Veridos Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE

Security Target Lite

NSCIB-2300087-01

Common Criteria / ISO 15408

EAL 5+

Document Version 1.8 • 2023-11-07

cv cryptovision GmbH • Munscheidstr. 14 • 45886 Gelsenkirchen • Germany
www.cryptovision.com • info@cryptovision.com • +49-209-167-2450

Content

Version Control

Version	Date	Author	Changes to Previous Version
1.7	2023-11-06	Thomas Zeggel	Security Target Lite derived from Security Target version 1.7.
1.8	2023-11-07	Thomas Zeggel	Security Target Lite derived from Security Target version 1.8.

1 Introduction

1.1 ST/TOE Identification

Title:	Veridos Suite v4.0 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE – Security Target Lite
Document Version:	v1.8
Origin:	cv cryptovision GmbH
Compliant to:	Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP) (BSI-CC-PP0056v2) [PP0056v2]
Product identification:	Veridos Suite v4.0 - cryptovision ePasslet Suite
TOE identification:	Veridos Suite v4.0 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE
Javacard OS platform:	SmartCafe Expert 8.0 C2 [ZertSmartCafe]
Security controller:	IFX SLC37GDA512 (Certificate: BSI-DSZ-CC-1107-V3-2022) [ZertIC]
TOE documentation:	Administration and user guide [Guidance_PRE], [Guidance_OPE], [Guidance_GEN]

1.2 ST overview

This document contains the security target for MRTD chips based on the MRTD-EAC application of the Veridos Suite v4.0 – cryptovision ePasslet Suite. Veridos Suite v4.0 – cryptovision ePasslet Suite is a set of Javacard applications intended to be used exclusively on the SmartCafe Expert 8.0 C2 Javacard OS platforms, which is certified according to CC EAL 6+ [ZertSmartCafe]. Veridos Suite v4.0 – cryptovision ePasslet Suite as well as the SmartCafe Expert 8.0 C2 operating system are provided on a smart card chip based on the IFX SLC37GDA512 security controller, which is itself certified according to CC EAL 6+ [ZertIC].

This Security Target defines the security objectives and requirements for the contact based / contactless smart card of machine readable travel documents based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Password Authenticated Connection Establishment, Extended Access Control, and Chip Authentication similar to the Active Authentication in ‘ICAO Doc 9303’ [ICAODoc].

This security target claims strict conformance to the Protection Profile *Machine Readable Travel Document with “ICAO Application”, Extended Access Control* with *PACE (EAC PP)* (BSI-CC-PP0056v2) [PP0056v2] and Protection Profile *Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)*, BSI-CC-PP-0068-V2-2011-MA-01 [PP0068v2].

The main objectives of this ST are:

- to introduce TOE and the MRTD application,
- to define the scope of the TOE and its security features,
- to describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- to describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.

- to specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functionalities.

The assurance level for the TOE is CC EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.[1]

1.3 TOE overview

The TOE is a Java Card (Veridos Suite v4.0 - cryptovision ePasslet Suite) configured to provide a contactless integrated circuit chip containing components for a machine readable travel document (MRTD chip). After instantiation and configuration as MRTD-EAC configuration it can be programmed amongst others according to the Logical Data Structure (LDS) defined in [ICAODoc] and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [ICAODoc] and BSI TR-03110 [TR-03110], respectively.

The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01 [PP0068v2].

1.4 TOE description

1.4.1 Overview of Veridos Suite v4.0 – cryptovision ePasslet Suite

Veridos Suite v4.0 – cryptovision ePasslet Suite is a set of Java Card applets for e-ID document applications built upon an underlying core library. The following *Table 1* provides an overview of the individual applications included in Veridos Suite v4.0 – cryptovision ePasslet Suite:

Product / Application	Specification	Configuration[2]
ICAO MRTD application with Basic Access Control (BAC) and Supplemental Access Control (SAC)	ICAO Doc 9303	ePasslet4.0/MRTD-BAC
ISO File System application	ISO 7816	ePasslet4.0/ISO-FS
ISO Driving License application with Basic Access Protection (BAP) or Supplemental Access Control (SAC)	ISO 18013	ePasslet4.0/IDL-Basic
ISO Driving License application with Extended Access Protection (EAP) or Extended Access Control (EACv1)	ISO 18013	ePasslet4.0/IDL-Extended
ICAO MRTD application with Extended Access Control (EACv1)	ICAO Doc 9303, TR03110v1.11	ePasslet4.0/MRTD-EAC
ICAO MRTD application with LDS 2	ICAO Doc 9303-10 LDS 2	ePasslet4.0/MRTD-LDS2
Secure Signature Creation Device application supporting PKI utilization	ISO 7816, PKCS#15	ePasslet4.0/SSCD
Secure Signature Creation Device application supporting PKI utilization – Device with key import	ISO 7816, PKCS#15	ePasslet4.0/SSCD-IMP

[1] In comparison to PP0056v2, which aims at assurance level EAL4 augmented, the higher evaluation assurance level EAL5 is target of this evaluation. Thus, the augmentation ATE_DPT.2 of PP0056v2 is superseded by ATE.DPT.3 of the EAL5 package.

[2] The names of the configurations reflect that the TOE is based on version 4.0 of ePasslet suite.

EU Electronic Vehicle Registration application	EU Council Directive 1999/37/EC	ePasslet4.0/eVR
German eID Document application	ICAO Doc 9303, TR03110v2.11, TR03127 v1.15	ePasslet4.0/GeID
Customizable eID Document application	ICAO Doc 09303 and TR03110v2.11	ePasslet4.0/GenID
EU Electronic Residence Permit application	TR03127 v1.15	ePasslet4.0/eRP

Table 1: Configurations of the Veridos Suite v4.0 – cryptovision ePasslet Suite. Please note that not all configurations are certified according to Common Criteria. ***The TOE of this ST is marked in yellow****.*

These configurations are based on one or more predefined applets; different configurations might use the same underlying applet.

The whole applet code resides in the Flash memory; the applets providing these different configurations are instantiated into Flash memory. Multiple configurations (and hence support for different applications) can be present at the same time by instantiating multiple applets with their distinct configurations. Such additional functionality is independent of the functionality of the TOE as described in this security target and the guidance manuals. This is ensured by the isolation properties of the Java Card platform.

A common combination could be an ICAO MRTD applet and an ePKI applet providing a travel application with LDS data and EAC authentication together with a signature application. Please note that other applications besides a MRTD applet shall not provide contactless trackable information without authentication with appropriate security level.

The following configurations are certified according to Common Criteria:

- configuration providing Machine Readable Travel Document with „ICAO Application”, Basic Access Control (BAC); this TOE is defined in a separate security target;
- configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE; this is the TOE of this security target;
- configuration providing Secure Signature Creation Device with key generation; this TOE is defined in a separate security target;
- configuration providing Secure Signature Creation Device with key import; this TOE is defined in a separate security target.

Combinations of certified and non-certified applications are possible.

Via configuration the instanciated applets can be tied to the contactless and/or the contact interface, respectively.

1.4.2 Standard build and MRTD-only build

Veridos Suite v4.0 – cryptovision ePasslet Suite is available in two different versions with different memory footprint:

- The standard build contains the full functionality to provide for the configurations listed in section 1.4.1.
- The MRTD-only build contains a redused set of functionality to provide for a part of the configurations listed in section 1.4.1, e.g. the configurations ePasslet4.0/MRTD-BAC and ePasslet4.0/MRTD-EAC.

This security target is valid for the standard build and the MRTD build.

1.4.3 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip containing components for a machine readable travel document (MRTD chip). After instantiation and configuration of the Veridos Suite v4.0 – cryptovision ePasslet Suite as MRTD-EAC configuration it can be programmed according to ICAO Technical Report "Supplemental Access Control for Machine Readable Travel Documents" [ICAO_SAC] (which means amongst others according to the Logical Data Structure (LDS) defined in [ICAODoc]) and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [ICAODoc] and BSI TR-03110 [TR-03110], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01 [PP0068v2].

The TOE consists of

- the circuitry of the chip (the integrated circuit, IC) including the contact-based interface with hardware for the contactless interface including contacts for the antenna, providing basic cryptographic functionalities,
- the platform with the Java Card operation system SmartCafe Expert 8.0 C2 by Giesecke&Devrient in the configuration 1 (compliant to the GlobalPlatform Card Common Implementation Configuration [GP_CIC], verifiable according to platform guidance [AGD_PRE], chapter 8),
- Veridos Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE,
- the associated Administrator and User Guidance [Guidance_PRE], [Guidance_OPE], [Guidance_GEN].

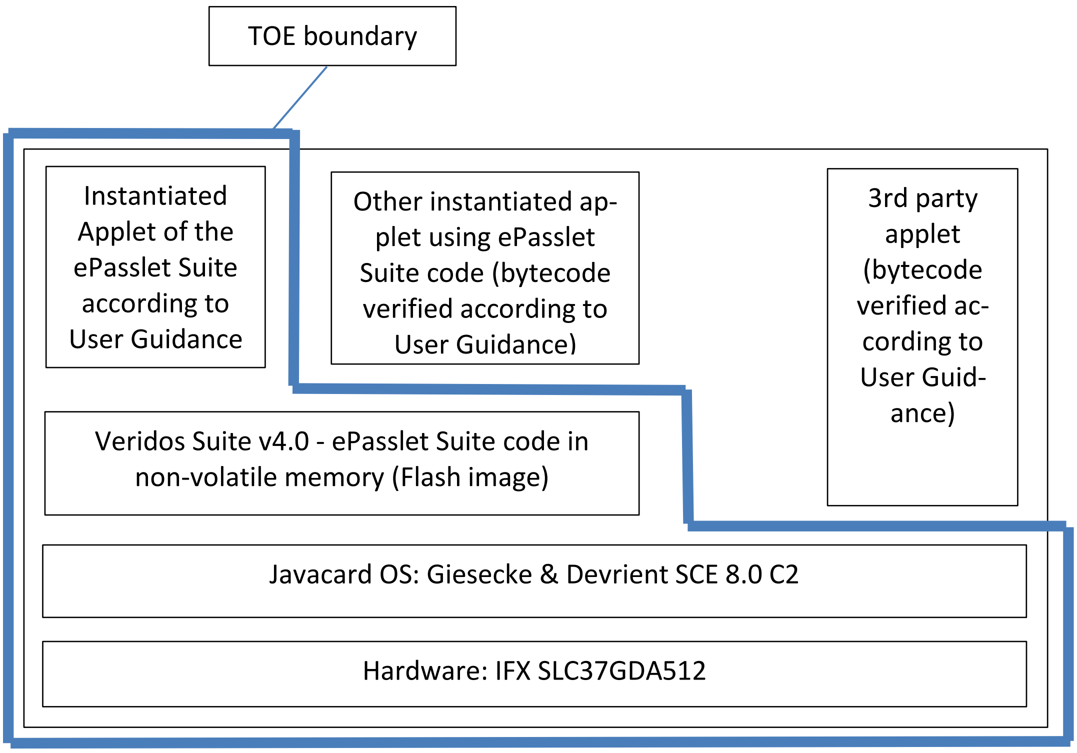

Figure 1: Schematic view on the Target of Evaluation (TOE) and its boundaries. The TOE is based on the certified hardware and Javacard OS. Besides the Veridos Suite v4.0 - ePasslet Suite code in non-volatile memory and the applet instantiated from it which forms the TOE of this security target, it may also contain additional applets which are not part of the TOE.

