP v.2.4.2 Revision 3 platform.

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Embedded Software (JCOP v.2.4.2 Revision 3 operating system) and develops the ePassport application and the guidance documentation associated with this TOE component.

The ePassport application (i.e. the IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 Applet run time code) may be integrated either in ROM or in EEPROM of the chip. Depending on the intention

(a) the ePassport application is securely delivered directly from the software developer (Morpho development dept.) to the IC manufacturer (NXP). The applet code will be integrated into the ROM mask code by the IC manufacturer, or
(b) either the ePassport application and the guidance documentation is securely delivered directly from the software developer (Morpho development dept.) to the travel document manufacturer (Morpho production dept.).

1.4.3.2 Phase 2 “Manufacturing”

(Step3) In a first step the TOE integrated circuit is produced containing the travel document’s chip Dedicated Software, the parts of the travel document’s chip Embedded Software, and in case of alternative a) the ePassport application in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacturer to the travel document manufacturer.

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

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

(Step5) The travel document manufacturer

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

(ii) creates the ePassport application,
(iii) equips travel document's chips with pre-personalization Data.

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

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

- IC Dedicated SW = Low level IC libraries
- travel document's chip Embedded Software = JCOP 2.4.2 Revision 3 operating system.
- ePassport application = the IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 Applet run time code or an instantiation of it.
- Pre-personalization Data = Personalization Agent Key Set and Card Production Life Cycle (CPLC) data.

Both the underlying platform and the IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 Applet provide configuration and life-cycle management functions required for TOE preparation. TOE preparation steps are performed in manufacturing phase and consists of the following 2 activities:

1. Platform initialisation
2. Pre-personalisation

Platform initialisation
Platform initialisation consists of the configuration of the JCOP platform in accordance with requirements specified in the JCOP platform administrator guidance [JCOP-ADM] by using the dedicated platform commands. Furthermore the Pre-Personalisation Agent key set is installed and (a part of) the CPLC data is updated.

Pre-personalisation
The pre-personalisation consists of the following steps:

a. IC (chip) Authentication and getting chip access with the pre-personalisation key set.
b. [optional] In case the IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 Applet runtime code does not reside in ROM, it is loaded into EEPROM.
c. Create applet instance for IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 Applet (i.e. installation of the IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 Applet);
d. Disabling further pre-personalisation functionality;
e. Set the MRTD irreversibly in its PERSONALISATION life-cycle state by installation of the Personalisation Agent specific personalisation key set;

During step c the CPLC data with the IC Identifier is configured in the ePassport application instance. The last step (e) finalizes the TOE. This is the moment the TOE starts to exist and is ready for delivery to the Personalisation Agent. The guidance documentation for the Personalisation Agent is [AGD_PRE].

The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation to the Personalisation Agent.

1.4.3.3 Phase 3 “Personalisation of the travel document”

(Step6) The personalisation of the travel document includes
(i) the survey of the travel document holder’s biographical data,
(ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
(iii) the personalization of the visual readable data onto the physical part of the travel document,
(iv) the writing of the TOE User Data and TSF Data into the logical travel document and
(v) configuration of the TSF if necessary.

The step (iv) is performed by the Personalisation Agent and includes but is not limited to the creation of
(i) the digital MRZ data (EF.DG1),
(ii) the digitized portrait (EF.DG2), and
(iii) the Document security object.

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

EAC PP Application note 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [CC-1] §92) comprise (but are not limited to) the Personalisation Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

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

.

1.4.3.4 Phase 4 “Operational Use”

(Step7) The TOE is used as a travel document's chip by the traveler and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organisation and can be used according to the security policy of the issuing State but they can never be modified.

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

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

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

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

2 Conformance Claims

2.1 CC Conformance Claim

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

- Common Criteria for Information Technology Security Evaluation, Part 1:Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [CC-1]
- Common Criteria for Information Technology Security Evaluation, Part 2:Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [CC-2]
- Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [CC-3]

  as follows:
  - Part 2 extended
  - Part 3 conformant

The Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012 [CEM] has been taken into account.

2.2 PP Claim

This security target (ST) claims strict conformance to Protection Profile Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5th December 2012) [EAC-PP-V2].

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

2.3 Package Claim

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

2.4 PP Conformance Rationale

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

Main aspects:

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

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

- All security objectives have been taken exactly from [EAC-PP, 4] in the same wording.

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

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

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

- The application notes from [EAC-PP-V2] and [PACE-PP] are either reproduced or modified to described their realisation.

3 Security Problem Definition

3.1 Introduction

3.1.1 Assets

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

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
Primary Assets travel document			
1	user data stored on the TOE	All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [ICAO-SAC] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-SAC]).This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [BAC-PP].	Confidentiality Integrity Authenticity
2	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 defined in [ICAO-SAC] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-SAC]). User data can be received and sent (exchange ⇔{receive, send}).	Confidentiality Integrity Authenticity
3	travel document tracing data	Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.	unavailability
Secondary Assets travel document			
4	Accessibility to the TOE functions and data only to authorized subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.	Availability

5	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
6	TOE internal secret Cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
8	travel document communication establishment authorisation data	Restricted-reveal able authorization information for a human user being used for verification of the authorisation attempts as authorized user (PACE password). These data are stored in the TOE and are not to be send to it.	Confidentiality Integrity

Table 1: Primary and secondary Assets (see [PACE-PP, 3.1])

PACE PP Application note 6: Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the travel document holder which also include his sensitive (i.e. biometric) data. Hence, the general security policy defined by the current ST also secures these specific travel document holder's data as stated in the table above.

PACE PP Application note 7: Since the travel document does not support any secret travel document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.

PACE PP Application note 8: Travel document communication establishment authorisation data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorisation attempt.
The TOE secures the reference information as well as – together with the terminal connected – the verification information in the 'TOE ↔ terminal' channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be send to the TOE.

All primary assets represent User Data in the sense of the CC. The secondary assets represent TSF and TSF-data in the sense of the CC, see [PACE-PP, 3.1]. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets.

Logical travel document sensitive User Data
Sensitive biometric reference data (EF.DG3, EF.DG4)

EAC PP Application note 5: Due to interoperability reasons the 'ICAO Doc 9303' [ICAO-9303] requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC [ICAO-9303]. Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [BAC-PP]). If supported, it is therefore recommended to used PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks.

A sensitive asset is the following more general one.

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 traveler to prove his possession of a genuine travel document.

Due to strict conformance to PACE PP, this Security Target also includes all assets listed in [PACE-PP], 3.1, namely the primary assets user data stored on the TOE (object 1), user data transferred between the TOE and the terminal connected (object 2), travel document tracing data (object 3), and the secondary assets accessibility to the TOE functions and data only for authorised subjects(object 4) Genuineness of the TOE (object 5), TOE intrinsic secret cryptographic keys (object 6), TOE intrinsic non secret cryptographic material (object 7), and travel document communication establishment authorisation data (object 8).

3.1.2 Subjects and External Entities

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

External Entity No.	Subject No.	Role	Definition
1	1	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).
2	-	Travel document presenter (traveler)	A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveler' in [BAC-PP]. Please note that a travel document presenter can also be an attacker (s. below)
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document

			presenter). This entity is commensurate with 'Terminal' in [BAC-PP].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority and verifying the travel document presenter as the travel Document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.
5	-	Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [ICAO-9303]. This role is usually delegated to a Personalisation Agent.
6	-	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 (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see [ICAO-9303], 5.5.1.
7	4	Personalisation Agent	An organization acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO-9303], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303](in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [BAC-PP].
8	5	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].
9	-	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. This external entity is commensurate with 'Attacker' in BAC-PP].

Table 2: Subjects and external entities (from [PACE-PP, 3.1])

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

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

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

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 traveler and verifying its authenticity and (ii) verifying the traveler as travel document holder.

The **Extended Inspection System (EIS)** performs the Advanced Inspection Procedure (see Figure 3 below) 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.

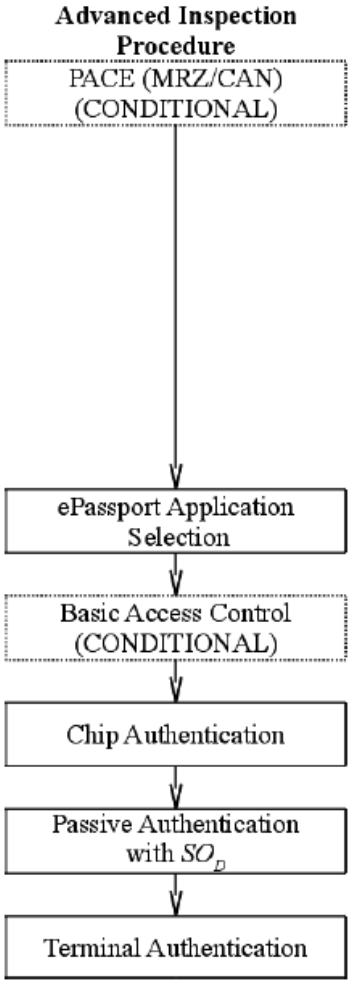


Figure 3: Advanced Inspection Procedure (Source: [EAC-PP-V2], figure 1)

EAC PP Application note 6: For definition of **Basic Inspection System (BIS)** resp. Basic Inspection System with PACE (BIS-PACE) see Table 2 above.

Attacker
Additionally to the definition in Table 2 above the definition of an attacker is refined as follows: A threat agent trying

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

(ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4),
(iii) to forge a genuine travel document, or
(iv) to trace a travel document.

EAC PP Application note 7: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged travel document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

3.2 Assumptions

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

A.Passive_Auth PKI for Passive Authentication
The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair,(ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [ICAO-9303].

A.Insp_Sys Inspection Systems for global interoperability
The Extended Inspection System (EIS) for global interoperability
includes the Country Signing CA Public Key and implements the terminal part of PACE [ICAO-SAC] and/or BAC [BAC-PP].
BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

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

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

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

This ST includes the assumption from [PACE-PP], chapter 3.4, namely A.Passive_Auth.

3.3 Threats

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

This ST includes
1. all threats from the [PACE-PP], chap 3.2, namely T.Skimming, T.Eavesdropping, T.Tracing, T.Abuse-Func, T.Information_Leakage, T.Phys-Tamper, T.Forgery and T.Malfunction,
2. all additional threats, refinements and extensions from the [EAC-PP-V2], namely T.Read_Sensitive_Data and T.Counterfeit.

The TOE in collaboration with its IT environment shall avert the threats as specified below.

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

Adverse action:	An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless/contact interface of the TOE.
Threat agent:	having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.
Asset:	confidentiality of logical travel document data.

PACE PP Application Note 10: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

PACE PP Application Note 11: MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder.

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

Adverse action:	An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.
Threat agent:	having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.
Asset:	confidentiality of logical travel document data.