The TOE's functionality claimed by this Security Target is realized by the Veridos Suite v4.0 – cryptovision ePasslet Suite in the MRTD-EAC configuration only.

1.4.4 TOE identification

Identification of the platform is performed by the procedure according to [AGD_PRE].

Once the platform is identified correctly, the correct version of the Java card layer of the TOE (Veridos Suite v4.0 - cryptovision ePasslet Suite) can be verified as descibed in [Guidance_PRE].

1.4.5 TOE usage and security features for operational use

This paragraph is directly based on the corresponding paragraph in the protection profile [PP0056v2].

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

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

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

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [ICAODoc]. 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 [ICAODoc], 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] as an alternative to the Active Authentication stated in [ICAODoc].

If BAC is supported by the TOE, the travel document has to be evaluated and certified separately. This is due to the fact that [PP0055] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)' [PP0068v2]. Note that [PP0068v2] considers high attack potential.

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

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

(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.

(iii) The travel document's chip and terminal computer perform a EC-Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys K_{MAC} and K_{ENC} 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], [ICAO_SAC].

The protection profile requires the TOE to implement the Extended Access Control as defined in [TR-03110]. 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 inspectionsystem and (ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.4.6 Major security features of the TOE

The TOE provides the following TOE security functionalities:

- TSF_Access manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data.
- TSF_Admin manages the storage of manufacturing data, pre-personalization data and personalization data.
- TSF_Secret ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These mechanisms are mainly provided by TSF_OS.
- TSF_Crypto performs high level cryptographic operations. The implementation is mainly based on the Security Functionalities provided by TSF_OS. The main supported crypto mechanisms are:
  - hashing with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512,
  - Diffie-Hellman (DH) key derivation protocol compliant with PKCS#3 and TR-03110 with parameter lengths of 1024, 1280, 1536, 1984, 2048, 4096 bit, and EC-Diffie-Hellman (ECDH) key derivation protocol compliant with ISO 15946 with cryptographic key sizes of 224, 256, 320, 384, 512 and 521 bit with specific elliptic curves (domain parameters) for Chip Authentication,
  - digital signature verification with ECDSA and cryptographic key sizes of 224, 256, 320, 384, 512 and 521 bit with specified curves, and RSA and cryptographic key sizes of 1024, 1280, 1536, 1984, 2048, 4096 bitbit,
  - key generation for the optional Active Authentication in accordance with RSA and cryptographic key sizes of 1024, 1280, 1536, 1984, 2048 and 4096 bit, or ECDSA with key sizes of 224, 256, 320, 384, 512 and 521 bit,
  - digital signature generation for the optional Active Authentication in accordance with RSA and cryptographic key sizes of up to 2048 bit, or ECDSA with key sizes of 224, 256, 320, 384, 512 and 521 bit,
  - encryption and decryption with AES and cryptographic key sizes 128, 192, 256 bit,
  - encryption and decryption with 3DES and cryptographic key sizes 112 bit,
  - AES CMAC and cryptographic key sizes of 128, 192, 256 bit,
  - Retail-MAC with cryptographic key size of 112 bit (based on 3DES),
  - ECDH compliant to ISO 15946 with cryptographic key sizes of 224, 256, 320, 384, 512 and 521 bit used for PACE, and
  - PACE Authentication.
- TSF_SecureMessaging realizes a secure communication channel with MACs and encryption based on AES (128, 192 or 256 bit key length) or 3DES (112 bit).
- TSF_Auth realizes different authentication mechanisms: TSF_Auth_PACE (key lengths 224, 256, 320, 384, 512 and 521 bit), TSF_Auth_Term (Terminal Authentication), TSF_Auth_Sym with AES used for personalization and TSF_Auth_Chip to manage the capability of the TOE to authenticate itself to the terminal using the Chip Authentication Protocol.
- TSF_Integrity protects the integrity of internal applet data like the Access control lists.
- TSF_OS contains all security functionalities provided by the certified platform (IC, Javacard operation system). Besides some minor additions, the cryptographic operations are provided by this platform.

1.4.7 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases. This paragraph is directly based on the corresponding paragraph in the protection profile [PP0056v2]; instead of the terms “ePassport” and “travel document” used in [PP0056v2] the akronym “MRTD” is used uniformly here.

1.4.7.1 Phase 1: Development

(Step 1) 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.

(Step 2) The software developer[3] uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

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

1.4.7.2 Phase 2: Manufacturing

(Step 3) In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software in the nonvolatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

The TOE delivery according to CC is the delivery of the IC (with the application code in ROM) from the IC manufacturer to the MRTD 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 MRTD manufacturer combines the IC with hardware for the contact based / contactless interface in the MRTD unless the travel document consists of the card only.

(Step5) The MRTD manufacturer (i) adds the IC Embedded Software or part of it in the non-volatile programmable memories (for instance EEPROM or FLASH) if necessary, (ii) creates the ePassport application, and (iii) equips the MRTD’s chips with pre-personalization Data.

PP application note1: Creation of the application implies applet instantiation.[4]

In this step the final (but not yet personalized) MRTD is generated from the certified components according to the binding initialization and pre-personalization guidelines provided in [Guidance_PRE].

The pre-personalized MRTD together with the IC Identifier is securely delivered fromthe MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

1.4.7.3 Phase 3: Personalisation of the MRTD

(Step 6) The personalization of the MRTD includes (i) the survey of the MRTD holder biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional

[3]Please note that in this ST the role software developer of the protection profile is subdivided into two separate roles: the operating system is developed by the OS software developer, and the MRTD application by the (MRTD) software developer.

[4]PP0056v2 and PP0068v2 application note 1.

biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD and their secure transfer to the personalisation agent, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) the writing the TSF Data into the logical MRTD and 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 (DG1), (ii) the digitised portrait (DG2), and (iii) the Document security object.

The signing of the Document security object by the Document signer [ICAODoc] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

PP and PP0068v2 application note 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE) comprise the Personalisation Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

PP and PP0068v2 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 [ICAODoc]. This approach allows but does not enforce the separation of these roles.

1.4.7.4 Phase 4: Operational use

(Step 7) The TOE is used as MRTD’s chip by the traveller and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the Issuing State or Organization and used according to the security policy of the Issuing State but they can never be modified.

PP and PP0068v2 application note 4: The intention of the underlying PP [PP0056v2] 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 Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. 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.

Some production steps, e.g. Step 4 in Phase 2 may also take place in the Phase 3.

Remark: This ST considers only phase 1 and parts of phase 2 (steps 1 - 3) as part of CC evaluation under ALC.

1.4.8 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 MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

PP0068v2 application note 5: A terminal shall always start a communication session using PACE. If successfully, it should then proceed with passive authentications. If the trial with PACE failed, the terminal may try to establish a communication session using other valid options as described above.

2 Conformance claims

2.1 CC conformance

This security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017; CCMB-2017-04-001, [CC_1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-002, [CC_2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-003, [CC_3],

as follows:

- Part 2 extended,
- Part 3 conformant
- Package conformant to EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC_3].

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017; CCMB-2017-04-004, [CC_4]

has to be taken into account.

The requirements for the evaluation of the TOE and its development and operating environment are those takenfrom the

Evaluation Assurance Level 5 (EAL5)

and augmented by taking the following components:

ALC_DVS.2 and **AVA_VAN.5**.

2.2 PP Claim

This security target claims strict conformance to

- the Protection Profile *Machine Readable Travel Document with "ICAO Application", Extended Access Control* with *PACE (EAC PP)* (BSI-CC-PP0056v2) [PP0056v2],
- the Protection Profile *Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP*), BSI-CC-PP-0068-V2-2011-MA-01 [PP0068v2].

This Security Target has been extended to include Active Authentication according to [ICAODoc].

The evaluation of the TOE uses the result of the CC evaluation of the chip platform claiming conformance to the PP [PP_Javacard]. The hardware part of the composite evaluation is covered by the certification report [ZertIC]. In addition, the evaluation of the TOE uses the result of the CC evaluation of the Javacard OS. The Javacard OS part of the composite evaluation is covered by the certification reports [ZertSmartCafe].

2.3 Statement of Compatibility concerning Composite Security Target

2.3.1 Assessment of the Platform TSFs

The following table lists all Security Functionalities of the underlying Platform ST and shows, which Security Functionalities of the Platform ST are relevant for this Composite ST and which are irrelevant. The first column addresses specific Security Functionality of the underlying platform, which is assigned to Security Functionalities of the Composite ST in the second column. The last column provides additional information on the correspondence if necessary.

Platform TSF-group	Correspondence in this ST	References/Remarks
SF.TRANSACTION	No correspondence, internal Java card mechanisms.	This security function provides atomic transactions according to the Java Card Transaction and Atomicity mechanism with commit and roll-back capability for updating persistent data in flash memory.
SF.ACCESS_CONTROL	No correspondence, internal Java card mechanisms.	This security function provides control for the TOE. It is in charge of the FIREWALL access control SFP and the JCVM information flow control SFP. It enforces applet isolation located in different packages and controls the access to global data containers shared by all applet instances.
SF.CRYPTO	TSF_Crypto	This security function controls all the operations related to the cryptographic key management and cryptographic operations.
SF.INTEGRITY	TSF_Integrity, TSF_Secret	This security function provides a means to check the integrity of checksummed data stored in flash memory.
SF.SECURITY	TSF_Secret	This security function ensures a secure state of information, the non-observability of operations on it and the unavailability of previous information content upon deallocation.
SF.APPLET	No correspondence, internal Java card mechanisms.	This security function ensures the secure loading of a package or installing of an applet and the secure deletion of applets and/or packages.
SF.CARRIER	TSF_Crypto (regarding Secure Messaging)	This security function ensures secure downloading of applications on the card.

Table 2: Relevant platform TSF-groups and their correspondence

2.3.2 Assessment of the Platform SFRs

The following table provides an assessment of all Platform SFRs. The Platform SFRs are listed in the order used within the security target of the platform [ST_SmartCafe].

Platform SFR	Correspondence in this ST	References/Remarks
CoreG_LC Security Functional Requirements (chapter 8.1.1 in platform ST)		
Firewall Policy (chapter 8.1.1.1 in platform ST)		
FDP_ACC.2/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FDP_ACF.1/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FDP_IFC.1/JCVM	No correspondence	Out of scope (internal Java Virtual Machine). No contradiction to this ST.
FDP_IFF.1/JCVM	No correspondence	Out of scope (internal Java Virtual Machine). No contradiction to this ST.
FDP_RIP.1/OBJECTS	No correspondence.	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.1/JCRE	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.1/JCVM	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_MSA.2/FIREWALL-JCVM	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FMT_MSA.3/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FMT_MSA.3/JCVM	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_SMF.1	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.
FMT_SMR.1	No correspondence	Out of scope (internal Java Card Firewall). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
Application Programming Interface (chapter 8.1.1.2 in platform ST)		
FCS_CKM.1 (FCS_CKM.1.1/RSA, FCS_CKM.1.1/ECC, FCS_CKM.1.1/3DES, FCS_CKM.1.1/AES)	FCS_CKM.1/AA FCS_CKM.1/DH-PACE FCS_CKM.1/CA	The requirement in this ST is equivalent to parts of the platform ST. FCS_CKM.1/AA is realized based on FCS_CKM.1.1/RSA and FCS_CKM.1.1/ECC of the platform ST. FCS_CKM.1/DH-PACE and FCS_CKM.1/CA are realized based on FCS_CKM.1.1/ECC of the platform ST. There are no contradictions to this ST.
FCS_CKM.4	FCS_CKM.4	The requirements are compatible (physically overwriting the keys, physically overwriting the keys with zeros).
FCS_COP.1 (FCS_COP.1.1/RSA-CRT-SIGN, FCS_COP.1.1/RSA-SIGN, FCS_COP.1.1/RSA-VERI, FCS_COP.1.1/MAC-DES FCS_COP.1.1/MAC-AES, FCS_COP.1.1/CMAC-AES, FCS_COP.1.1/3DES, FCS_COP.1.1/AES, FCS_COP.1.1/RSA-DEC, FCS_COP.1.1/RSA-CRT-DEC, FCS_COP.1.1/RSA-ENC, FCS_COP.1.1/ECDSA-SIGN, FCS_COP.1.1/ECDSA-VERI, FCS_COP.1.1/HASH, FCS_COP.1.1/ECDH)	FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_ENC FCS_COP.1/CA_MAC FCS_COP.1/SIG_VER FCS_COP.1/SIG_GEN FCS_CKM.1/CA	The platform requirements are necessary to fulfill the requirements of this ST: FCS_COP.1/PACE_ENC of this ST corresponds to the platform SFRs FCS_COP.1.1/AES and FCS_COP.1.1/3DES. FCS_COP.1/PACE_MAC of this ST corresponds to the platform SFR FCS_COP.1.1/CMAC-AES and FCS_COP.1.1/MAC-DES. FCS_COP.1/CA_ENC of this ST corresponds to the platform SFRs-FCS_COP.1.1/AES and FCS_COP.1.1/3DES. FCS_COP.1/CA_MAC of this ST corresponds to the platform SFRs-FCS_COP.1.1/CMAC-AES and FCS_COP.1.1/MAC-DES. FCS_COP.1/SIG_VER of this ST corresponds to the platform SFRs FCS_COP.1.1/ECDSA-VERI and FCS_COP.1.1/RSA-VERI. FCS_COP.1/SIG_GEN of this ST corresponds to the platform SFR FCS_COP.1.1/RSA-SIGN and FCS_COP.1.1/ECDSA-SIGN. FCS_COP.1.1/HASH of the platform is used within Active Authentication,

Platform SFR	Correspondence in this ST	References/Remarks
		PACE, Chip and Terminal Authentication: • FCS_COP.1/SIG_VER • FCS_COP.1/SIG_GEN • FCS_CKM.1/CA • FIA_API.1 • FIA_API.1/AA. FCS_COP.1.1/RSA-DEC is used for the implementation of the Diffie-Hellman calculation in FCS_CKM.1/CA. No contradictions to this ST.
FCS_RNG.1	FCS_RND.1	In this ST, random numbers according to AIS20 class DRG.3 are required. The platform generates random numbers with a defined quality metric (DRG.3) that can be used directly.
FDP_RIP.1/ABORT	FDP_RIP.1	Implicitly used for this ST. No contradiction to this ST.
FDP_RIP.1/APDU	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/GlobalArray	FDP_RIP.1	Implicitly used for this ST. No contradiction to this ST.
FDP_RIP.1/bArray	FDP_RIP.1	Implicitly used for this ST. No contradiction to this ST.
FDP_RIP.1/KEYS	FDP_RIP.1	Implicitly used for this ST. No contradiction to this ST.
FDP_RIP.1/TRANSIENT	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ROL.1/FIREWALL	No correspondence.	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
Card Security Management (chapter 8.1.1.3 in platform ST)		
FAU_ARP.1	FPT_FLS.1, FPT_PHP.3	Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. Internal counter for security violations complement Java Card OS mechanisms-No contradiction to this ST.
FDP_SDI.2	FPT_FLS.1, FPT_PHP.3	Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FPR_UNO.1	FPT_EMS.1	Not directly corresponding, but relevant for the fullfillment of FPT_EMS.1. No contradiction to this ST.
FPT_FLS.1	FPT_FLS.1	The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction to this ST.
FPT_TDC.1	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_TST.1	FPT_TST.1	Self-testing is provided by the Java Card platform during initial start-up.
Aid Management (chapter 8.1.1.4 in platform ST)		
FIA_ATD.1/AID	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UID.2/AID	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_USB.1/AID	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MTD.1/JCRE	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MTD.3/JCRE	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
INSTG Security Functional Requirements (chapter 8.1.2 in platform ST) This group consists of the SFRs related to the installation of the applets, which addresses security aspects outside the runtime.		
FDP_ITC.2/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_RCV.3/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
ADELG Security Functional Requirements (chapter 8.1.3 in platform ST) This group consists of the SFRs related to the deletion of applets and/or packages, enforcing the applet deletion manager (ADEL) policy on security aspects outside the runtime.		
FDP_ACC.2/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ACF.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FDP_RIP.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
ODELG Security Functional Requirements (chapter 8.1.4 in platform ST) The following requirements concern the object deletion mechanism. This mechanism is triggered by the applet that owns the deleted objects by invoking a specific API method.		
FDP_RIP.1/ODEL	FDP_RIP.1	Implicitly used for this ST. No contradiction to this ST.
FPT_FLS.1/ODEL	FPT_FLS.1	The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction to this ST.
CARG Security Functional Requirements (chapter 8.1.5 in platform ST) This group includes requirements for preventing the installation of packages that has not been bytecode verified, or that has been modified after bytecode verification.		
FCO_NRO.2/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_IFC.2/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_IFF.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_UIT.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UID.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FMT_SMR.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FTP_ITC.1/CM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
CMGR Security Functional Requirements (chapter 8.1.6 in platform ST) In the PP of the Java Card certification [PP_Javacard], objectives for Card Management were objectives for the environment. Since the card manager has been defined to be part of the TOE, they were transformed into objectives for the TOE and are covered by SFRs in the platform ST.		
FTP_ITC.1/CMGR	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
SCPG Security Functional Requirements (chapter 8.1.7 in platform ST) In the PP of the Java Card certification [PP_Javacard], objectives for the smart card platform are objectives for the environment. Since the smart card platform has been defined to be part of the TOE, they were transformed into objectives for the TOE and are covered by SFRs in the platform ST.		
FPT_PHP.3	FPT_PHP.3 FPT_EMS.1	The fulfillment of the SFR in this ST is based on the platform SFR (together with additional countermeasures).

Table 3: Assessment of the platform SFRs.

2.3.3 Assessment of the Platform Objectives

The following table provides an assessment of all relevant Platform objectives.

Platform Objective	Correspondence in this ST	References/Remarks
O.SID	No correspondence	Out of scope. No contradiction to this ST.
O.FIREWALL	No correspondence	Out of scope. No contradiction to this ST.
O.GLOBAL_ARRAYS_CONFID	OT.Data-Confidentiality	No contradiction to this ST.
O.GLOBAL_ARRAYS_INTEG	OT.Data-Integrity	No contradiction to this ST.
O.ARRAY_VIEWS_CONFID	OT.Data-Confidentiality	No contradiction to this ST.
O. ARRAY_VIEWS_INTEG	OT.Data-Integrity	No contradiction to this ST.
O.NATIVE	No correspondence	Out of scope. No contradiction to this ST.
O.OPERATE	No correspondence	Out of scope. No contradiction to this ST.
O.REALLOCATION	No correspondence	Out of scope. No contradiction to this ST.
O.RESOURCES	No correspondence	Out of scope. No contradiction to this ST.
O.ALARM	No correspondence	Out of scope. No contradiction to this ST.

Platform Objective	Correspondence in this ST	References/Remarks
O.CIPHER	No correspondence	Indirectly relevant for the correct function of the TOE of this ST, but no corresponding objectives for the TOE of this ST. No contradictions.
O.RNG	No correspondence	No contradiction to this ST.
O.KEY-MNGT	No correspondence	Out of scope. No contradiction to this ST.
O.PIN-MNGT	No correspondence	Out of scope. No contradiction to this ST.
O.TRANSACTION	No correspondence	Out of scope. No contradiction to this ST.
O.OBJ-DELETION	No correspondence	Out of scope. No contradiction to this ST.
O.DELETION	No correspondence	Out of scope. No contradiction to this ST.
O.LOAD	No correspondence	Out of scope. No contradiction to this ST.
O.INSTALL	No correspondence	Out of scope. No contradiction to this ST.
O.CARD-MANAGEMENT	No correspondence	Out of scope. No contradiction to this ST.
OT.SCP.IC	OT.Prot_Phys-Tamper	The objectives are related. No contradiction to this ST.
OT.SCP.RECOVERY	OT.Prot_Malfunction	The objectives are related. No contradiction to this ST.
O.SCP.SUPPORT	No correspondence	Out of scope. No contradiction to this ST.

Table 4: Assessment of the platform objectives.

2.3.4 Assessment of Platform Threats

The following table provides an assessment of all relevant Platform threats.

Platform Threat	Correspondence in this ST	References/Remarks
T.CONFID-APPLI-DATA	No correspondence	Out of scope. No contradiction to this ST.
T.CONFID-JCS-CODE	No correspondence	Out of scope. No contradiction to this ST.
T.CONFID-JCS-DATA	T.Information_Leakage	No contradiction to this ST.
T.INTEG-APPLI-CODE	No correspondence	Out of scope. No contradiction to this ST.

Platform Threat	Correspondence in this ST	References/Remarks
T.INTEG-APPLI-CODE.LOAD	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-APPLI-DATA	T.Forgery	No contradiction to this ST.
T.INTEG-APPLI-DATA.LOAD	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-JCS-CODE	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-JCS-DATA	No correspondence	Out of scope. No contradiction to this ST.
T.SID.1	No correspondence	Out of scope. No contradiction to this ST.
T.SID.2	No correspondence	Out of scope. No contradiction to this ST.
T.EXE-CODE.1	No correspondence	Out of scope. No contradiction to this ST.
T.EXE-CODE.2	No correspondence	Out of scope. No contradiction to this ST.
T.NATIVE	No correspondence	Out of scope. No contradiction to this ST.
T.RESOURCES	No correspondence	Out of scope. No contradiction to this ST.
T.DELETION	No correspondence	Out of scope. No contradiction to this ST.
T.SECURE_DELETION	No correspondence	Out of scope. No contradiction to this ST.
T.INSTALL	No correspondence	Out of scope. No contradiction to this ST.
T.OBJ-DELETION	No correspondence	Out of scope. No contradiction to this ST.
T.PHYSICAL	T.Phys-Tamper	No contradiction to this ST.

Table 5: Threats of the platform ST.

2.3.5 Assessment of Platform Organisational Security Policies

The Organisational Security Policy "OSP.VERIFICATION" focuses on the integrity of loaded applets, which is fulfilled by the TOE of this ST since the applet is loaded secured by platform security measures into the flash memory. This policy does not contradict to the policies of this ST.

2.3.6 Assessment of Platform Operational Environment

2.3.6.1 Assessment of Platform Assumptions

In the first column, the following table lists all assumptions of the Platform ST. The last column provides an explanation of relevance for the Composite TOE.

Platform Assumption	Relevance for Composite ST
A.CAP_FILE	A.APPLET states that applets loaded post-issuance do not contain native methods. This assumption leads to appropriate directives in the user guidance [Guidance_PRE].
A.VERIFICATION	This assumption targets the applet code verification. Regarding post-issuance loading of third party applets, this assumption leads to appropriate directives in the user guidance [Guidance_PRE].