PACE PP Application Note 12: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

T.Tracing Tracing travel document

Adverse action:	An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE.
Threat agent:	having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.
Asset:	privacy of the travel document holder

PACE PP Application Note 13: This Threat completely covers and extends “T.Chip-ID” from the BAC PP [BAC-PP].

PACE PP Application Note 14: A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this ST.

PACE PP Application Note 15: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document’s chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document) cannot be averted by the current TOE.

T.Forgery Forgery of Data

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

EAC PP Application note 8: T.Forgery from the PACE PP [PACE-PP] has been extended in this ST by the Extended Inspection System (EIS) additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

T.Abuse-Func Abuse of Functionality

Adverse action:	An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the travel document holder.
Threat agent:	Having high attack potential, being in possession of one or more legitimate travel documents.
Asset:	Integrity and authenticity of the travel document, availability of the functionality of the travel document.

PACE PP Application Note 16: Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage Information Leakage from travel document

Adverse action:	An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.
Threat agent:	having high attack potential
Asset:	confidentiality of User Data and TSF-data of the travel document

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

T.Phys-Tamper Physical Tampering

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

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

T.Malfunction Malfunction due to Environmental Stress

Adverse action:	An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.
Threat agent:	having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation
Asset:	integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and

	TSF-data of the travel document

PACE PP Application note 19: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

T.Read_Sensitive_Data Read the sensitive biometric reference data

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

T.Counterfeit Counterfeit of travel document chip data

Adverse action:	An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveler by possession of a travel document. The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.
Threat agent:	having high attack potential, being in possession of one or more legitimate travel documents
Asset:	authenticity of user data stored on the TOE

3.4 Organizational Security Policies

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

This ST includes

1. all OSPs from the PACE PP [PACE-PP], chapter 3.3, namely P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI, P.Manufact and P.Terminal and
2. OSPs and security rules from EAC PP [EAC PP], namely P.Sensitive_Data and P.Personalisation.

P.Manufact Manufacturing of the MRTD's chip
The Initialisation Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

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

1. The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
2. The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE
3. The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. section 1.4.3.4 above.
4. If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

P.Card_PKI PKI for Passive Authentication (issuing branch)

PACE PP Application note 20: The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1. The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (CCSCA).
2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate

(C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [ICAO-9303], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [ICAO-9303], 5.5.1.

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

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

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

1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [ICAO-9303].
2. They shall implement the terminal parts of the PACE protocol [ICAO-SAC], of the Passive Authentication [ICAO-9303] and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication(determination of the authenticity of data groups stored in the travel document, [ICAO-9303]).
5. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the PP [PACE-PP].

P.Sensitive_Data Privacy of sensitive biometric reference data
The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1[3].

[3] Should read: **Terminal Authentication** Version 1

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

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

This ST includes

1. all Security Objectives for the TOE from the PACE PP [PACE-PP], chapter 4.1, namely OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Tracing, OT.Prot_Abuse-Func, OT.Prof_Inf_Leak, OT.Prot_Phys-Tamper, OT.Identification, OT.AC_Pers and OT.Prot_Malfunction and
2. all Security Objectives for the TOE from the EAC PP [EAC-PP-V2], chapter 4.1, namely OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

4.1.1 TOE security objectives independent of TOE environment

The following TOE security objectives address the protection provided by the TOE *independent* of TOE environment.

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

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

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

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

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

OT.Prot_Inf_Leak Protection against Information Leakage
The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document
- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

PACE PP Application note 22: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Phys-Tamper Protection against Physical Tampering
The TOE must provide protection the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with high attack potential by means of
- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data) with a prior
- reverse-engineering to understand the design and its properties and functions.

OT.Prot_Malfunction Protection against Malfunctions
The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (especially electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

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

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

EAC PP Application note 9: The OT.Chip_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip.
This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [ICAO-9303] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

4.1.2 TOE security objectives involving *TOE's environment*

The following TOE security objectives address the aspects of identified threats to be countered *involving TOE's environment*.

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

OT.AC_Pers **Access Control for Personalization of logical MRTD**
The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO-9303] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

4.2 Security Objectives for the Operational Environment

This ST includes

1. all Security Objectives of the TOE environment from the PACE PP [PACE-PP], chapter 4.2, namely OE.Legislative_Compliance, OE.Passive_Auth_Sign, OE.Personalisation, OE.Terminal, and OE.Travel_Document_Holder and
2. all Security Objectives of the TOE environment from the EAC PP [EAC-PP-V2], chapter 4.2, namely OE.Auth_Key_Travel_Document, OE.Authoriz_Sens_Data, OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document, OE.Ext_Insp_Systems

4.2.1 Issuing State or Organization

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

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

OE.Auth_Key_Travel_Document Travel document Authentication Key
The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

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

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

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

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

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the PACE PP Application Note 20):

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

(i) generate a cryptographically secure CSCA Key Pair,
(ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and
(iii) publish the Certificate of the CSCA Public Key (C_{CSCA}). Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must

(i) generate a cryptographically secure Document Signing Key Pair,
(ii) ensure the secrecy of the Document Signer Private Key,
(iii) hand over the Document Signer Public Key to the CSCA for certification,
(iv) sign Document Security Objects of genuine travel documents in a secure operational environment only.

The digital signature in the Document Security Object relates to all hash values for each data group in use according to [ICAO-9303].The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO-9303]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

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

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

4.2.3 Terminal operator: Terminal's receiving branch

OE.Terminal Terminal operating
The terminal operators must operate their terminals as follows:

1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [ICAO-9303].
2.) The related terminals implement the terminal parts of the PACE protocol [ICAO-SAC], of the Passive Authentication [ICAO-SAC](by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3.) The related terminals need not to use any own credentials.
4.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [ICAO-9303]).
5.) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

PACE PP Application note 24: OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from BAC PP [BAC-PP].

4.2.4 Travel document holder Obligations

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

4.2.5 Receiving State or Organisation

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

OE.Exam_Travel_Document Examination of the physical part of the travel document
The inspection system of the receiving State or Organisation must examine the travel document presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [ICAO-SAC]and/or the Basic Access Control [ICAO-9303].Extended Inspection Systems perform additionally to these

points the Chip Authentication Protocol Version 1toverify the Authenticity of the presented travel document's chip.

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

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

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

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

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

4.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage. The objectives, threats and assumptions marked in *italic letters* are originally included from the PACE-PP [PACE-PP] which is claimed by the EAC PP [EAC-PP-V2].

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	*OT.AC_Pers*[4]	*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_Dat	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	*OE.Personalisation*	*OE.Passive_Auth_Sign*	*OE.Terminal*	*OE.Travel_Document_Holder*	*OE.Legislative_Compliance*
T.Read_Sensitive_Data	x													x			x					
T.Counterfeit		x											x		x							
T.Skimming[5]				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.Personalisation			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: Security Objective Rationale

[4] The Objectives marked *in italic letters* are included from the claimed PACE-PP [PACE-PP]. They are listed for the complete overview of the security objectives.

[5] Threats, policies and assumptions included from the claimed PACE-PP [PACE-PP] are marked *in italic letters.* They are listed for the complete overview of threats and assumptions.

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 [PACE-PP]. **OE.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 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 [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 [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.

5 Extended Components Definition

This ST uses components defined in the PACE PP [PACE-PP] and EAC PP [EAC-PP-V2], which have been defined as extensions to CC part 2 [CC-2]. In more detail this ST uses

1. all Extended Component Definitions from the PACE PP [PACE-PP], chapter 5, namely FAU_SAS, FCS_RND, FMT_LIM, FPT_EMS and
2. all Extended Component Definitions from the EAC PP [EAC-PP-V2], chapter 5, namely FIA_API.

5.1 Definition of the Family FAU_SAS

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

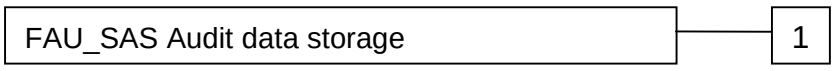
The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behaviour

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

Component leveling



FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1
	There are no management activities foreseen.
Audit:	FAU_SAS.1
	There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic keys unlike the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

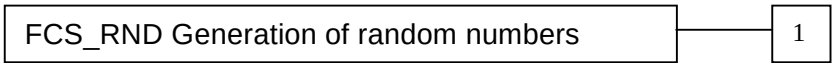
The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behaviour

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

Component leveling:



FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.
FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3 Definition of the Family FMT_LIM

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

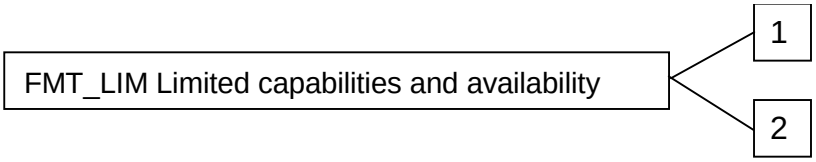
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

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

Component levelling:



FMT_LIM.1	Limited capabilities require that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.
Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: *Limited capability and availability policy*].
FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].

PP_PACE Application note 25: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

1. the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced or conversely or conversely

2. the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

5.4 Definition of the Family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electro magnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [CC-2].

The family 'TOE Emanation (FPT_EMS)' is specified as follows

FPT_EMS TOE emanation

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS.1 TOE emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No dependencies
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMS.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

5.5 Definition of the Family FIA_API

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

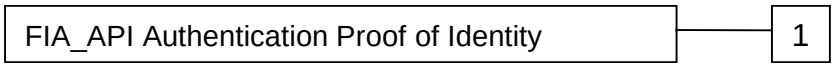
EAC PP Application note 10: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common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

FIA_API Authentication Proof of Identity

Family behavior

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

Component leveling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in

FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6 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 [CC-1]. Each of these operations is used in this security target and the underlying PP.

The **refinement** operation is used to *add* detail to a requirement, and thus further restricts a requirement. Refinement of security requirements that add or change words are 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. Selections filled in by the ST author appear as *italic and underlined text* and the original text is given by a footnote.

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. Assignments to be filled in by the ST author appear as *italic and underlined text* and the original text of the component is given by a footnote.

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”, “Personalization 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-2]. The operation “load” is synonymous to “import” used in [CC-2]

Definition of security attributes:

Security attribute	Values	Meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR-03110-1]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [TR-03110-1]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR-03110-1]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [TR-03110-1]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	-
	DG4 (Iris)	Read access to DG4: (cf. [TR-03110-1])
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR-03110-1])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [TR-03110-1])

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

Name	Data
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.