Table 6: Assumptions of the Platform ST.

2.3.6.2 Assessment of Platform Objectives for the Operational Environment

There are the following Platform Objectives for the Operational Environment that have to be considered.

Platform Objective for the Environment	Relevance for Composite ST
OE.CAP_FILE	The platform objective for the environment states that applets loaded post-issuance do not contain native methods. This objective for the environment leads to appropriate directives in the user guidance [Guidance_PRE].
OE.VERIFICATION	The platform objective for the environment targets the applet code verification. This is fulfilled by the TOE of this ST; regarding third-party-code, this objective for the environment leads to appropriate directives in the user guidance [Guidance_PRE]. There it is stated that all applets loaded to the TOE have to be verified.
OE.CODE-EVIDENCE	The platform objective for the environment focusses on application code loaded pre-issuance or post-issuance. It has to be ensured that the loaded application has not been changed since the code verification. This objective for the environment leads to appropriate directives in the user guidance [Guidance_PRE].

Table 7: Platform Security Objectives and SFRs for the Operational Environment

3 Security problem definition

This chapter has been taken from [PP0056v2] and [PP0068v2] with only minor modifications.

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 the claimed PACE PP [PP0068v2], chap 3.1.

PP0068v2 application note 6: Please note that user data being referred to in [PP0068v2] 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 also secures these specific travel document holder's data as stated in the table above.

PP0068v2 application note 7: Since the travel document does not support any secret travel document holderauthentication 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.

PP0068v2 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 shall secure 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.

3.1.1.1 Logical MRTD sensitive User Data

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

PP application note5: Due to interoperability reasons the 'ICAO Doc 9303' [ICAODoc] 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 [ICAODoc]. Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [PP0055]). If supported, it is therefore recommended to used PACE instead of BAC. <u>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.</u>

A sensitive asset is the following more general one.

3.1.1.2 Authenticity of the MRTD's chip

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

Due to strict conformance to PACE PP, this security target also includes all assets listed in [PP0068v2], chap 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). Due to identical names and definitions these are not repeated here.

3.1.2 Subjects

This Security Target considers the following subjects additionally to those defined in the PACE PP [PP0068v2]:

3.1.2.1 Country Verifying Certification Authority

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. 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.

3.1.2.2 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 Systemsfor the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.

3.1.2.3 Terminal

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

3.1.2.4 Inspection system (IS)

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

The Extended Inspection System (EIS) performs the Advanced Inspection Procedure and therefore (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 [5] 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.

PP Application note 6: For definition of Basic Inspection System (BIS) resp. Basic Inspection System with PACE (BIS-PACE) see PACE PP [PP0068v2].

3.1.2.5 Attacker

Additionally to the definition from PACE PP [PP0068v2], chap 3.1 the definition of an attacker is refined as followed: 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.

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.

PP0068v2 application note 9: Since the TOE does not use BAC, a Basic Inspection System with BAC (BIS-BAC) cannot be recognised by the TOE.

This ST includes all subjects from the PACE Protection Profile [PP0068v2], chap 3.1, namely Manufacturer, Personalisation Agent, Basic Inspection System (with PACE), Document Signer (DS), and Country Signing Certification Authority (CSCA), Travel Document Holder and Travel Document Presenter (traveller). Due to identical definitions and names they are not repeated here.

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.

3.2.1 A.Insp_Sys Inspection Systems for global interoperability

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [ICAO_SAC] and/or BAC [PP0055]. 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 [PP0068v2] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality of the TOE.

3.2.2 A.Auth_PKI PKI for Inspection Systems

The issuing and receiving States or Organizations 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 Organizations 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 Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their MRTD’s chip.

This ST includes the assumption from the PACE PP [PP0068v2], chap 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.

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

3.3.1 T.Read_Sensitive_Data Read the sensitive biometric reference data

Adverse action:	An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document’s chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [PP0055]) 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)

3.3.2 T.Counterfeit MRTD's chip

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

This ST includes all threats from the PACE PP [PP0068v2], chap 3.2, namely T.Skimming, T.Eavesdropping, T.Tracing, T.Abuse-Func, T.Information_Leakage, T.Phys-Tamper, and T.Malfunction. Due to identical definitions and names they are not repeated here as well.

PP0068v2 application notes 10 – 19: <informational only>

PP Application note 8: T.Forgery from the PACE PP [PP0068v2] is extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

3.3.3 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 the Extended Inspection System 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

3.4 Organizational security policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CCpart 1 [CC_1], section 3.2).

3.4.1 P.Sensitive_Data Privacy of sensitive biometric reference data

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the MRTD holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the MRTD 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 MRTD'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.

3.4.2 P.Personalization Personalization of the MRTD by issuing State or Organization only

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

This ST includes all OSPs from the PACE PP [PP0068v2], chapter 3.3, namely P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI, P.Manufact and P.Terminal. Due to identical definitions and names they are also not repeated here.

PP0068v2 application note 20:<informational 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.

4.1.1 OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 andEF.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 forthe successful authentication and shall be a non-strict subset of the authorization defined in theDocument Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks withhigh attack potential.

4.1.2 OT.Chip_Auth_Proof Proof of MRTD's chip authenticity

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

PP application note 9: The OT.Chip_Auth_Proof implies the MRTD's chip to have (i) a unique identity as given by the MRTD'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 MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [ICAODoc] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

This ST includes all Security Objectives for the TOE from the PACE PP [PP0068v2], chap 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. Due to identical definitions and names they are not repeated here as well.

PP0068v2 application notes 21 – 23: <informational only>

The following Security Objective for the TOE is defined in addition to the objectives given by the Protection Profiles to cover the Active Authentication mechanism.

4.1.3 OT.Active_Auth_Proof Proof of travel document's chip authenticity

The TOE shall support the Basic 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 Active Authentication as defined in [ICAODoc]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

4.2 Security Objectives for the Operational Environment

4.2.1 Issuing State or Organization

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

4.2.1.1 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 [PP0068v2] 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 the Protection Profile [PP0056v2] and not in [PP0068v2].

4.2.1.2 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 [PP0068v2] 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 the Protection Profile [PP0056v2] and not in [PP0068v2].

4.2.2 Receiving State or Organization

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

4.2.2.1 OE.Exam_Travel_Document Examination of the travel document passport book

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [ICAO_SAC] and/or the Basic Access Control [6]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

Justification: This security objective for the operational environment is needed additionally to those from [PP0068v2] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [PP0068v2] and therefore also counters T.Forgery and A.Passive_Auth from [PP0068v2]. This is done because a new type of Inspection System is introduced in the protection profile [PP0056v2] as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

4.2.2.2 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 [PP0068v2] 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.

4.2.2.3 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 [PP0068v2] 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.

This ST includes all Security Objectives of the TOE environment from the PACE PP [PP0068v2], chap. 4.2, namely OE.Legislative_Compliance, OE.Passive_Auth_Sign, OE.Personalisation, OE.Terminal, and OE.Travel_Document_Holder. Due to identical definitions and names they are not repeated here.

PP0068v2 application note 24: <informational only>

The following objective for the environment was added:

4.2.2.4 OE.Active_Auth_Key_MRTD:

The inspection system of the receiving State or Organisation must carry out Active Authentication to verify the Authenticity of the presented travel document's chip.

Justification: This security objective for the operational environment is needed additionally to those from [PP0068v2]and [PP0056v2] in order to handle the Threat T.Counterfeit. It neither mitigates a threat meant to be addressed by security objectives for the TOE – this is achieved by chip authentication alone - nor fulfils an OSP meant to be addressed by security objectives for the TOE.

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	*OT.AC_Pers*[5]	*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*	OT.Active_Auth_Proof	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	*OE.Prot_Logical_Travel_Document*	*OE.Ext_Insp_Systems*	*OE.Personalisation*	*OE.Passive_Auth_Sign*	*OE.Terminal*	*OE.Travel_Document_Holder*	*OE.Legislative_Compliance*	OE.Active_Auth_Key_MRTD
T.Read_Sensitive_Data	x														x			x						
T.Counterfeit		x											x	x		x								x
T.Skimming[6]				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 8: Overview of the security objectives coverage

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

[5] The Objectives marked in italic letters are included from the claimed PACE-PP [PP0068v2]. They are listed for the complete overview of the security objectives.

[6] Threats and assumptions included from the claimed PACE-PP [PP0068v2] are marked in italic letters. They are listed for the complete overview of threats and assumptions.

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 [PP0068v2]. **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 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 [PP0068v2] 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 [PP0068v2] 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.Authorize_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.

In addition to the rationale given by the Protection Profiles, the threat **T.Counterfeit**"Conterfeit of travel document's chip data" is thwarted through the chip by anidentification and authenticity proof required by **OT.Active_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 Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by OE**.Active_Auth_Key_MRTD** “Travel Document ActiveAuthentication Key”.

5 Extended Component Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [PP0068v2], other components are defined in the protection profile [PP0056v2].

5.1 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.

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. [PP0056v2] defines the family FIA_API in the style of [CC_2] 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 Authentication Proof of Identity	1

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 claimedidentity.
Audit:	There are no actions defined to be auditable.
FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a [assignment:*authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

This ST includes all Extended Component Definitions from the PACE PP [PP0068v2], chap. 5, namely FAU_SAS, FCS_RND, FMT_LIM, FPT_EMS. These definitions are taken over as described in [PP0068v2], therefore they are not repeated here.

PP0068v2 application note 25: <informational only>

6 IT 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 [CC_1] of the CC. Each of these operations is used in this ST and the underlying PP.

Operations already performed in the underlying PPs [PP0056v2, PP0068v2] are uniformly marked by ***bold italic*** font style; for further information on details of the operation, please refer to [PP0068, PP0056v2].

Operations performed within this Security Target are marked by **<u>bold underlined</u>** font style; further information on details of the operation is provided in foot notes.

6.1 Security Definitions

Definition of security attributes:

Security Attribute	Values	Meaning
Terminal Authentication Status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR-03110]); 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]); Terminal is authenticated as domestic Document Verifierafter successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR-03110]); 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]); 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])
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR-03110])
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [TR-03110])

Table 9: Definition of security attributes.

The following table provides an overview of the keys and certificates used. Further keys and certificates are listed in [PP0068v2].

Name	Abbreviation	Description
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	Abbreviation	Description
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. [PP0055] 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 attributes.
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 11770-3 [ISO11770-3].
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 MRTD and used by the inspection system for Chip Authentication of the MRTD'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 MRTD's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair		Country Signing Certification Authority of the Issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by Receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.

Name	Abbrevia-tion	Description
Document Signer Key Pairs		Document Signer of the Issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the Receiving State or organization with the Document Signer Public Key.
Chip Authentication Session Key		Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.
PACE Session KEys	K_{ENC}, K_{MAC}	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.
Active Authentication KeyPair		The Active Authentication Key Pair (KPr_{AA}, KPu_{AA}) is used for the Active Authentication mechanism according to [ICAO-Doc].
Active Authentication Public Key	KPu_{AA}	The Active Authentication Public Key (KPu_{AA}) is stored in EF.DG15 and used by the inspection system for Active Authentication of the travel document's chip. It is part of the user data provided by the TOE for the IT environment. A hash representation of DG15 (Public Key (KPu_{AA}) info) is stored in the Document Security Object (SO_D).
Active Authentication Private Key	KPr_{AA}	The Active Authentication Private Key (KPr_{AA}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

Table 10: Overview of the keys and certificates.

PP application note 11: The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization.

6.2 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. Note that this ST contains SFRs from PP0068v2 and PP0056v2. SFRs from the PACE PP [PP0068v2] are not repeated in PP0056v2 but listed in the following *Table 11*. Only those SFRs from PACE PP that are extended are written down in PP0056v2.

SFRs taken directly from PACE PP [PP0068v2]
FAU_SAS.1
FCS_CKM.1/DH_PACE

FCS_CKM.4[7]
FCS_COP.1/PACE_ENC
FCS_COP.1/PACE_MAC
FCS_RND.1[8]
FIA_AFL.1/PACE
FIA_UAU.6/PACE
FDP_RIP.1[9]
FDP_UCT.1/TRM[10]
FDP_UIT.1/TRM[11]
FMT_SMF.1
FMT_MTD.1/INI_ENA
FMT_MTD.1/INI_DIS
FMT_MTD.1/PA
FPT_TST.1
FPT_FLS.1
FPT_PHP.3
FTP_ITC.1/PACE[12]

Table 11: SFRs taken from PACE PP

6.2.1 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.

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

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/
DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: **based on ECDH compliant to ISO 15946 with the**

[7]Please also refer to PP Application note 15 in this ST

[8]Please also refer to PP Application note 26 in this ST

[9]Please also refer to PP Application note 15 in this ST

[10]Please also refer to PP Application note 35 in this ST

[11]Please also refer to PP Application note 35 in this ST

[12]Please also refer to PP Application note 25 in this ST

domain parameters provided in NIST DSS standard FIPS 186-3 [FIPS186-3] Appendix D or in Brainpool ECC Standard Curves [Brainpool] chapters 3.1 to 3.5[13] with cryptographic key sizes **224, 256, 320, 384, 512 or 521 bit, respectively**[14] that meet the following: **[ICAO_SAC].**

PP0068v2 application note 26: <informative only>

PP0068v2 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]: fulfilled by FCS_COP.1/CA_ENCand FCS_COP.1/CA_MAC FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: **Diffie-Hellman key derivation or ECDH protocol with the domain parameters provided in NIST DSS standard FIPS 186-3 [FIPS186-3] Appendix D or in Brainpool ECC Standard Curves [Brainpool] chapters 3.1 to 3.5** with cryptographic key sizes of **1024, 1280, 1536, 1984, 2048, 4096 bit, or of 224, 256, 320, 384, 512, 521 bit, respectively**[15] that meet the following: **based on the Diffie-Hellman key derivation protocol compliant to [PKCS#3] and [TR-03110] , or ECDH protocol compliant to ISO 15946** [16].

PP Application note 12: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [TR-03110].

PP Application note 13: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [TR-03110]. This protocol is based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [PKCS#3]), or on ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [TR-03111], 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]).

PP Application note 14: The PP application note was refined due to inconsistencies between [PP0056v2], [TR-03110] (part 3) and [ICAO_SAC]:

a) The TOE uses SHA-1 to derive 128 (AES) bit session keys for secure messaging.
b) According to requirements given in section 4.2 of [ICAO_SAC] and section A.2.3 of [TR-03110] (part 3), the bit-length of the hash function shall be greater or equal to the bit-length of the derived key. For this reason the Chip Authentication Protocol implemented by the TOE uses SHA-256 to derive session keys for secure messaging based on AES with 192 and 256 bit keys.

[13] [assignment: cryptographic key generation algorithm]

[14] [assignment: cryptographic key sizes]

[15] [assignment: cryptographic key sizes]

[16] [selection: based on the Diffie-Hellman key derivation protocol compliant to [PKCS#3] and [TR-03110], based on an ECDH protocol compliant to [ISO 15946]]

c) The Terminal Authentication implemented by the TOE supports SHA-1, SHA-224, and SHA-256, SHA-384, SHA-512.

PP Application note 15: <applied, see section FCS_CKM.4 below>.

The following SFR has been added with respect to the Active Authentication mechanism.

FCS_CKM.1/AA Cryptographic key generation – Active Authentication key pair

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/AA	The TSF shall generate cryptographic keys pair in accordance with a specified cryptographic key generation algorithm: **RSA key generation with or without CRT, or ECDSA key generation**[17] with cryptographic key sizes **of 1024, 1280, 1536, 1984, 2048, 4096 bit; or of 224, 256 and 320, 384, 512, 521 bit**[18] that meet the following: **RSA key generation with or without CRT compliant with [ISO9796-2]; or ECDSA key generation following [ISO15946]** [19].

Application Note: The Active Authentication key pair can either be generated in the TOE or imported by the Personalisation Manager (cf. FMT_MTD.1/AA). This SFR has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

FCS_CKM.4 Cryptographic key destruction

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**[20] that meets the following: **none**[21].

PP0068v2 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.

6.2.1.1 Cryptographic operation (FCS_COP.1)

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

[17] [assignment: cryptographic key generation algorithm]

[18] [assignment: cryptographic key sizes]

[19] [assignment: list of standards]

[20] [assignment: cryptographic key destruction method]

[21] [assignment: list of standards]

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/ PACE_ENC	The TSF shall perform ***secure messaging – encryption and decryption*** in accordance with a specified cryptographic algorithm: **AES, or 3DES in CBC mode**[22] and cryptographic key size **128, 192, 256, or 112 bit**[23] that meets the following: **compliant to [ICAO_SAC]**.

PP0068v2 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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/ PACE_MAC	The TSF shall ***perform secure messaging – message authentication code*** in accordance with a specified cryptographic algorithm: **AES-CMAC, or Retail-MAC**[24] and cryptographic key size **128, 192, 256 bit, or 112 bit**[25] that meets the following: ***[ICAO_SAC]***.

PP0068v2 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 the FCS_CKM.1/DH_PACE (PACE-KMAC). Note that in accordance with [ICAO_SAC] the (two-key) Triple-DES can be used in Retail mode for secure messaging.

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

Hierarchical to:	No other components.

---

[22] [assignment: cryptographic algorithm]

[23] [assignment: cryptographic key sizes]

[24] [assignment: cryptographic algorithm]

[25] [assignment: cryptographic key sizes]

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/CA
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_COP.1.1/CA_ENC The TSF shall ***perform secure messaging – encryption and decryption*** in accordance with a specified cryptographic algorithm: **AES in CBC mode, or 3DES in CBC mode**[26] and cryptographic key size **128, 192, 256 bit, or 112 bit**[27] that meets the following: **[ICAO_SAC]**[28].

PP Application note 16: This SFR requires the TOE to implement the cryptographic primitives (3DES 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.

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]: fulfilled by FCS_CKM.1/CA
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_COP.1.1/CA_MAC The TSF shall ***perform secure messaging – message authentication code*** in accordance with a specified cryptographic algorithm: **AES-CMAC, or Retail-MAC**[29] and cryptographic key size **128, 192 and 256 bit, or 112 bit**[30] that meets the following: ***[TR-03110]***.

PP Application note 18: 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.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD

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/CA
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

---

[26] [assignment: cryptographic algorithm]

[27] [assignment: cryptographic key sizes]

[28] [assignment: list of standards]

[29] [assignment: cryptographic algorithm]

[30] [assignment: cryptographic key sizes]

FCS_COP.1.1/SIG_VER The TSF shall perform ***digital signature verification*** in accordance with a specified cryptographic algorithm: **RSASSA-PSS with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512; or ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 and the domain parameters provided in NIST DSS standard FIPS 186-3 [FIPS186-3] Appendix D or in Brainpool ECC Standard Curves [Brainpool] chapters 3.1 to 3.5**[31] and cryptographic key sizes **of 1024, 1280, 1536, 1984, 2048, 4096 bit; or of 224, 256 and 320, 384, 512, 521 bit**[32] that meet the following: **[PKCS1]; or [ISO15946]**[33].

PP Application note 17: Applied. 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.

FCS_COP.1/SIG_GEN Cryptographic operation – Signature generation by MRTD

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**[34] in accordance with a specified cryptographic algorithm: **RSA-Digital Signature Scheme 1 with SHA-1 or SHA-256; or ECDSA** [35] and cryptographic key sizes **of 1024, 1280, 1536, 1984, 2048, 4096 bit; or of 224, 256 and 320, 384, 512, 521 bit** [36] that meet the following: **[ISO9796-2]; or [TR-03111]**[37].

Application Note: The TOE performs digital signature generation with RSA or ECDSA. This SFR has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in section 2.2. The digital signature creation is necessary to allow Active Authentication (AA). This extension does not conflict with the strict conformance to the claimed Protection Profiles.

6.2.1.2 Random Number Generation (FCS_RND.1)

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 **the AIS20 Class DRG.3 quality metric**[38].

---

31 [assignment: cryptographic algorithm]

32 [assignment: cryptographic key sizes]

33 [assignment: list of standards]

34 [assignment: list of cryptographic operations]

35 [assignment: cryptographic algorithm]

36 [assignment: cryptographic key sizes]

37 [assignment: list of standards]

38 [assignment: a defined quality metric]

PP0068v2 application note 31: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE.

Developer note: The corresponding platform SFR (FCS_RNG.1) states that the platform provides a deterministic random number generator (RNG) that fulfills the following:

- (DRG.3.1) The internal state of the RNG (= slave CTR_DRBG) uses a DRNG (= master CTR_DRBG) of class DRG.3 as a random source. The master CTR_DRBG uses a PTRNG of class PTG.2 as a random source.The internal state of the RNG uses a PTRNG of class PTG.2 as a random source.
- (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 generates output for which 2^34 + 1 output strings of bit length 128 are mutually different with probability 1 - 2^-16.
- (DRG.3.5) Statistical test suites cannot practically distinguish the random number from output sequences of an ideal RNG. The random numbers pass test procedure A as defined in AIS20/31.

6.2.2 Class FIA Identification and Authentication

PP Application note 19, extended to include Active Authentication: The following table provides an overview of the authentication mechanisms used:

Name	SFR for the TOE
Symmetric Authentication Mechanismfor Personalisation Agents	FIA_UAU.4/PACE
Chip Authentication Protocol	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol	FIA_UAU.5/PACE
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE
Active Authentication Mechanism	FIA_API.1/AA

Table 12: Overview on authentication SFR

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

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

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

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1/PACE	The TSF shall detect when **10**[39] unsuccessful authentication attempt occurs related to ***authentication attempts using the PACE password as shared password***.
FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **delay each of the following authentication attempt until the next successful authentication attempt by an increasing amount of time**[40].

PP0068v2 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[41], 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[42] requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of this ST. 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'.

FIA_API.1 Authentication Proof of Identity

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

PP Application note 30: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [TR-03110]. 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 [ICAODoc]. 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 (Active Authentication)

---

[39] [assignment: positive integer number]

[40][assignment: list of actions]

[41] ≥ 100 bits; a theoretical maximum of entropy which can be delivered by a character string is N*ld(C), whereby N is the length of the string, C – the number of different characters which can be used within the string.

[42] guessing CAN or MRZ, see T.Skimming above

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA The TSF shall provide **the Active Authentication Mechanisms according to [ICAO-Doc]**[43] to prove the identity of the **TOE**[44].