Name	Data
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} 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 (C_{CVCA})	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 (PK_{CVCA}) 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 (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (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 (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication v.1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the Issuing State or Organization signs the Document Signer Public Key Certificate(C_{DS}) with the Country Signing Certification Authority Private Key (SK_{CSCA})and the signature will be verified by Receiving State or Organization (e.g. an Extended Inspection

Name	Data
	System) with the Country Signing Certification Authority Public Key (PK_{CSCA}). The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) to be distributed by strictly secure diplomatic means, see [ICAO-9303], 5.5.1.
Document Signer Key Pairs and Certificates	The Document Signer Certificate C_{DS} is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key ($PK_{DS)}$ as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object ($SO_{D)}$ of the travel document with the Document Signer Private Key (SK_{DS}) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK_{DS})
Chip Authentication Session Key	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys (PACE-K_{MAC}, PACE-K_{Enc})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or 3DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol, see [ICAO_SAC].
PACE authentication ephemeral key pair (ephem-SK_{PICC}-PACE,ephem-PK_{PICC}-PACE)	The ephemeral PACE Authentication Key Pair {ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE } is used for Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 [TR-03111], cf. [ICAO_SAC].

Table 4: Keys and Certificates

6.1 Security Functional Requirements for the TOE

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

6.1.1 Class Cryptographic Support (FCS)

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

6.1.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1/DH_PACE	**Cryptographic key generation – Diffie-Hellman for PACE session keys**[6]
Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: fulfilled by FCS_CKM.2/DH 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 the cryptographic key generation algorithms *ECDH compliant to [TR-03111]*[7] and specified cryptographic key sizes *192, 224,256 and 320 bits in combination with 112 bits 3DES or 128, 192 or 256 bits AES*[8] that meet [ICAO-SAC] [9]

.

PACE PP Application note 26: The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO-SAC]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [RSA-PKCS#3]) or on the ECDH compliant to TR-03111 [TR-03111] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [ICAO-SAC] and [TR-03111] for details). The shared secret value K used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC},

[6] Taken from [PACE-PP]
[7] [selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [TR-03111]]
[8] [assignment: cryptographic key sizes]
[9] [assignment: list of standards]

PACE-K_{Enc}) according to [ICAO-SAC] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

PACE PP Application note 27: FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO-SAC].

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 the specified cryptographic key generation algorithm *Chip Authentication Protocol Version 1[TR-03110-1]* [10] *based on the ECDH protocol compliant to [TR-03111]* [11] with specified cryptographic key sizes *192, 224, 256, 320 bits in combination with 112 bits 3DES or 128, 192 or 256 bits AES* [12] and *based on the Diffie-Hellman protocol compliant to [RSA-PKCS#3] and [TR-03110-1]* [11] with specified cryptographic key *size of 2048 bits in combination with 112 bits 3DES or 128, 192 or 256 bits AES* [12]

EAC PP Application note 12: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO-SAC].

EAC PP Application note13: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [TR-03110-1]. This protocol may be based on the Diffie Hellman-Protocol compliant to PKCS#3 (i.e.

[10] [selection: based on the Diffie-Hellman key derivation protocol compliant to [RSA-PKCS#3] and [TR-03110-1] , based on an ECDH protocol compliant to [TR-03111]]
[11] [assignment: cryptographic key generation algorithm]
[12] [assignment: cryptographic key sizes]

modulo arithmetic based cryptographic algorithm, cf. [RSA-PKCS#3]) or on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [TR03111] for details). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [TR-03110-1]).

EAC PP Application note 14: The TOE implements keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocolv.1 uses SHA1 (cf. [TR-03110-1]). The TOE implements additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1.

FCS_CKM.4 Cryptographic key destruction – Session keys[13]

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 *physically overwriting the keys*[14] that meets the following: *none*[15].

PACE PP Application note 28: The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

EAC PP Application note 15: The TOE destroys any session keys in accordance with FCS_CKM.4 after

(i) detection of an error in a received command by verification of the MAC and

(ii) after successful run of the Chip Authentication Protocol v.1.

(iii) The TOE destroys the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys.

(iv) The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA. The TOE uses Java Card functionality for key destruction.

6.1.1.2 Cryptographic operation (FCS_COP.1)

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

[13] directly from [PACE-PP] except application note
[14] [assignment: *cryptographic key destruction method*]
[15] [assignment: *list of standards*]

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 byFCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled byFCS_CKM.1/DH_PACE
FCS_COP.1.1/ PACE_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *3DES and AES* in CBC mode and cryptographic key sizes *respectively 112 and 128, 192 and 256* bits that meet the following: compliant to [ICAO-SAC].

PACE PP Application note 29: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{Enc}).

FCS_COP.1/PACE_MAC Cryptographic operation MAC[16]

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.1/DH_PACE
FCS_COP.1.1/ PACE_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *Retail-MAC and CMAC* and cryptographic key sizes: *respectively 112 and 128, 192, 256* bit that meet the following: compliant to [ICAO-SAC].

PACE PP Application note 30: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to theFCS_CKM.1/DH_PACE (PACE-K_{MAC}).Note that in accordance with [ICAO-SAC] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

[16] Taken from [PACE-PP]

FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption[17]

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 in accordance with a specified cryptographic algorithm *3DES and AES* in CBC mode and cryptographic key sizes *respectively 112 and 128, 192 and 256* bits that meet the following *[TR-03110-1]*.

EAC PP Application note 16: This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

[17] Taken from [PACE-PP]

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
FCS_COP.1.1/ SIG_VER	The TSF shall perform digital signature verification[18] in accordance with a specified cryptographic algorithm *ECDSA*[19] with cryptographic key sizes *192, 224 and 256 bits* that meet the following: *ISO15946-2 specified in [ISO15946-2],in combination SHA1, SHA224, SHA256 digest algorithms* [20].

EAC PP Application note 17: The ST writer shall perform the missing operation of the assignments for the signature algorithms key lengths and standards implemented by the TOE for the Terminal Authentication Protocol v.1 (cf. [TR-03110-1]). The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

[18] [assignment: *list of cryptographic operations*]
[19] [assignment: *cryptographic algorithm]*
[20] [assignment: *list of standards*]

FCS_COP.1/SIG_GEN Cryptographic operation – Signature generation 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
FCS_COP.1.1/ SIG_GEN	The TSF shall perform digital signature generation[21] in accordance with a specified cryptographic algorithm *ECDSA and RSA*[22] with cryptographic key sizes *192, 224, 256 and 320 bits for ECDSA and 1536, 1792 and 2048 bits for RSA*[23] that meet the following: *ISO15946-2 specified in [ISO15946-2] for ECDSA and ISO9796-2 specified in [ISO9796-2] for RSA, in combination with SHA1, SHA224, and SHA256 digest algorithms specified in [NIST-180-4] for both ECDSA and RSA signatures*[24].

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

FCS_COP.1/CA_MAC Cryptographic operation – 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/ CA_MAC	The TSF shall perform secure messaging – message authentication code[25] in accordance with a specified cryptographic algorithm *3DES Retail-MAC and AES CMAC* [26] and cryptographic key sizes *112 bits 3DES and 128, 192 and 256 bits AES* [27] that meet the following: *[ICAO-9303] for 3DES Retail-MAC and [NIST-800-38B] for AES CMAC* [28].

[21] [assignment: *list of cryptographic operations*]
[22] [assignment: *cryptographic algorithm]*
[23] [assignment: *cryptographic key sizes*]
[24] [assignment: *list of standards*]
[25] [assignment: *list of cryptographic operations*]

EAC PP Application note18: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the authentication mechanism.

[26] [assignment: *cryptographic algorithm*]
[27] [assignment: *cryptographic key sizes*]
[28] [assignment: *list of standards*]

6.1.1.3 Random Number Generation (FCS_RND.1)

FCS_RND.1 Quality metric for random numbers[29]

Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet *Class DRG.3 of [KS2011]*[30].

PACE PP Application note 31: The TOE uses the provided platform functionality to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE.

ST Application note 1: The class DRG.3 defines requirements for deterministic RNGs. It shall not be possible to distinguish the generated random numbers from output sequences from an ideal RNG by statistical tests, and the generated random numbers sequence shall have at least some minimum amount of Min-entropy (contained in the seed), and enhanced backward secrecy is ensured. The class DRG.3 includes the requirements of class DRG.2.

While (DRG.2.2) and (DRG.2.3) require forward and backward secrecy (i.e., unknown output value cannot be determined from known output values), the security capabilities (DRG.3.2) and (DRG.3.3) additionally require enhanced backward secrecy. This means that previous output values cannot even be determined with knowledge of the current internal state and current and future output values. Enhanced backward secrecy might be relevant, for instance, for software implementations of a DRNG when the internal state has been compromised while all random numbers generated in the past shall remain secret (e.g., cryptographic keys).

The requirements to a deterministic random generator of class DRG.3 are (see [KS2011], ch. 4.8):

(DRG.3.1)If initialized with a random seed [selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]], the internal

[29] Taken from [PACE-PP]
[30] [assignment: a defined quality metric]

state of the RNG shall [selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]].

(DRG.3.2) The RNG provides forward secrecy.

(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.

(DRG.3.4) The RNG, initialized with a random seed [assignment: requirements for seeding], generates output for which [assignment: number of strings] strings of bit length 128 are mutually different with probability [assignment: probability].

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A [assignment: additional test suites].

The platform provides a deterministic random number generator which provides random numbers which meet class DRG.3 of [KS2011]. It is initialised with a random seed using the certified TRNG of the underlying Hardware platform to Seed. The internal state of the RNG has at least 100 bit MIN entropy. The RNG provides forward secrecy. Enhanced backward secrecy is ensured. The random numbers have passed test procedure A. The RNG provides forward secrecy and enhanced backward secrecy. Initialized with a random seed - initialization is initiated at start-up when the first APDU is received using the PTRNG of the HW platform conform to class P2 in [AIS31] - generates output for which 2^{35} strings of bit length 128 are mutually different with probability above $1-2^{-37}$.

The predefined class DRG.3 of [KS2011] complies with class K4 of the former definitions of [AIS20V1] (see [KS2011, 4.1 / 4.8]).

6.1.2 Class FIA Identification and Authentication

EAC PP Application note 19: The following table provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes
Authentication Mechanism for Personalisation Agents	FIA_UAU.5/PACE FIA_UAU.4/PACE FIA_UAU.1/PACE	3DES with 112 bit keys AES-128 bits AES-192 bits AES-256 bits
Chip Authentication Protocol v.1	FIA_API.1/CA FIA_UAU.5/PACE, FIA_UAU.6/EAC	ECDH and DH PKCS#3 with - 3DES Retail-MAC, 112 bit keys and - AES-CMAC with 128, 192 and 256 bits
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE	ECDSA with SHA1 ECDSA with SHA224 ECDSA with SHA256
PACE protocol[31]	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE	as required by FCS_CKM.1/DH_PACE
Passive Authentication	FIA_UAU.5/PACE	no related cryptographic operations by the TOE
Active Authentication	FIA_API.1/AA	RSA: 1536, 1792 and 2048 bits in combination with SHA1, SHA224 and SHA256 ECDSA: 192, 224, 256 and 320 bits in combination with SHA1, SHA224 and SHA256

Table 5: Overview on authentication SFR

Note the Chip Authentication Protocol Version1 as defined in this Security Target includes

- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the

[31] Only listed for information purposes.

terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authorisation data[32]

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled byFIA_UAU.1/PACE
FIA_AFL.1.1/ PACE	The TSF shall detect when *three*[33]unsuccessful authentication attempts occur related to authentication attempts using the PACE password as shared password.[34]
FIA_AFL.1.2/ PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall *wait an administrator configurable time, with a minimum of 1 second, before the next authentication attempt can be performed*[35]*.*

PACE PP Application note 32: The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [ICAO-SAC]) or for an arbitrary subset of them or may also separately be defined for each datum in question.
Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy, the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the current PP.
One of some opportunities for performing this operation might be 'consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords'.