Application Note: The SFR FIA_API.1/AA has been included inthis security target in addition to the SFRs defined by the Protection Profiles claimed insection 2.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

FIA_UID.1/PACE Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/PACE The TSF shall allow

1. ***to establish the communication channel*,**
2. **carrying out the PACE Protocol according to [ICAO_SAC],**
3. ***to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,***
4. ***to carry out the Chip Authentication Protocol v.1 according to [TR-03110],***
5. ***to carry out the Terminal Authentication Protocol v.1 according to [TR-03110],***
6. **to carry out the Active Authentication Mechanism**[45]

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.

PP0068v2 application note 33: User identified after a successfully performed PACE protocol is a PACE authenticated BIS-PACE. Please note that neither CAN nor MRZ effectively represent secrets (but other PACE passwords may do so), but are restricted-revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE).

PP Application note 20: The SFR FIA_UID.1/PACE in PP0056v2 covers the definition in PACE PP [PP0068v2] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.

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 Initialization 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

[43] [assignment: authentication mechanism]

[44] [assignment: authorized user or role]

[45] [assignment: list of TSF-mediated actions]

identify itself as (i) 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).

PP Application note 22: User identified 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 (Basic Inspection System with PACE).

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).

FIA_UAU.1/PACE Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1/PACE	The TSF shall allow 1. ***to establish the communication channel***, 2. ***carrying out the PACE Protocol according to [ICAO_SAC],*** 3. ***to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS***, *4.* ***to identify themselves by selection of the authentication key,*** *5.* ***to carry out the Chip Authentication Protocol v.1 according to [TR-03110],*** *6.* ***to carry out the Terminal Authentication Protocol v.1 according to [TR-03110],*** 7. **<u>to carry out the Active Authentication Mechanism</u>**[46] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/PACE	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

PP0068v2 application note 34: <Superseded by PP application note 25 below>.

PP application note 24: The SFR FIA_UAU.1/PACE in this ST covers the definition in PACE PP [PP0068v2] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.

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-KMAC, PACE-KEnc), cf. FTP_ITC.1/PACE.

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

[46] [assignment: list of TSF-mediated actions]

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. ***PACE Protocol according to [ICAO_SAC]***
2. ***Authentication Mechanism based on AES,***[47]
3. ***Terminal Authentication Protocol v.1 according to [TR-03110]***[48]

PP0068v2 application note 35: For the PACE protocol, the TOE randomly selects a nonce s of 128 bits length being (almost) uniformly distributed.

PP application note 26: The SFR FIA_UAU.4.1 in this ST covers the definition in PACE PP [PP0068v2] 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 [PP0068v2].

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.

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 [ICAODoc],***
3. ***Secure Messaging in MAC-ENC mode according to [ICAO_SAC],***
4. ***Symmetric Authentication Mechanism based on AES***[49]***,***
5. ***Terminal Authentication Protocol v.1 according to [TR-03110]***[50]

to support user authentication.

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

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

[47] [selection: Triple-DES, AES or other approved algorithms].

[48][assignment: identified authentication mechanism(s)]

[49] The TOE implements a symmetric authentication mechanism based on AES for the Personalization Agent as defined in [ISO18013-3], which is equivalent to the BAC protocol, but based on AES (in CBC mode for encryption and decryption following [NIST800-38A] and as a CMAC for message authentication following [NIST800-38B]).

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

2. ***The TOE accepts the authentication attempt as Personalisation Agent by*** **<u>Authentication Mechanism with Personalization Agent Keys</u>**[51].
3. ***After run of the Chip Authentication Protocol v. 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v. 1.***
4. ***The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Protocol v.1***.[52]
5. **<u>None.</u>**[53]

PP application note 28: The SFR FIA_UAU.5.1/PACE in this ST covers the definition in PACE PP [PP0068v2] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in this ST covers the definition in PACE PP [PP0068v2] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

PP0068v2 application note 36: Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of ePassport application.

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***.

PP application note 29: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAODoc] 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.

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.***

[51][selection: the Authentication Mechanism with Personalisation Agent Key(s)]

[52] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

[53][assignment: rules describing how the multiple authentication mechanisms provide authentication]

PP0068v2 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.

6.2.3 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*** on ***terminals gaining access to the User data and data stored in EF.Sod of the logical travel document***.

PP Application note 31: The SFR FDP_ACC.1.1 in this ST covers the definition in PACE PP [PP0068v2] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to PACE PP.

PP0068v2 application note 38:<applied>

FDP_ACF.1/TRM Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

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

1. ***Subjects:***
   a. ***Terminal,***
   b. ***BIS-PACE,***
   c. ***Extended Inspection System.***
2. ***Objects:***
   a. ***data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logicalMRTD,***
   b. ***data in EF.DG3 of the logical MRTD,***
   c. ***data in EF.DG4 of the logical MRTD,***
   d. ***all TOE intrinsic secret cryptographic keys stored in the travel document.***
3. ***Security attributes:***
   a. ***PACE Authentication,***
   b. ***Terminal Authentication v.1,***
   c. ***Authorization of the Terminal.***

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

	data objects from FDP_ACF.1.1/TRM according to [TR-03110] after a successful PACE authentication as required by FIA_UAU.1/PACE.
FDP_ACF.1.3/TRM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***none***.
FDP_ACF.1.4/TRM	The TSF shall explicitly deny access of subjects to objects based on the ***rule***: ***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.***

PP application note 32: The SFR FDP_ACF.1.1/TRM in this ST covers the definition in PACE PP [PP0068v2] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in this ST cover the definition in PACE PP [PP0068v2]. The SFR FDP_ACF.1.4/TRM in this ST covers the definition in PACE PP [PP0068v2] and extends it by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP.

PP0068v2 application note 39: <applied>

PP application note 33: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [TR-03110]. 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.

PP application note 34, PP0068v2 application note 40: Please note that the Document Security Object (SOD) stored in EF.SOD (see [ICAODoc]) 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].

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 Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

PP0068v2 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

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 **deallocation of the resource from**[54] 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)*** ***3. None***[55]

PP0068v2 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 destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD

Hierarchical to:	No other components.
Dependencies:	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]: fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/TRM
FDP_UCT.1.1/TRM	The TSF shall enforce the ***Access Control SFP*** to be able to ***transmit and receive*** user data in a manner protected from unauthorized disclosure**.**

FDP_UIT.1/TRM Data exchange integrity

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

6.2.4 Class FTP Trusted Path/Channels

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

Hierarchical to:	No other components.

[54][selection: allocation of the resource to, deallocation of the resource from]

[55][assignment: list of objects]

Dependencies: No dependencies.

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

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

FTP_ITC.1.3/PACE The TSF shall ~~initiate~~ **enforce** communication via the trusted channel ***for any data exchange between the TOE and the Terminal***.

PP0068v2 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.

PP0068v2 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_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

PP0068v2 application note 45: Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

6.2.5 Class FAU Security Audit

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

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

PP0068v2 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 (see FMT_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.

6.2.6 Class FMT Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

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

1. ***Initialization,***
2. ***Pre-personalization,***

3. ***Personalization,***
4. ***Configuration.***

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

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

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

PP application note 37: The SFR FMT_SMR.1.1/PACE in this ST covers the definition in PACE PP [PP0068v2] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

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.

PP0068v2 application note 47: For explanation on the role Manufacturer and Personalisation Agent please refer to the glossary of [PP0068v2]. The role Terminal is the default role for any terminal being recognised by the TOE as not PACE authenticated BIS-PACE (‘Terminal’ is used by the travel document presenter).

The TOE recognises the travel document holder or an authorised other person or device (BIS-PACE) by using PACE authenticated BIS-PACE (FIA_UAU.1/PACE).

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,***
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,***
5. ***sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.***

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:

Deploying Test Features after TOE Delivery does not allow

1. ***User Data to be manipulated,***
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,***
5. ***sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.***

PP application note 39: The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might 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 of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.

PP0068v2 application note 48: 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.

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.

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

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/
CVCA_INI

The TSF shall restrict the ability to ***write*** the

1. ***initial Country Verifying Certification Authority Public Key,***
2. ***initial Country Verifying Certification Authority Certificate,***
3. ***initial Current Date***
4. ***None***[56]

To **the Personalization Agent**[57].

PP application note 41:<applied>. 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.

[56][assignment: list of TSF data]

[57] [assignment: the authorised identified roles]

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/CVCA_UPD

The TSF shall restrict the ability to ***update*** the

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

to ***Country Verifying Certification Authority.***

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]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [TR-03110]).

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

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

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

PP application note 43: The authorized roles are identified in their certificate (cf. [TR-03110]) 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]).

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **load**[58] the ***Chip Authentication Private Key*** to **the Personalization Agent**[59]**.**

PP application note 44: <applied> The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. Thus according to PP application note 44 no additional key generation SFR is necessary.

---

[58] [selection: create, load]

[59] [assignment: the authorised identified roles]

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Prepersonalization Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/INI_ENA

The TSF shall restrict the ability to write ***the Initialization Data and Prepersonalization Data*** to ***the Manufacturer***.

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Prepersonalization Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/INI_DIS

The TSF shall restrict the ability to ***disable read access for users to*** the ***Initialization Data*** to ***the Personalization Agent***.

PP0068v2 application note 49: The TOE may restrict the ability to write the Initialisation Data and the Prepersonalisation 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/KEY_READ Management of TSF data – Key Read

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

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

1. ***PACE passwords,***
2. ***Chip Authentication Private Key,***
3. ***Personalization Agent Keys,***

to ***none***.

PP application note 45: The SFR FMT_MTD.1/KEY_READ in [PP0056v2] covers the definition in PACE PP [PP0068v2] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.

FMT_MTD.1/PAManagement of TSF data – Personalisation Agent

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

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

PP0068v2 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/AAManagement of TSF data – Active Authentication Private Key

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/AA The TSF shall restrict the ability to **create or load**[60] the **Active Authentication Private Key**[61] to the **Manufacturer and the Personalisation Agent**[62].

Application Note: This SFR has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in section 2.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

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 and the Access Control***.

Refinement: The certificate chain is valid if and only if

1. **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date ofthe Inspection System Certificate is not before the Current Date of the TOE,**
2. **the digital signature of the Document Verifier Certificate can be verified as correct´with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,**
3. **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.**

[60] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

[61] [assignment: list of TSF data]

[62] [assignment: the authorised identified roles]

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.

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.

PP application note 46: The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

6.2.7 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. With respect to the forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSFtesting (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFRs "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and"Resistance to physical attack (FPT_PHP.3)" together with the SAR "Security architecture-description" (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE security functionality.

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 timing during command execution**[63] in excess of **non-useful information**[64] 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. ***none***[65]
5. ***Personalization Agent Key(s),***
6. ***Chip Authentication Private Key***[66]***,***
7. ***Active Authentication Private Key***[67]***.***

FPT_EMS.1.2 The TSF shall ensure ***any users*** are unable to use the following interface: ***smart card circuit contacts*** **or contactless interface**[68] to gain access

[63] [assignment: types of emissions]

[64] [assignment: specified limits]

[65] [assignment: list of types of TSF data]

[66] [assignment: type of users]

[67] [assignment: list of types of user data]

[68] [refinement: type of connection]

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. **<u>none</u>**[69]
5. ***Personalization Agent Key(s),***
6. ***Chip Authentication Private Key***[70]***,***
7. **<u>Active Authentication Private Key</u>**[71]***.***

PP application note 47: The SFR FPT_EMS.1.1 in this ST covers the definition in PACE PP [PP0068v2] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in this ST covers the definition in PACE PP [PP0068v2] and extends it by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

PP application note 48: <applied>

PP0068v2 application note 51: 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 has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC7816-2 as well. 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.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: ***1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,*** ***2. Failure detected by TSF according to FPT_TST.1.*** ***3.* <u>None.</u>**[72]

FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests **<u>during initial start-up</u>**[73] to demonstrate the correct operation of ***the TSF***.

[69] [assignment: list of types of TSF data]

[70] [assignment: type of users]

[71] [assignment: list of types of user data]

[72] [assignment: list of types of failures in the TSF]

[73] [*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]*]

FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of ***TSF data***.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of ***stored TSF executable code***.

PP0068v2 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 calculation with aprivate key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

FPT_PHP.3 Resistance to physical attack

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

PP0068v2 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.

6.3 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 5 (EAL5)

and augmented by taking the following components:

ALC_DVS.2 and **AVA_VAN.5**.

PP application note 49: The TOE shall protect the assets against high attack potential under the assumption that the inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol v.1 (OE.Prot_Logical_MRTD). 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).

6.4 Security Requirements Rationale

6.4.1 Security Functional 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*	OT.Active_Auth_Proof
FAU_SAS.1[74]			X				X						
FCS_CKM.1/DH_PACE				X	X	X							
FCS_CKM.1/CA	X	X	X	X	X	X							
FCS_CKM.1/AA													X
FCS_CKM.4	X		X	X	X	X							
FCS_COP.1/PACE_ENC						X							
FCS_COP.1/PACE_MAC				X	X								
FCS_COP.1/CA_ENC	X	X	X	X		X							
FCS_COP.1/CA_MAC	X	X	X	X									
FCS_COP.1/SIG_VER	X		X										
FCS_COP.1/SIG_GEN													X
FCS_RND.1	X		X	X	X	X							
FIA_AFL.1/PACE										X			
FIA_API.1		X											
FIA_API.1/AA													X
FIA_UID.1/PACE[75]	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							
FDP_ACC.1/TRM	X		X	X		X							
FDP_ACF.1/TRM	X		X	X		X							
FDP_RIP.1				X	X	X							
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					
FMT_LIM.2								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									

[74] SFRs and security objectives from PACE PP [PP0068v2] are marked in italic letters.

[75] SFRs from PACE PP [PP0068v2] 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*	OT.Active_Auth_Proof
FMT_MTD.1/PA			X	X	X	X							
FMT_MTD.1/AA													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 13: Overview of the security functional requirements coverage.

This security target claims strict conformance to the Protection Profiles given insection 2.2. Therefore this security target includes the Security Requirements Rationale of the Protection Profiles as summarized above; for details on the Rationale please refer to the Protection Profiles [PP0056v2] and [PP0068v2].

The security objective **OT.Active_Auth_Proof** “Proof of travel document’s chipauthenticity” is ensured by the Active Authentication Mechanism [ICAODoc] provided by FIA_API.1/AA proving the identity of the TOE. The Active Authentication Protocol defined by FIA_API.1/AA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AA. This key can either be written to the TOE as defined by FMT_MTD.1/AA or created on the TOE itself as supported by FCS_CKM.1/AA. The Active Authentication Protocol requires additional TSF according to FCS_COP.1/SIG_GEN.

6.4.2 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.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies.	n.a.
FCS_CKM.1/DH_PACE	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Justification 2 for non-satisfied dependencies Fulfilled by FCS_CKM.4
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
FCS_CKM.1/AA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/SIG_GEN, Justification 3 for non-satisfied dependencies
FCS_CKM.4 from[PP0068v2]	[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.1/AA and FCS_CKM.1/CA
FCS_COP.1/PACE_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/DH_PACE, Fulfilled by FCS_CKM.4
FCS_COP.1/PACE_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/DH_PACE, Fulfilled by FCS_CKM.4

FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographickey generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA, Fulfilled by FCS_CKM.4
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
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
FCS_COP.1/SIG_GEN	[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/AA, See justification No. 3.
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1/PACE	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_UID.1/PACE	No dependencies	n.a.
FIA_UAU.1/PACE	FIA_UID.1 Timing ofidentfication	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	No dependencies	n.a.
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 accesscontrol, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM, Justification 1 for non-satisfied dependencies
FDP_RIP.1	No dependencies	n.a.
FDP_UCT.1/TRM	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FDP_UIT.1/TRM	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FMT_SMF.1	No dependencies	n.a.
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/INI_ENA	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE

FMT_MTD.1/ PA	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/AA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI andFMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	n.a.
FTP_ITC.1/PACE	No dependencies	n.a.

Table 14: Dependencies between the SFR for the TOE

Justifications 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.

No. 2: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.[76]

No. 3: The Active Authentication key pair cannot be deleted or regenerated.

6.4.3 Security Assurance Requirements Rationale

The EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices and a Java card platform that offers cryptographic functionality certified according to EAL5 or higher.

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

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

The component ALC_DVS.2 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.

[76] This justification was taken from [PP0068v2].

6.4.4 Security Requirements – Mutual Support and Internal Consistency

This security target claims strict conformance to the Protection Profiles given insection 2.2. Therefore this security target includes the analysis of the internal consistency of the Security Requirements of the Protection Profiles without repeating these here.

As the complete Security Problem Definition, the Extended Components and the Security Functional Requirements have also been included, the consistency analysis of the Protection Profiles is also valid for this security target.

The additions made to include the Active Authentication Mechansim have been integrated in a consistent way to the model designed by the Protection Profiles, e. g. by using the subject, object and operation definitions.

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 ofthese two groups of security requirements.

7 TOE summary specification (ASE_TSS)

7.1 TOE Security Functionality

7.1.1 TSF_Access: Access Control

This security functionality manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data. Access control for initialization and pre-personalization in Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying SmartCafe Expert 8.0 C2 Java Card platform (SF.APPLET).

Access is granted (or denied) in accordance to access rights that depend on appropriate identification and authentication mechanisms.

TSF_Access covers the following SFRs:

- FIA_UID.1.1/PACE requires that the TSF shall allow to establish the communication channel, to carry out the PACE Protocol, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to carry out the Chip Authentication Protocol, to carry out the Terminal Authentication Protocol, and to carry out the Active Authentication Mechanism on behalf of the user to be performed before the user is identified. FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights, TSF_Auth the authentication mechanisms.
- FIA_UAU.1/PACE requires that the TSF shall allow to establish the communication channel, to carry out the PACE Protocol, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to identify themselves by selection of the authentication key, to carry out the Chip Authentication Protocol, to carry out the Terminal Authentication Protocol, and to carry out the Active Authentication Mechanism on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.4/PACE requires that the TSF shall prevent reuse of authentication data related to the PACE Protocol, the Terminal Authentication Protocol, and the Authentication Mechanism based on AES. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.5.1/PACE requires that the TSF shall provide the PACE Protocol, Passive Authentication, Terminal Authentication, Secure messaging in MAC-ENC mode, Symmetric Authentication Mechanism based on AES, and the Terminal Authentication Protocol to support user authentication. FIA_UAU.5.2/PACE requires that the TSF shall authenticate any user's claimed identity according to specified rules. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.6/PACE requires that the TSF shall re-authenticate the user under the condition that each command sent to the TOE after successful run of the PACE Protocol shall be verified as being sent by the terminal. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.6/EAC requires that the TSF shall re-authenticate the user under the condition that each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the Inspection System. TSF_Access realizes the appropriate control of the access rights.
- FDP_ACC.1/TRM requires that the TSF shall enforce the Access Control SFP on terminals gaining access to the User data and data stored in EF.Sod of the logical travel document.. TSF_Access realizes the appropriate control of the access rights.

- FDP_ACF.1/TRM: FDP_ACF.1.1 requires that the TSF shall enforce the Access Control SFP to objects based on Subjects (Terminal,BIS-PACE, Extended Inspection System), Objects (data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical MRTD, data in EF.DG3 of the logical MRTD, data in EF.DG4 of the logical MRTD, all TOE intrinsic secret cryptographic keys stored in the travel document) and Security attributes (PACE Authentication,Terminal Authentication v.1,Authorization of the Terminal). FDP_ACF.1.2 requires that the TSF shall enforce the following rules to determine if an operation among con-trolled subjects and controlled objects is allowed: a BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [TR-03110] after a successful PACE authentication as required by FIA_UAU.1/PACE. FDP_ACF.1.3 requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. FDP_ACF.1.4 requires that the TSF shall explicitly deny access of subjects to objects based on the 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.TSF_Access realizes the appropriate control of the access rights.
- FDP_UCT.1/TRM requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure. TSF_Access realizes the appropriate control of the access rights.
- FDP_UIT.1/TRM requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors. FDP_UIT.1.2 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred. TSF_Access realizes the appropriate control of the access rights.
- FMT_SMR.1/PACE requires that the TSF shall maintain the roles (1.) Manufacturer, (2.) Personalization Agent, (3) Terminal, (4) PACE authenticated BIS-PACE, (5) Country Verifying Certification Authority, (6) Document Verifier, (7) Domestic Extended Inspection System, (8) Foreign Extended Inspection System. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. TSF_Access realizes the appropriate control of the access rights.
- FMT_LIM.1 requires that 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, (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, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed. This is realized by TSF_Access.
- FMT_LIM.2 requires that the TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be manipulated, (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, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed. This is realized by TSF_Access.

- FMT_MTD.1.1/CVCA_INI requires that the TSF shall restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Date to the Personalization Agent. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/CVCA_UPD requires that the TSF shall restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/DATE requires that the TSF shall restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/CAPK requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the (1.) PACE passwords, the (2.) Chip Authentication Private Key, and the (3.) Personalization Agent Keys to none. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1/AA requires that the TSF shall restrict the ability to create or load the Active Authentication Private Key to the Manufacturer and the Personalisation Agent. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1/PA requires that the TSF shall restrict the ability to write the Document Security Object (SOD) to the Personalisation Agent. TSF_Access realizes the appropriate control of the access rights.
- FIA_AFL.1/PACE requires that the TOE shall detect when 10 unsuccessful authentication attempts have occured related to authentication attempts using the PACE password, and that there shall be an delay by an increasing amount of time after each of the following authentication attempt until the next successful authentication attempt has happened. This is realized by TSF_Access.
- FTP_ITC.1/PACE: FTP_ITC.1.1/PACE requires that the TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure; FTP_ITC.1.2/PACE requires that the TSF shall permit another trusted IT product to initiate communication via the trusted channel, and FTP_ITC.1.3/PACE requires that the TSF shall initiate enforce communication via the trusted channel for any data exchange between the TOE and the Terminal. The according access rights are realized by TSF_Access.

7.1.2 TSF_Admin: Administration

This Security Functionality manages the storage of manufacturing data, pre-personalization data and personalization data. This storage area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Management of manufacturing and pre-personalization data in Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying Java Card platform (SF.APPLET and SF.CARRIER). During Operational Use phase, read access is only possible after successful authentication.

TSF_Admin covers the following SFRs:

- FAU_SAS.1: FAU_SAS.1 requires that the TSF shall provide the Manufacturer with the capability to store the Initialisation and Pre-Personalisation Data in the audit records. This is realized by TSF.Admin.