[32] Taken from [PAC-PP]
[33] [assignment: *positive integer number*]
[34] [assignment: *list of authentication events*]
[35] [assignment: *list of actions*]

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

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 Initialisation Data if it is not disabled by TSF, according to FMT_MTD.1/INI_DIS, 4. to carry out the Chip Authentication Protocol v.1 according to [TR-03110-1], 5. to carry out the Terminal Authentication Protocol v.1] according to [TR-03110-1], 6. *None* [36] 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.

EAC PP Application note 20: The SFR FIA_UID.1/PACE in the current PP covers the definition in PACE PP [PACE-PP] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP. mediate

EAC PP Application note 21: In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC. The travel document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 “Personalisation of the travel document”. The users in role Personalisation Agent identify themselves by means of selecting the authentication key. After personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i)

[36][assignment: *list of TSF-mediated actions*]

Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

EAC PP Application note 23: In the life-cycle phase ‘Manufacturing’ the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC. Please note that a Personalisation Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role ‘Personalisation Agent’, when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

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

FIA_UAU.1/PACE Timing of identification

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-SAC], 3. to read the Initialisation Data if it is not disabled by TSF, according to FMT_MTD.1/INI_DIS, 4. to identify themselves by selection of the authentication key 5. to carry out the Chip Authentication Protocol v.1 according to [TR-03110-1], 6. to carry out the Terminal Authentication Protocol v.1] according to [TR-03110-1], 7. to carry out Personalisation Agent Authentication based on a symmetric mechanism according to [ICA0-9303] for 3DES and [ISO18013-3] for AES-128, -192 and 256 8. *None*[37] on behalf of the user to be performed before the user is identified.
FIA_UAU.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.

EAC PP Application note 24: The SFR FIA_UAU.1/PACE. in the current PP covers the definition in PACE PP [PACE-PP] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.

EAC PP Application note 25: The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE).If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

[37][*assignment: list of TSF-mediated actions*]

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:	FIA_UID.1 Timing of identification
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 *Triple-DES and AES*[38] 3. Terminal Authentication Protocol Version 1 according to [TR-03110-1]

Application note 26: The SFR FIA_UAU.4.1 in the current ST covers the definition in PACE PP [PACE-PP] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [PACE-PP].

Application note 27: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (Common Criteria Part 2).

[38] [selection: *Triple-DES, AES or other approved algorithms*]

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 *Triple-DES and AES* [39] 5. Terminal Authentication Protocol Version 1 according to [TR-03110-1] to support user authentication.

[39] [selection: *Triple-DES, AES or other approved algorithms*]

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

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.

2. The TOE accepts the authentication attempt from the Personalisation Agent by means of either
the ICAO BAC authentication mechanism and secure messaging protocol defined in [ICAO-9303] for 112 bits 3DES

   or

   ISO18013 BAP authentication mechanism defined in [ISO18013-3] for AES-128, 192 or 256 bits using AES secure messaging (CMAC, IV value, tags) as specified in EAC TR-03110 [TR-03110-1] [40]

3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.

4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1

5. *None*[41]

EAC PP Application note28: The SFR FIA_UAU.5.1/PACE in the current PP covers the definition in PACE PP [PACE-PP] and extends it by EAC aspect 5). The SFR FIA_UAU.5.2/PACE in the current ST covers the definition in PACE PP [PACE-PP] and extends it by EAC aspects 2), 3), 4)and 5). These extensions do not conflict with the strict conformance to PACE PP.

[40] [assignment: *identified authentication mechanism(s)*]
[41] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

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

FIA_UAU.6/EAC Re-authenticating – 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.[42]

EAC PP Application note 29: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO-9303] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). 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.

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

FIA_UAU.6/PACE Re-authenticating – 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.[43]

PACE PP Application note 37: The PACE protocol specified in [ICAO-SAC] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

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

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

FIA_API.1/CA Authentication Proof of Identity - MRTD

Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_API.1.1/CA	The TSF shall provide a Chip Authentication Protocol Version 1 according to [TR-03110-1][44] to prove the identity of the TOE.[45]

EAC PP Application note 30: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [TR-03110-1]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO-9303]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AA Authentication Proof of Identity - MRTD

Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_API.1.1/AA	The TSF shall provide an Active Authentication Protocol according to [ICAO-9303][46] to prove the identity of the TOE.[47]

[44] [assignment: *authentication mechanism*]
[45] [assignment: *authorized user or role*]
[46] [assignment: *authentication mechanism*]
[47] [assignment: *authorized user or role*]

6.1.3 Class FDP User Data Protection

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.1.1/ TRM	The TSF shall enforce the Access Control SFP[48] on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document [49]

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

[48] [assignment: *access control SFP*]
[49] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

FDP_ACF.1.1/TRM Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control
FDP_ACF.1.1/ TRM	The TSF shall enforce the Access Control SFP [50] 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[51], 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[52]
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.[53]
FDP_ACF.1.3/ TRM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[54]

[50] [assignment: *access control SFP*]
[51] e.g. Chip Authentication Version 1 and ephemeral keys
[52] [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*]
[53] [assignment*: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[54] [assignment*: rules, based on security attributes, that explicitly authorise access of subjects to objects*]

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.[55]

EAC PP Application note 32: The SFR FDP_ACF.1.1/TRM in the current ST covers the definition in PACE PP [PACE-PP] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in the current ST cover the definition in PACE PP. The SFR FDP_ACF.1.4/TRM in the current ST covers the definition in PACE PP and extends it by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP.

EAC PP Application note 33: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [TR-03110-1]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

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

EAC PP Application note 34: Please note that the Document Security Object (SO_D) stored in EF.SOD (see [ICAO-9303]) does not belong to the user data, but to the TSF data. The document Security Object can be read out by Inspection Systems using PACE, see [ICAO-SAC].

EAC PP Application note 35: FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment and the Chip AuthenticationProtocolv.1establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

PACE PP Application note 41: Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.

FDP_RIP.1 Subset residual information protection[56]

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 *de-allocation of the resource from* the following objects: 1. Session Keys (immediately after closing related communication session) 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K)[57] 3. *None*[58]

PP PACE Application note 42: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's

[56] Taken from [PACE-PP]
[57] according to [ICAO-SAC]
[58] [assignment: *list of objects*]

destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

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[59]

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 byFDP_ACC.1/TRM
FDP_UCT.1.1/ TRM	The TSF shall enforce the Access Control SFP[60] to be able to transmit and receive[61] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/TRM Data exchange integrity[62]

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[63] to be able to transmit and receive[64] user data in a manner protected from modification, deletion, insertion and replay errors
FDP_UIT.1.2/ TRM	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[65] has occurred.

[59] taken from [PACE-PP]
[60] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[61] [selection: *transmit, receive*]
[62] taken from [PACE-PP]
[63] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[64] [selection: *transmit, receive*]
[65] [selection: *modification, deletion, insertion, replay*]

6.1.4 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE Inter-TSF trusted channel after PACE[66]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/ PACE	The TSF shall provide a communication channel between it self 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.[67]

PACE PP Application note 43: The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word “initiate” is changed to ‘enforce”, as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

PACE PP Application note 44: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}): this secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENCand FCS_COP.1/PACE_MAC.

The establishing phase of the PACE trusted channel does not enable tracing due to the requirementsFIA_AFL.1/PACE.

PACE PP Application note 45: Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

[66] Taken from [PACE-PP]
[67] [assignment: *list of functions for which a trusted channel is required*]

6.1.5 Class FAU Security Audit

FAU_SAS.1 Audit storage[68]

Hierarchical to:	No other components.
Dependencies:	No dependencies
FAU_SAS.1.1	The TSF shall provide the Manufacturer[69] with the capability to store the Initialisation and Pre-Personalisation Data[70] in the audit records.

PP PACE Application note 46: The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE.
The audit records are usually write-only-once data of the travel document (seeFMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.1.6 Class FMT Security Management

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

FMT_SMF.1 Specification of Management Functions[71]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1	The TSF shall be capable of performing the following management functions: 1. Initialization 2. Pre-personalisation 3. Personalisation 4. Configuration[72]

[68] Taken from [PACE-PP]
[69] [assignment: *authorised users*]
[70] [assignment: *list of audit information*]
[71] Taken from [PACE-PP]
[72] [assignment: *list of management functions to be provided by the TSF*]

EAC PP Application note 36: The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data.

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below.

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 [73]
FMT_SMR.1.2/ PACE	The TSF shall be able to associate users with roles.

EAC PP Application note 37: The SFR FMT_SMR.1.1/PACE in the current ST covers the definition in PACE PP [PACE-PP] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

EAC PP Application note 38: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

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

[73] [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.[74]

The TOE shall meet the requirement "Limited capabilities (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 capability (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. [75]

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

EAC PP Application note 39: The formulation of “Deploying Test Features …” in FMT_LIM.2.1might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination ofFMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.

Note that the term “software” in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

EAC PP Application note 40: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

The TOE shall meet the requirement “Management of TSF data (FMT_MTD.1)” as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data – Writing Initialisation and Pre-personalisation Data[76]

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled byFMT_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 [77]the Initialisation Data and Pre-personalisation Data[78] to the Manufacturer.[79]

[76] Taken from [PACE-PP]
[77] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[78] [assignment: *list of TSF data*]
[79] [assignment: *the authorised identified roles*]

FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data[80]

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 the Initialisation Data and Pre-personalisation Data to the Personalisation Agent.

PACE PP Application note 49: The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases ‘manufacturing’ and ‘issuing’, but being not needed and may be misused in the ‘operational use’. Therefore, read and use access to the Initialisation Data shall be blocked in the ‘operational use’ by the Personalisation Agent, when he switches the TOE from the life cycle phase ‘issuing’ to the life cycle phase ‘operational use’.

FMT_MTD.1/PA Personalisation Agent[81]

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 the Document Security Object (SO_D)to the Personalisation Agent.

[80] Taken from [PACE-PP]
[81] Taken from [PACE-PP]

PACE PP Application note 50: By writing SO_D into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user-and TSF- data.

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[82] the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date, 4. *none*[83] to *the Personalization Agent*[84]

EAC PP Application note 41: The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalisation phase or by the Personalisation Agent (cf. [TR-03110-1]). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

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

Hierarchical to:	No other components.

[82] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[83] [assignment: *list of TSF data*]
[84] [assignment: *the authorised identified roles*]

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[85] the 1. Country Verifying Certification Authority Public Key, 2. Country Verifying Certification Authority Certificate.[86] to Country Verifying Certification Authority [87]

EAC PP Application note 42: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [TR-03110-1]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificate (cf. FMT_MTD.3) is provided by the terminal (cf. [TR-03110-1]).

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[88] the Current date[89] to 1. Country Verifying Certification Authority, 2. Document Verifier, 3. Domestic Extended Inspection System[90].

EAC PP Application note 43: The authorized roles are identified in their certificate (cf. [TR-03110-1]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal authentication v.1 (cf. to [TR-03110-1]).

[85] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[86] [assignment: *list of TSF data*]
[87] [assignment: *the authorised identified roles*]
[88] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[89] [assignment: *list of TSF data*]
[90] [assignment: *the authorised identified roles*]

FMT_MTD.1/CAPK 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 *load* [91] the Chip Authentication Private Key[92] to *the Personalization Agent*[93].

EAC PP Application note 44: The component FMT_MTD.1/CAPK is refined by (i) selecting other operations and (ii) defining a selection for the operations “create” and “load” to be performed by the ST writer. The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb “create” means here that the Chip Authentication Private Key is generated by the TOE itself. In the latter case the ST writer shall include an appropriate instantiation of the component FCS_CKM.1/CA as SFR for this key generation. The ST writer shall perform the assignment for the authorized identified roles in the SFR component FMT_MTD.1/CAPK.

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

[91] selection: create, load]
[92] [assignment: *list of TSF data*]
[93] [assignment: the authorized identified roles]

FMT_MTD.1/AAPK Active Authentication Private Key (AA)

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to *load* [94] the *Active Authentication Private Key*[95] to *the Personalization Agent*[96].

FMT_MTD.1/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/ KEY_READ	The TSF shall restrict the ability to read[97] the 1. PACE passwords, 2. Chip Authentication Private Key, 3. Personalisation Agent Keys 4. Active Authentication Private Key [98] to none.[99]

EAC PP Application note 45: The SFR FMT_MTD.1/KEY_READ in the current ST covers the definition in PACE PP [PACE-PP] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.

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

[94] selection: create, load]
[95] [assignment: *list of TSF data*]
[96] [assignment: the authorized identified roles]
[97] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[98] [assignment: *list of TSF data*]
[99] [assignment: *the authorised identified roles*]

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 [100].

Refinement: The certificate chain is valid **if and only if**

1. the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,

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

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

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

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

EAC PP Application note 46: The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and

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

FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

6.1.7 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent by passing, deactivation and manipulation of the security features or misuse of TOE functions.

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

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 variations in power consumption or variations in timing during command execution[101] in excess of non-useful information[102] enabling access to 1. Chip Authentication Session Keys 2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}), 3. the ephemeral private key ephem SK_{PICC}-PACE, 4. Active Authentication Private Key[103], 5. Personalisation Agent Key(s), 6. Chip Authentication Private Key and 7. none.[104]

[101] [assignment: *types of emissions*]
[102] [assignment: *specified limits*]
[103] [assignment: *list of types of TSF data*]
[104] [assignment: *list of types of user data*]

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

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem SK_{PICC}-PACE,
4. Active Authentication Private Key[105],
5. Personalisation Agent Key(s),
6. Chip Authentication Private Key and
7. none.[106]

EAC PP Application note 48: The ST writer shall perform the operation in FPT_EMS.1.1 andFPT_EMS.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 [ISO7816] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

[105] [assignment: *list of types of TSF data*]
[106] [assignment: list of types of user data]

FPT_FLS.1 Failure with preservation of secure state[107]

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, *3. None*

FPT_TST.1 TSF Testing[108]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up*[109] to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.[110]
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.[111]

PACE PP Application note 52: If the travel document's chip uses state of the art smart card technology, it will run some self tests at the request of an authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the 'authorised user' Manufacturer in the life cycle phase' Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a

[107] Taken from [PACE-PP]
[108] Taken from [PACE-PP]
[109] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]
[110] [selection: [assignment: *parts of TSF*], *TSF data*]
[111] [selection: [assignment: *parts of TSF*], *TSF*]

calculation with a private key by the reverse calculation with the corresponding public key as a counter measure against Differential Failure Analysis.

FPT_PHP.3 Resistance to physical attack[112]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[113] to the TSF[114] by responding automatically such that the SFRs are always enforced.

PACE PP Application note 53: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii)countermeasures are provided at any time.

[112] Taken from [PACE-PP]
[113] [assignment: *physical tampering scenarios*]
[114] [assignment: *list of TSF devices/elements*]

6.2 Security Assurance Requirements for the TOE

The security assurance requirements (SAR) for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 5 (EAL5) augmented by the following components:

- ALC_DVS.2,
- ATE_DPT.3 and
- AVA_VAN.5.

EAC PP Application note 49: The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using the Chip Authentication Protocol v.1 (OE.Prot_Logical_Travel_Document). If the TOE is operated in non-certified mode using the BAC-established communication channel, the confidentiality of the standard data shall be protected against attackers with at least Enhanced-Basic attack potential (AVA_VAN.3).

The following table lists all SARs for the evaluation of the TOE:

Assurance class	Assurance component	Denotation
Development	ADV_ARC.1	Security architecture description
	ADV_COMP.1	Design compliance with the platform certification report, guidance and ETR_COMP
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals

Assurance class	Assurance component	Denotation
	ADV_TDS.4	Semiformal modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_COMP.1	Integration of the application into the underlying platform and Consistency check for delivery and acceptance procedures
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle statel
	ALC_TAT.2	Tools and techniques – Compliance with implementation standards
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_COMP.1	Consistency of Security Target
	ASE_ ECD.1	Extended components definition
	ASE_INT.1	Security objectives
	ASE_OBJ.2	PP claims
	ASE_REQ.2	IT security requirements
	ASE_SPD.1	Security problem definition

Assurance class	Assurance component	Denotation
	ASE_TSS.1	TOE summary specification
Tests	ATE_COMP.1	Composite product functional testing
	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Depth – Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_COMP.1	Composite product vulnerability assessment
	AVA_VAN.5	Advanced methodical vulnerability analysis

Table 1: Security Assurance Requirements

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 the assurance that the TOE is shown to be highly resistant to penetration attacks to meet the security objectives OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.

The Assurance Requirements for the selected level EAL 5 augmented are described in the Common Criteria for IT Security Evaluation documents. They are not listed in detail here.

6.3 Security Requirements Rationale

6.3.1 Functional Security Requirements Rationale

The following table provides an overview for security functional requirements coverage.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
FAU_SAS.1[115]			x				x					
FCS_CKM.1/DH_PACE				x	x	x						
FCS_CKM.1/CA[116]	x	x	x	x	x	x						
FCS_CKM.4	x		x	x	x	x						
FCS_COP.1/PACE_ENC						x						
FCS_COP.1//CA_ENC	x	x	x	x		x						
FCS_COP.1/PACE_MAC				x	x							
FCS_COP.1/CA_MAC	x	x	x	x								
FCS_COP.1/SIG_VER	x		x									
FCS_COP.1/SIG_GEN [117]		x										
FCS_RND.1	x		x	x	x	x						
FIA_AFL.1/PACE										x		
FIA_UID.1/PACE[118]	x		x	x	x	x						
FIA_UAU.1/PACE	x		x	x	x	x						
FIA_UAU.4/PACE	x		x	x	x	x						
FIA_UAU.5/PACE	x		x	x	x	x						
FIA_UAU.6/PACE				x	x	x						
FIA_UAU.6/EAC	x		x	x	x	x						
FIA_API.1/CA		x										
FIA_API.1/AA		x										
FDP_ACC.1/TRM	x		x	x		x						
FDP_ACF.1/TRM	x		x	x		x						
FDP_RIP.1				x	x	x						

[115] SFRs and security objectives from [PACE PP] are marked in italic letters.
[116] SFRs and security objectives from [EAC PP] are marked in normal letters.
[117] SFRs and security objectives introduced additionally by the ST are marked in italic and bold letters.
[118] SFRs from [PACE PP] which are extended in EAC PP are marked in bold letters.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
FDP_UCT.1/TRM	x			x		x						
FDP_UIT.1/TRM				x		x						
FMT_SMF.1		x	x	x	x	x	x					
FMT_SMR.1/PACE		x	x	x	x	x	x					
FMT_LIM.1			x					x				
FMT_LIM.2			x					x				
FMT_MTD.1/INI_ENA			x				x					
FMT_MTD.1/INI_DIS			x				x					
FMT_MTD.1/CVCA_INI	x											
FMT_MTD.1/CVCA_UPD	x											
FMT_MTD.1/DATE	x											
FMT_MTD.1/CAPK	x	x		x								
FMT_MTD.1/AAPK	x	x		x								
FMT_MTD.1/PA			x	x	x	x						
FMT_MTD.1/KEY_READ	x	x	x	x	x	x						
FMT_MTD.3	x											
FPT_EMS.1			x						x			
FPT_TST.1									x			x
FPT_FLS.1									x			x
FPT_PHP.3				x					x		x	
FTP_ITC.1/PACE				x	x	x				x		

Table 6: Coverage of Security Objective for the TOE by SFR

The security objective **OT.Identification** “Identification of the TOE” addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE’s chip. This will be ensured by TSF according to SFR FAU_SAS.1. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key set). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cycle phase ‘operational use’. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.AC_Pers** “Access Control for Personalisation of logical travel document” addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data. The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SO_D and, in generally, personalization data). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1./KEY_READ and FPT_EMS.1 restrict the access to the Personalisation Agent Keys, the Chip Authentication Private Key and the Active Authentication Private key.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE.

If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalisation Agent Keys, the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication).

If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with the Personalisation Agent Key, the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The security objective **OT.Data_Integrity** “Integrity of personal data” requires the TOE to protect the integrity of the logical travel document stored on the travel document’s chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to

write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf.FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1 and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENCand FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ requires that the Active Authentication Key cannot be written unauthorized or read afterwards.

The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself. This objective is mainly

achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).
FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords, the Chip Authentication Private Key and the Active Authentication Private Key.
FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy.
The SFR FCS_RND.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

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

The security objective **OT.Sense_Data_Conf**“ Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER.

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ requires that the Active Authentication Key cannot be written unauthorized or read afterwards.

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.Chip_Auth_Proof**“ Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Protocolv.1 provided by FIA_API.1/CA and by Active Authentication provided by FIA_API.1/AA proving the identity of the TOE. The Chip Authentication Protocolv.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocolv.1 [TR-03110-1] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging). The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The Active Authentication defined by FCS_COP.1/SIG_GEN for the generation of the RSA Signature is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ. According to FDP_ACF.1, only the successfully authenticated Inspection Systems are allowed to request active authentication (FDP_ACF.1.2, rule 2).

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

The security objective **OT.Prot_Inf_Leak** “Protection against Information Leakage” requires the TOE to protect confidential TSF data stored and/or processed in the travel document’s chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ). This objective is achieved as follows:

(i) while establishing PACE communication with CAN or MRZ (non-blocking authorization data) – by FIA_AFL.1/PACE;

(ii) for listening to PACE communication (is of importance for the current PP, since SO_D is card-individual) – FTP_ITC.1/PACE.

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

The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by

(i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and

(ii) the SFRFPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

6.3.2 Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

The table 8 shows the dependencies between the SFR and of the SFR to the SAR of the TOE.

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/CA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC, fulfilled by FCS_CKM.4 from [PACE-PP]
FCS_CKM.4 from [PACE-PP]	[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 from [PACE-PP] and FCS_CKM.1/CA
FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user	Fulfilled by FCS_CKM.1/CA,

SFR	Dependencies	Support of the Dependencies
	data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [PACE-PP]
FCS_COP.1/CA_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/CA, Fulfilled by FCS_CKM.4 from [PACE-PP]
FCS_COP.1/SIG_VER	[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/CA, Fulfilled by FCS_CKM.4 from [PACE-PP]
FCS_COP.1/SIG_GEN	[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	Fulfilled by FCS_CKM.1/CA, and Fulfilled by FCS_CKM.4 from [PACE-PP]
FIA_UID.1/PACE	No dependencies	n.a.
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	n.a.
FIA_UAU.5/PACE	No dependencies	n.a.
FIA_UAU.6/EAC	No dependencies	n.a.
FIA_API.1/CA	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1/TRM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM, justification 1 for non-satisfied dependencies
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [PACE-PP] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [PACE-PP] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [PACE-PP] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [PACE-PP] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [PACE-PP] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/ PA	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1 from [PACE-PP]

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	n.a.

Table 7: Dependencies between the SFR for the TOE

Justification for **non-satisfied dependencies** between the SFR for TOE:

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

6.3.3 Security Assurance Requirements Rationale

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

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 fulfill the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The component ALC_DVS.2 has no dependencies.

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

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

- The dependency analysis in section 6.3.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-satisfied dependencies are appropriately explained.

- All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these ‘shared’ items.

- The assurance class EAL5 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

- Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.3.2 Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specification (ASE_TSS)

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

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

- Identification and Authentication mechanisms
- Cryptographic functions support
- Access control /Storage and protection of logical travel document data
- Secure messaging
- Security and Life-cycle management

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

The following sub paragraphs shows how these security features satisfy the security functional requirements (SFRs) specified in chapter 6.1.

7.1 SF.I&A Identification and Authentication

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

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

The TOE supports the following authentication mechanisms:

1. Password Authenticated Connection Establishment (PACE)
2. EAC Chip Authentication v. 1
3. EAC Terminal Authentication Protocol v.1
4. Authentication of the Personalization Agent with a personalisation key set based on a symmetric authentication mechanism.
5. ICAO Active Authentication

SF.I&A.1 Password Authenticated Connection Establishment (PACE)
This security functionality realizes the PACE authentication mechanism as described in [ICAO-SAC] and [TR-03110-1]. In OPERATIONAL life-cycle state the TOE supports both CAN and MRZ as input parameters.

The implementation of PACE contributes to:

- FIA_AFL.1/ PACE, Authentication failure handling – PACE authentication using non-blocking authorisation data. The TOE increases the reaction time of the TOE after an unsuccessful authentication attempt with a wrong PACE passwords.
- FIA_UID.1/ PACE, Timing of identification
  The TOE allows to carry out the PACE Protocol after successful user identification
- FIA_UAU.1/ PACE, Timing of identification
  The TOE prevents reuse of authentication data related to the PACE protocol, i.e. according authentication mechanisms.
- FIA_UAU.4/PACE, Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
- FIA_UAU.5/ PACE, Multiple authentication mechanisms to support user authentication.
  The TOE provides multiple authentication mechanisms, PACE, symmetric key based authentication mechanism, etc.
- FIA_UAU.6/PACE, Re-authenticating of Terminal by the TOE
  The TOE re-authenticates the connected terminal, if a secure messaging error occurred.
- FCS_CKM.1/DH_PACE, Diffie-Hellman key generation for PACE session keys
  provided by SF.CF.6
- FCS_CKM.4, Cryptographic key destruction – Session keys
  provided by SF.CF.7
- FCS_COP.1/ PACE_ENC, Cryptographic operation – Encryption / Decryption AES / 3DES
  provided by SF.CF.1
- FCS_COP.1/ PACE_MAC, Cryptographic operation MAC/CMAC
  provided by SF.CF.1
- FDP_ACF.1/TRM, Security attribute based access control,
  provided by SF.AC
- FDP_UCT.1/TRM,Basic data exchange confidentiality – MRTD
  provided by SF.AC
- FDP_UIT.1/TRM,Data exchange integrity
  provided by SF.AC
- FDP_RIP.1, Subset residual information protection
  provided by SF.AC
- FMT_MTD.1/KEY_READ, Management of TSF data – Key Read
  protection of PACE Passwords
  provided by SF.LCM.6

SF.I&A.2 Chip Authentication v.1 of the travel document's chip The Chip Authentication v.1 protocol establishes Secure Messaging between an MRTD chip and a terminal based on a static private key stored on the MRTD chip and enables the terminal to verify that the MRTD chip is genuine. The protocol in version 1 provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys.
The implementation Chip Authentication v1. contributes to • FIA_API.1/CA, Authentication Proof of Identity – MRTD Requires to implement Chip Authentication. • FIA_UAU.6/EAC Re-authenticating of Terminal by the TOE The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user. • FMT_SMR.1, Security Roles provided by SF.LCM.2 • FMT_MTD.1/CAPK, Chip Authentication Private Key provided by SF.LCM.2 • FMT_MTD.1/KEY_READ, Management of TSF data – Key Read provided by SF.LCM.6

SF.I&A.3 Terminal Authentication v.1 for Extended Access Control Terminal Authentication v.1 protocol for Extended Access Control uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Domestic and foreign Extended Inspection Systems have the certificates (provided by the Country Verifier Certification Authority and Document Verifier) to use Terminal Authentication.
The implementation of Terminal Authentication v.1 contributes to • FIA_UAU.5/ PACE, Multiple authentication mechanisms required to provide Terminal Authentication v1 • FIA_UID.1/ PACE, Timing of identification • FMT_MTD.3 Secure TSF data • FMT_SMR.1 Security Roles • FCS_COP.1/SIG_VER (ECDSA signatures only)

SF.I&A.4 Authentication of the Personalization Agent based on a symmetric authentication mechanism

In PERSONALISATION life-cycle state the TOE enforces mutual authentication between Personalisation Agent and TOE based on either of the following symmetric key authentication mechanisms.

- ICAO BAC authentication mechanism and secure messaging protocol defined in [ICAO-9303] for 112 bits 3DES with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.
- ISO18013 BAP authentication mechanism defined in [ISO18013-3] for AES-128, 192 or 256 bits using AES secure messaging (CMAC, IV value, tags etc.) as specified in EAC TR-03110 [TR-03110-1] with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.

The Personalization Agent authenticates by two symmetric keys (MAC and ENC). The KEK key may be used for secure replacement of an existing key set.

The Personalisation Key values and as well as the secure messaging protocol are installed and configured into the TOE by the Manufacturer during pre-personalisation. In both PRE-PERSONALISATION and PERSONALISATION life-cycle state the TOE supports the reading of IC Identification data for supporting key diversification of the Personalisation Agent Key set.

The implementation contributes to

- FIA_UAU.5/PACE, Multiple authentication mechanisms,
  requires to authenticate the Personalization Agent by symmetric authentication mechanisms Triple-DES or AES which is provided by the TOE.
- FIA_UAU.4/PACE Single-use authentication of the Terminal by the TOE
- FIA_UAU.1/PACE Timing of authentication
- FMT_SMR.1 Security Roles

SF.I&A.5 Active Authentication of the MRTD's chip

This protocol provides evidence of the MRTD's chip authenticity as described in [ICAO-9303]. The TOE support Active Authentication for both RSA and ECDSA mechanisms. Active Authentication may be used by Generic, Basic and Extended Inspection Systems.

The implementation of Active Authentication contributes to

- FIA_API.1/AA Authentication Proof of Identity – MRTD
- FMT_SMR.1 Security Roles
  provided by SF.LCM.2
- FMT_MTD.1/AAPK, Active Authentication Private Key
  provided by SF.LCM.2
- FMT_MTD.1/KEY_READ, Management of TSF data – Key Read
  provided by SF.LCM.6
- FCS_COP.1/SIG_GEN, Cryptographic operation – Signature generation by travel document (RSA and ECDSA)

7.2 SF.CF Cryptographic functions support

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

SF.CF Cryptographic functions include:
1. 3DES and AES cipher operations for secure messaging
2. Digest calculations (SHA-1, SHA-224, and SHA-256)
3. Signature generation (ECDSA, RSA)
4. Signature verification (ECDSA, RSA)
5. Diffie-Hellman Key Agreement (ECDH and DH)
6. Key Generation (PACE ECDH/DH ephemeral keys and secure messaging MAC and ENC session keys)
7. Key Destruction
8. True Random Number generation

With respect to the ECC domain parameters for the elliptic curve cryptographic functions supported by the TOE in this section, the following application note is applicable.

ST Application note 2

The ECC Brainpool and NIST domain parameters are regarded cryptographically strong by the German Certification body, the Bundesamt für Sicherheit in der Informationstechnik (BSI) see [TR-02102]. The FRP256v1 have been defined by French Certification Body, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) and are also regarded as cryptographically strong, see [ANSSI-FRP256V1].

SF.CF.1 3DES and AES cipher operations for secure messaging
3DES (112 bit keys) and AES (128, 192 and 256 bit keys) are provided by the platform. The TOE uses 3DES and AES for en-/decryption (CBC and ECB) and Message Authentication Code (MAC for DES, CMAC for AES) generation and verification. The implementation of this security function contributes to: • FCS_COP.1/ PACE_ENC Cryptographic operation – Encryption / Decryption • FCS_COP.1/ PACE_MAC Cryptographic operation MAC • FCS_COP.1/ CA_ENC Cryptographic operation – Symmetric Encryption / Decryption • FCS_COP.1/ CA_MAC Cryptographic operation – Cryptographic operation MAC

SF.CF.2 Digest calculations (SHA-1, SHA-224, and SHA-256)

The platform digest functions are used by the ePassport implementations of:

- **PACE**:
  - SHA-1 is used for deriving Kπ from MRZ data according to [ICAO-SAC] and [TR-03110-1]
  - SHA-1 is used for deriving 3DES and AES-128 MAC and ENC sessions keys according to [TR-03110-3] section A.2.3.1
  - SHA-256 is used for deriving AES-192 and AES-256 MAC and ENC sessions keys according to [TR-03110-3] section A.2.3.2
- **Chip Authentication v1:**
  - SHA-1 is used for compression of DH public key according to [TR-03110-3], section A.2.2.3.
  - SHA-1 is used for deriving 3DES and AES-128 MAC and ENC sessions keys according to [TR-03110-3] section A.2.3.1
  - SHA-256 is used for deriving AES-192 and AES-256 MAC and ENC sessions keys according to [TR-03110-3] section A.2.3.2
- **Active Authentication**
  SHA-1, SHA-224 and SHA-256 are used by the TOE for the hash calculation and the creation of the ISO9796 signature format with explicit hash identifier prior to calling the platform RSA signature generation function.
- **[Basic Access Control] (not part of this ST)**[119]
  The TOE implements the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism (cf. [ICAO-9303], Volume 2, Appendix 5 to Section IV. par. A5.1).

The implementation of this security function contributes to:

- FCS_COP.1/SIG_GEN
- FCS_COP.1/SIG_VER
- FCS_CKM.1/DH_PACE
- FCS_CKM.1/CA (implicitly contains the requirements for the hashing functions used for key derivation)
- FIA_API.1/AA

[119] BAC support in the OPERATIONAL life-cycle state is not applicable within the scope of this document. This document addresses the TOE in SAC/EAC configuration only. BAC may be configured next to PACE, however Inspection systems MUST use PACE instead of BAC in order not to break the Common Criteria certification.

SF.CF.3 Signature generation (ECDSA, RSA)

Signature generation functions performed by the ePassport implementation for:

- **Active Authentication - ECDSA cf. [ISO15946-2]**:
  - Supported key sizes within the scope of this ST are 192, 224, 256 and 320 bits
  - Supported domain parameters for ECDSA in accordance with [RFC-5639], [NIST-186-3] and [ANSSI-FRP256V1]:
    - Brainpool192r1
    - Brainpool224r1
    - Brainpool256r1
    - Brainpool320r1
    - NIST P-192 (secp192r1)
    - NIST P-224 (secp224r1)
    - NIST P-256 (secp256r1)
    - ANSSI FRP256v1
  - Supported signature formats:
    - ECDSA_SHA-1
    - ECDSA_SHA-224
    - ECDSA_SHA-256
- **Active Authentication - RSA cf. [ISO9796-2]**:
  - Supported key sizes within the scope of this ST are 1536, 1792 and 2048 bits
  - Supported signature formats:
    - ISO9796 with SHA-1 (with implicit hash identifier)
    - ISO9796 with SHA-224 (with explicit hash identifier)
    - ISO9796 with SHA-256 (with explicit hash identifier)

The implementation of this security function contributes to:

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

SF.CF.4 Signature verification (ECDSA)

All signature verifications are performed by the platform. SHA-1, SHA-224 and SHA-256 hash values are calculated by platform as part of the signature verification calls made by the ePassport implementation. The TOE performs signature verification of CV certificates during Terminal Authentication v1. cf. [TR-03110-3] section A.6.4.

Signature verification functions performed by the ePassport implementation:

- **Terminal Authentication v.1 - ECDSA cf. [TR-03110-1] and [ISO 15946-2]**
  - Supported key sizes within the scope of this ST are 192, 224 and 256 bits
  - TOE supports the Brainpool [RFC-5639], NIST [NIST-186-3] and ANSSI [ANSSI-FRP256V1] defined ECC curves with cofactor =1. For a Common Criteria EAL5+ certified product only the following ECC domain parameters may be configured for ECDH during personalisation:
    - Brainpool192r1
    - Brainpool224r1
    - Brainpool256r1
    - Brainpool320r1
    - NIST P-192 (secp192r1)
    - NIST P-224 (secp224r1)
    - NIST P-256 (secp256r1)
    - ANSSI FRP256v1
  - Supported signature formats:
    - ECDSA_SHA-1
    - ECDSA_SHA-224
    - ECDSA_SHA-256

The implementation of this security function contributes to:

- FCS_COP.1/SIG_VER (ECDSA signature verification)

SF.CF.5 Diffie-Hellman Key Agreement (ECDH and DH)
Diffie-Hellman key agreement function performed by the ePassport implementation during PACE: • ECDH: Diffie-Hellman key agreement with EC over GF(p) [DH],[ISO15946-3] and [TR-03111]: o Supported key sizes within the scope of this ST are 192, 224, 256 and 320 bits o TOE supports the Brainpool [RFC-5639], NIST [NIST-186-3] and ANSSI [ANSSI-FRP256V1] defined ECC curves with cofactor =1. For a Common Criteria EAL5+ certified product only the following ECC domain parameters may be configured for ECDH during personalisation: ▪ Brainpool192r1 ▪ Brainpool224r1 ▪ Brainpool256r1 ▪ Brainpool320r1 ▪ NIST P-192 (secp192r1) ▪ NIST P-224 (secp224r1) ▪ NIST P-256 (secp256r1) ▪ ANSSI FRP256v1 Diffie-Hellman key agreement function performed by the ePassport implementation during Chip Authentication (CA): • ECDH: Diffie-Hellman key agreement with EC over GF(p) [DH],[ISO15946-3] and [TR-03111]: o Supported key sizes within the scope of this ST are 192, 224, 256 and 320 bits o TOE supports the Brainpool [RFC-5639], NIST [NIST-186-3] and ANSSI [ANSSI-FRP256V1] defined ECC curves with cofactor =1. For a Common Criteria EAL5+ certified product only the following ECC domain parameters may be configured for ECDH during personalisation: ▪ Brainpool192r1 ▪ Brainpool224r1 ▪ Brainpool256r1 ▪ Brainpool320r1 ▪ NIST P-192 (secp192r1) ▪ NIST P-224 (secp224r1) ▪ NIST P-256 (secp256r1) ▪ ANSSI FRP256v1

- DH: PKCS#3 Diffie-Hellman key agreement according to [DH], [RSA-PKCS#3]
  - Supported key size within the scope of this ST are:
    - 2048 bits

The implementation of this security function contributes to:

- FIA_API.1/CA
- FCS_CKM.1/CA
- FCS_CKM.1/DH_PACE

SF.CF.6 Cryptographic key generation
The TOE uses Java Card platform functionality for key generation. The TOE supports (on board) session key generation for the following cryptographic keys: • PACE protocol (available in TOE's OPERATIONAL and PERSONALISATION Life-cycle state) o Ephemeral ECDH during PACE protocol o MAC and ENC 3DES, AES-128, AES-192 or AES-256 bits session keys for secure messaging in MAC_ENC mode derived from the Diffie-Hellman agreed shared secret. • Chip Authentication v1 protocol o MAC and ENC 3DES, AES-128, AES-192 or AES-256 bits session keys for secure messaging in MAC_ENC mode derived from the Diffie-Hellman agreed shared secret. (available in PERSONALISATION and OPERATIONAL life-cycle state) The implementation of this security function contributes to: • FCS_CKM.1/DH_PACE Cryptographic key generation – Diffie-Hellman for PACE session keys • FCS_CKM.1/CA Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys

SF.CF.7	**Destruction of cryptographic keys**

- The TOE uses Java Card platform functionality for key destruction. A special `javacard.security` method of the JCOP platform is used. The transient keys will be reset by the JCOP platform if a deselect of the ePassport application or a reset occurs in an authenticated phase of the TOE.
- The TOE destroys all session keys in accordance with FCS_CKM.4 after
  - (i) detection of an error in a received command by verification of the MAC and
  - (ii) after successful run of the Chip Authentication Protocol v.1.
  - (iii) The TOE destroys the MAC and ENC secure messaging session keys derived by PACE after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys.
  - (iv) The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

The implementation of this security function contributes to:

- FCS_CKM.4/ Cryptographic key destruction – Session keys
- FDP_RIP.1.

SF.CF.8	**Random number generation**

The TOE uses platform for true random number generation.

- Platform function used by the ePassport implementation provides random number generation in accordance with class DRG.3 of [KS2011]

The implementation of this security function contributes to:

- FCS_RND.1/ Quality metric for random numbers

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

SF.ILTB.1	**Protection against interference, logical tampering and bypass**

Security domains are supported by the Java Card platform used by the TOE underlying platform JCOP v. 2.4.2 R3. The JCOP platform provides protection against physical attack and performs self tests as described in [JCOP-ST].

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

The IDeal Pass v2 - SAC/EAC JC ePassport Applet uses transient memory where a hardware reset always reverts the IDeal Pass v2 - SAC/EAC JC ePassport Applet into an unauthenticated state.

The implementation of this security function contributes to:

- FPT_FLS.1 Failure with preservation of secure state
- FPT_TST.1 TSF testing
- FPT_PHP.3 Resistance to physical attack

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

SF.AC.1	**Access control / Storage and protection of logical travel document data**

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

The implementation of this security function contributes to:

- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_ACC.1/TRM Subset access control
- FDP_ACF.1/TRM Security attribute based access control,
- FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD
- FDP_UIT.1/TRM Data exchange integrity
- FDP_RIP.1 Subset residual information protection

7.5 SF.SM Secure Messaging

SF.SM.1	**Secure Messaging**

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

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

The implementation of this security function contributes to::

- FTP_ITC.1/PACE: trusted channel after PACE
- FCS_COP.1/PACE_ENC: Encryption/Decryption after PACE
- FCS_COP.1/PACE_MAC: MAC generation/verification after PACE
- FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE)
- FCS_COP.1/CA_ENC Encryption/Decryption after Chip Authentication v1
- FCS_COP.1/CA_MAC MAC generation/verification after Chip Authentication v1
- FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD (ENC), after Chip Authentication v1
- FDP_UIT.1/TRM Data exchange integrity – MRTD (MAC), after Chip Authentication v1

SF.SM.2	**Secure Messaging – Re-authentication**

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

The implementation of this security function contributes to:

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

7.6 SF.LCM Security and life cycle management

SF.LCM.1 Management of phases and roles

For the IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 TOE the following life-cycle phases have been identified:

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

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

Life-cycle phase	***Role***
Manufacturing phase	**IC Manufacturer**
	MRTD Manufacturer (Platform initialisation)
	MRTD Manufacturer (Pre-personalisation)
Personalisation phase	**Personalisation Agent**
Operational phase	**Basic or Extended Inspection system**
Terminated phase	**None**

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

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

In case the TOE has detected an integrity error or perturbation attack, all MRTD functionality is permanently blocked.

The implementation of this security function contributes to:

- FMT_SMF.1 Specification of Management Functions (Initialisation part)

- FMT_SMR.1.1 Security roles (Manufacturer)
- FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialisation Data and Pre-personalization Data
- FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialisation Data and Pre-personalization Data
- FMT_MTD.1/PA

SF.LCM.2 Life Cycle states of the IDeal Pass v2 - SAC/EAC JC ePassport Applet

The TOE supports the following life-cycle states:

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

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

Life-cycle phase	***Life-cycle state (maintained by applet)***	***Role***
Manufacturing phase	**-** ***(Applet not instantiated)***	**IC Manufacturer**
	- ***(Applet not instantiated)***	**MRTD Manufacturer (Platform initialisation)**
	PRE-PERSONALISATION	**MRTD Manufacturer (Pre-personalisation)**
Personalisation phase	**PERSONALISATION**	**Personalisation Agent**
Operational phase	**OPERATIONAL**	**Basic or Extended Inspection system**
Termination phase	**TERMINATED**	**None**

The implementation of this security function contributes to:

- FMT_SMF.1 Specification of Management Functions

(Personalization and Configuration)

- FMT_SMR.1.1 Security roles
  (Personalization Agent)
- FMT_MTD.1/PA, Personalization Agent
  Ability to write the Document Security Object (SO_D)
- FMT_MTD.1/CVCA_INI Management of TSF data – Initialisation of CVCA Certificate and Current Date
- FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key Restriction of the ability to load the Chip Authentication Private Key to the Personalization Agent.
- FMT_MTD.1/AAPK Management of TSF data – Active Authentication Private Key Restriction of the ability to load the Active Authentication Private Key to the Personalization Agent.

SF.LCM.3	**Management of TSF-Data**

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

In OPERATIONAL life-cycle state the management of TSF-Data can only be performed after successful Terminal Authentication.

Updating the Country Verifier Certification Authority Public Key and Certificate is restricted to the *Country Verifier Certification Authority.* Modifying the Current Date is restricted to the *Country Verifier Certification Authority*, the *Document Verifier and* the *domestic Extended Inspection System*

The implementation of this security function contributes to:

- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles (Personalization Agent)
- FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifier Certification Authority
- FMT_MTD.3 Secure TSF data
- FMT_MTD.1/DATE Current date

SF.LCM.4	**Protection of test features**

The IDeal Pass v2 - SAC/EAC JC ePassport Applet does not have any dedicated test features implemented.

The test features of the JCOP platform are protected by ways described in JCOP ST and guidance documentation.

The platform implementation provides this security function and contributes to:

- FMT_LIM.1 Limited capabilities
- FMT_LIM.2 Limited availability

SF.LCM.5	**Protection of keys and PACE passwords**

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

In all TOE life-cycle states the Personalization Agent Key set (MAC, ENC, KEK), the PACE passwords (derived from MRZ and/or CAN), the Chip Authentication Private Key, the Active Authentication Private Key are protected from disclosure. The IDeal Pass v2 - SAC/EAC JC ePassport Applet only stores keys in Java Card specified Key structures, which are protected by JCOP platform.

The implementation of this security function contributes to:

- FMT_MTD.1/KEY_READ Management of TSF data – Key Read
- FPT_EMS.1 TOE Emanation

SF.LCM.6	**IC Identification data**

During initialisation the IDeal Pass v2 - SAC/EAC JC ePassport Applet is installed and initiated with the Pre-Personalisation Agent key and the IC Identification data.

The INSTALL for INSTALL method of the JCOP platform will be used to store the IC Identification data.

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

8 Annex

Glossary

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [TR-03110-1].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [ICAO-SAC], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SOD and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
Agreement	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [ICAO-9303]. Option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialisation Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [ICAO-9303] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
Biographical data (bio data).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa.
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.
Certificate chain	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A

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

Term	Definition
Document Basic Access Key Derivation Algorithm	The [ICAO-9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Details Data	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [ICAO-9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [ICAO-9303]
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [TR-03110-1] and [ICAO-9303]. This role is usually delegated to a Personalisation Agent.
Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [TR-03110-1]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this ST. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy) [120] [121]

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

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

Term	Definition
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO-9303]
ePassport application	[PP-SAC] definition A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [TR-03110-1]. [PP-EAC] definition Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes • the file structure implementing the LDS [ICAO-9303], • the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and • the TSF Data including the definition the authentication data but except the authentication data itself.
Extended Access Control	Security mechanism identified in [ICAO-9303] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO-9303]
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.

Term	Definition
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document.
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO-9303]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (cf. paragraph 1.4.3.2, TOE life-cycle, Phase 2 Manufacturing, Step 3).
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO-9303]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303]]
Issuing State	The Country issuing the MRTD. [ICAO-9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the MRTD's chip.

Term	Definition
Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) 1. personal data of the travel document holder 2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 3. the digitized portraits (EF.DG2), 4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5. the other data according to LDS (EF.DG5 to EF.DG16). 6. EF.COM and EF.SOD
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO-9303]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO-9303] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO-9303]
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [TR-03110-1]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.

Term	Definition
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [ICAO-SAC]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
PACE passwords	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO-SAC],
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the “Enrolment” (cf. paragraph 1.4.3.3, TOE life-cycle, Phase 3, Step 6).
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document 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 [TR-03110-1], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303] (in the role of DS). Please note that the role ‘Personalisation Agent’ may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalisation Data	A set of data incl. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.

Term	Definition
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalisation Agent.
Personalisation Agent Key	Symmetric cryptographic key or key set (MAC, ENC) used (i) by the Personalisation Agent to prove his identity and get access to the logical travel document and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE.
Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.
Pre-personalization	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (cf. paragraph 1.4.3.2, TOE life-cycle, Phase 2, Step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair and Chip Life-Cycle Production data (CPLC data).
Pre-personalised travel document's chip	Travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the MRTD holder is applying for entry. [ICAO-9303]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means [ICAO-9303].
Secure messaging in encrypted /combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.

Term	Definition
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [ICAO-SAC], namely (i) PACE or BAC and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE. Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).
Terminal Authorization	Intersection of the Certificate Holder Authorizations of the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be valid for the Current Date.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO-9303] (there "Machine readable travel document").
Travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
Travel document's Chip	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO-9303], sec III.
Traveler	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.

Term	Definition
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC-1]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialisation Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
User data	All data (being not authentication data) (i) stored in the context of the ePassport application of the travel document as defined in [5] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC-1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC-2]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO-9303]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Abbreviations

CC	Common Criteria, see [CC]
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
SEF	Security Enforcing Functions
SOF	Strength Of Function
TOE	Target of Evaluation
TSF	TOE Security Functions

References

Reference	Description
[AIS20V1]	Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 2.0, 02.12.1999
[AIS20V2]	Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitaetsklassen und Evaluationsmethodologie fuer deterministische Zufallszahlengeneratoren, Version 2.1, 02.12.2011, Bundesamt fuer Sicherheit in der Informationstechnik.
[ANSSI-FRP256V1]	Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français NOR: PRMD1123151V (Le 18 avril 2012)- ANSSI (http://www.ssi.gouv.fr/).
[BAC-PP]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1:Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2:Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
[CEM]	The Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
[DH]	Rescorla, Eric, RFC 2631: Diffie-Hellman key agreement method, 1999
[EAC-PP-V2]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012, Version 1.3.2, December 5th 2012, BSI
[ICAO-9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, Version Sixth Edition, 2006 (this includes the latest supplemental for ICAO Doc 9303 which also should be considered)
[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
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11
[ISO15946-1]	ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002
[ISO15946-2]	ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.
[ISO15946-3]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key

Reference	Description
	establishment, 2002
[ISO18013-3]	ISO/IEC 18013-3: Information technology — Personal identification — ISO-compliant driving licence. Part 3: Access control, authentication and integrity validation, 2009-03-01 Including ISO/CEI 18013-3/AC1:2011, TECHNICAL CORRIGENDUM 1, Published 2011-12-01
[ISO7816]	ISO/IEC 7816: Identification cards — Integrated circuit cards, Version Second Edition, 2008
[ISO9796-2]	ISO/IEC 9796-2: 2002, Information Technology - Security Techniques - Digital Signature Schemes giving message recovery - Part 2: Integer factorization based mechanisms
[ISO9797]	ISO/IEC 9797-1:1999, Information technology —Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.
[JAVA-3.0.1]	Application Programming Interface Java Card(tm) Platform, Version 3.0.1, Classic Edition, May 2009, Sun Microsystems, Inc.
[JCOP-ADM]	JCOP V2.4.2 Revision 3 Secure Smart Card Controller - Administrator Manual for NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, J2E082_M65, J3E081_M64, J3E081_M66, J2E081_M64, J3E081_M64_DF, J3E081_M66_DF, J3E016_M64, J3E041_M64, J3E016_M66, J3E041_M66, J3E016_M64_DF, J3E041_M64_DF, J3E016_M66_DF and J3E041_M66_DF Secure Smart Card Controller Revision 3 Rev.0.5, 16 July 2013, NXP (NSCIB-CC-13-37760)
[JCOP-ST]	Security Target JCOP2.4.2R3 NXP J3E145_M64, J3E120_M65,J3E082_M65, J2E145_M64, J2E120_M65 and J2E082_M65 Secure Smart Card Controller Revision 3 Rev. 01.01 — 25th July 2013, NXP (NSCIB-CC-13-37760)
[JCOP-UM]	JCOP V2.4.2 Revision 3 Secure Smart Card Controller - User manual for NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, J2E082_M65, J3E081_M64, J3E081_M66, J2E081_M564, J3E081_M64_DF, J3E081_M66_DF, J3E016_M64, J3E041_M64, J3E016_M66, J3E041_M66, J3E016_M64_DF, J3E041_M64_DF, J3E016_M66_DF and J3E041_M66_DF Secure Smart Card Controller Revision 3 Rev.0.6, 16 July 2013, NXP (NSCIB-CC-13-37760)
[KS2011]	A proposal for: Functionality classes for random number generators, Version 2.0, September 18, 2011 - W. Killmann, W. Schindler
[NIST-180-4]	NIST. FIPS 180-4, Secure Hash Standard, February 2011.
[NIST-186-3]	NIST. Digital Signature Standard (DSS), FIPS 186-3, 2009
[NIST-197]	NIST. Specification for the Advanced Encryption Standard (AES), FIPS PUB 197, 2001
[NIST-800-38B]	NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, 2005
[PACE-PP]	Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011, Version 1.0, 2nd November 2011, BSI
[RFC-5639]	Lochter, Manfred; Merkle, Johannes. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, 2010
[RSA-PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

Reference	Description
[SIC-PP]	Security IC Platform Protection Profile; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007, Version 1.0, June 2007 – BSI
[ST-BAC]	7301-9302-107 ASE IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 (BAC)
[TR-02102]	TR-02102 Technische Richtlinie Kryptographische Algorithmen und Schlüssellängen, Version 2013.02, January 9th 2013 by BSI
[TR-03110-1]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012 by BSI
[TR-03110-3]	TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, version 2.10, 2012-03-07 by BSI
[TR-03111]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009