- FMT_SMF.1: FMT_SMF.1.1 requires that the TSF shall be capable of performing the following management functions: (1.) Initialization, (2.) Pre-personalization, (3.) Personalization, (4.) Configuration. This is realized within TSF_Admin.
- FMT_SMR.1/PACE requires that the TSF shall maintain the roles (1.) Manufacturer, (2.) Personalization Agent, (3) Terminal, (4) PACE authenticated BIS-PACE, (5) Country Verifying Certification Authority, (6) Document Verifier, (7) Domestic Extended Inspection System, (8) Foreign Extended Inspection System. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. This is realized within TSF_Admin.
- FMT_LIM.1 requires that 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, (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, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed. This is realized by TSF_Admin.
- FMT_LIM.2 requires that the TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be manipulated, (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, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed. This is realized by TSF_Admin.
- FMT_MTD.1.1/CVCA_INI requires that the TSF shall restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Dateto the Personalization Agent. This is realized within TSF_Admin.
- FMT_MTD.1.1/CVCA_UPD requires that the TSF shall restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority. This is realized within TSF_Admin.
- FMT_MTD.1.1/DATE requires that the TSF shall restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System. This is realized within TSF_Admin.
- FMT_MTD.1.1/CAPK requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. This is realized within TSF_Admin.
- FMT_MTD.1/AA requires that the TSF shall restrict the ability to create or load the Active Authentication Private Key to the Manufacturer and the Personalisation Agent. This is realized within TSF_Admin.
- FMT_MTD.1/PA requires that the TSF shall restrict the ability to write the Document Security Object (SOD) to the Personalisation Agent. This is realized within TSF_Admin.

7.1.3 TSF_Secret: Secret key management

This Security Functionality ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These functions make use of SF.SECURITY of the underlying Java Card OS.

TSF_Secret covers the following SFRs:

- FMT_MTD.1.1/CAPK requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. This is realized by TSF_Admin, TSF_Access and TSF_OS. This is realized within TSF_Secret.

- FMT_MTD.1/KEY_READ requires that the TSF shall restrict the ability to read (1.) the PACE passwords, (2.) the Chip Authentication Private Key, and (3.) the Personalization Agent Keys to none. This is realized within TSF_Secret.
- FMT_MTD.1/PA requires that the TSF shall restrict the ability to write the Document Security Object (SOD) to the Personalisation Agent. This is realized within TSF_Secret.
- FMT_MTD.1/AA requires that the TSF shall restrict the ability to create or load the Active Authentication Private Key to the Manufacturer and the Personalisation Agent. This is realized within TSF_Secret.

7.1.4 TSF_Crypto: Cryptographic operations

This Security Functionality performs high level cryptographic operations. The implementation is based on the Security Functionalities provided by TSF_OS.

TSF_Crypto covers the following SFRs:

- FCS_CKM.1/DH_PACE and FCS_CKM.1/CA require that the TSF shall generate cryptographic keys based on ECDH compliant to ISO 15946 with specific domain parameters, meeting [TR-03110], Annex A.1, or DH based on the Diffie-Hellman key derivation protocol compliant to [PKCS#3] and [TR-03110]. This is realized within TSF_Crypto (Diffie-Hellman) and TSF_OS (ECDH).
- FCS_CKM.1/AA requires that the TSF shall provide RSA CRT key generation compliant with [ISO9796-2]. This is realized within TSF_OS. This is realized in the security functionalities provided by TSF_Crypto based on the functionality of TSF_OS.
- FCS_CKM.4: FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys by method (e.g. clearKey of [Java_RES]) or automatically on applet deselection. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FDP_RIP.1 requires that any previous information about specific keys is made unavailable upon the deallocation of the resource. This is realized in the security functionality provided by TSF_Crypto by using key objects as provided by TSF_OS.
- FCS_COP.1/PACE_MAC requires that the TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm: CMAC and cryptographic key size 128, 192, 256 bit, or Retail-MAC and cryptographic key size 112 bit. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FCS_COP.1/PACE_ENC requires that the TSF shall shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm: AES in CBC mode and cryptographic key size 128, 192, 256 bit, or 3DES in CBC mode and cryptographic key size 112 bit. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FCS_COP.1/CA_ENC requires that the TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm: AES and cryptographic key size 128, 192, 256 bit , or 3DES in CBC mode and cryptographic key size 112 bit. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FCS_COP.1/CA_MAC requires that the TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm: CMAC and cryptographic key size 128, 192 and 256 bit, or Retail-MAC and cryptographic key size 112 bit. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FCS_COP.1.1/SIG_VER requires that the TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm: ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 and specified elliptic curves and cryptographic key sizes of 224, 256, 320, 384, 512, or 521 bit, respectively that meet the following: [ISO15946]. This is realized within TSF_Crypto and TSF_OS.

FCS_COP.1.1/SIG_VER also requires that the TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm: RSASSA-PSS with SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 and specified elliptic curves and cryptographic key sizes 1024, 1280, 1536, 1984, 2048, 4096 bit, that meet the following: [PKCS1]. This is realized within TSF_Crypto and TSF_OS.

- FCS_COP.1/SIG_GEN requires that the TSF shall perform digital signature generation in accordance with RSA with cryptographic key sizes of 1024, 1280, 1536, 1984, 2048, 4096 bit, or ECDSA with key sizes of 224, 256, 320, 384, 512, or 521 bit and specified elliptic curves. This is realized within TSF_Crypto and TSF_OS.
- FIA_API.1.1/AA requires that the TSF shall provide the Active Authentication Mechanisms according to [ICAODoc] to prove the identity of the TOE. This is provided by TSF_Crypto (based on SFR FCS_COP.1/SIG_GEN).
- FIA_UAU.1.1/PACE requires that the TSF shall allow to establish the communication channel, to carry out the PACE Protocol, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to identify themselves by selection of the authentication key, to carry out the Chip Authentication Protocol, to carry out the Terminal Authentication Protocol, and to carry out the Active Authentication Mechanism on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. Active Authentication is provided by TSF_Crypto.
- FIA_UAU.5.1/PACE requires that the TSF shall provide the PACE Protocol, Passive Authentication, Terminal Authentication, Secure messaging in MAC-ENC mode, Symmetric Authentication Mechanism based on AES, and the Terminal Authentication Protocol to support user authentication. FIA_UAU.5.2/PACE requires that the TSF shall authenticate any user’s claimed identity according to specified rules. TSF_Crypto adds parts of the cryptographic implementation.

7.1.5 TSF_ SecureMessaging: Secure Messaging

This Security Functionality realizes a secure communication channel after successful authentication for personalization and after successful PACE protocol and chip authentication during operational use. Please note that SFRs of the FCS_COP group are realized within TSF_Crypto, even if they are used by TSF_SecureMessaging.

TSF_SecureMessaging covers the following SFRs:

- FIA_UAU.5.1/PACE requires that the TSF shall provide the PACE Protocol, Passive Authentication, Terminal Authentication, Secure messaging in MAC-ENC mode, Symmetric Authentication Mechanism based on AES, and the Terminal Authentication Protocol to support user authentication. FIA_UAU.5.2/PACE requires that the TSF shall authenticate any user’s claimed identity according to specified rules.TSF_SecureMessaging provides the secure messaging mechanism.
- FDP_UIT.1/TRM requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors. FDP_UIT.1.2 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred. TSF_SecureMessaging provides the protected communication.
- FTP_ITC.1/PACE: FTP_ITC.1.1/PACE requires that the TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure; FTP_ITC.1.2/PACE requires that the TSF shall permit another trusted IT product to initiate communication via the trusted channel, and FTP_ITC.1.3/PACE re-

quires that the TSF shall initiate enforce communication via the trusted channel for any data exchange between the TOE and the Terminal. The according secure messaging is realized by TSF_ SecureMessaging.

7.1.6 TSF_Auth: Authentication protocols

This security functionality realizes different authentication mechanisms.

7.1.6.1 TSF_Auth_Term

TSF_Auth_Term performs the Terminal Authentication to authenticate the terminal (EAC). TSF_Auth_Term covers the following SFRs:

- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide Terminal Authentication Protocol, Secure messaging in MAC-ENC mode, and Symmetric Authentication Mechanism based on AES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user's claimed identity according to specified rules. The authentication mechanisms are provided by TSF_Auth_Term.
- FIA_UID.1.1/PACE requires that the TSF shall allow to establish the communication channel, to carry out the PACE Protocol, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to carry out the Chip Authentication Protocol, to carry out the Terminal Authentication Protocol, and to carry out the Active Authentication Mechanism on behalf of the user to be performed before the user is identified. FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights, TSF_Auth the authentication mechanisms.
- FDP_ACC.1/TRM requires that the TSF shall enforce the Access Control SFP on terminals gaining access to the User data and data stored in EF.Sod of the logical travel document TSF_Access realizes the appropriate control of the access rights.. The authentication mechanism is provided by TSF_Auth_Term.
- FDP_ACF.1/TRM: FDP_ACF.1.1 requires that the TSF shall enforce the Access Control SFP to objects based on Subjects (Terminal,BIS-PACE, Extended Inspection System), Objects (data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical MRTD, data in EF.DG3 of the logical MRTD,data in EF.DG4 of the logical MRTD, all TOE intrinsic secret cryptographic keys stored in the travel document) and Security attributes (PACE Authentication,Terminal Authentication v.1,Authorization of the Terminal).FDP_ACF.1.2 requires that the TSF shall enforce the following rules to determine if an operation among con-trolled subjects and controlled objects is allowed: a BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [TR-03110] after a successful PACE authentication as required by FIA_UAU.1/PACE. FDP_ACF.1.3 requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. FDP_ACF.1.4 requires that the TSF shall explicitly deny access of subjects to objects based on the 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 ob-jects 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. This is realized within TSF_Auth_Term.

- FIA_UAU.5.1/PACE requires that the TSF shall provide the PACE Protocol, Passive Authentication, Terminal Authentication, Secure messaging in MAC-ENC mode, Symmetric Authentication Mechanism based on AES, and the Terminal Authentication Protocol to support user authentication. FIA_UAU.5.2/PACE requires that the TSF shall authenticate any user's claimed identity according to specified rules.TSF_Auth_Term provides the Terminal Authentication.
- FMT_MTD.3.1 requires that the TSF shall ensure that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control. This is realized by TSF_Auth_Term. The refinement to FMT_MTD.3.1 requires that the certificate chain is valid if and only if
  - the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,
  - the digital signature of the Document Verifier Certificate can be verified as correct´with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,
  - the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

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

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

  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.

  This is realized by TSF_Auth_Term.
- FTP_ITC.1/PACE: FTP_ITC.1.1/PACE requires that the TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure; FTP_ITC.1.2/PACE requires that the TSF shall permit another trusted IT product to initiate communication via the trusted channel, and FTP_ITC.1.3/PACE requires that the TSF shall initiate enforce communication via the trusted channel for any data exchange between the TOE and the Terminal. The according terminal authentication is realized by TSF_Auth_Term.

7.1.6.2 TSF_Auth_Sym

TSF_Auth_Sym performs an authentication mechanism based on AES used for symmetric authentication with pre-shared keys for personalization and the PACE authentication. TSF_Auth_Sym covers the following SFRs:

- FDP_ACF.1: FDP_ACF.1.1 requires that the TSF shall enforce the Access Control SFP to objects based on subjects (Personalization Agent, Extended Inspection System, Terminal), objects (data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, data EF.DG3 and EF.DG4 of the logical MRTD, data in EF.COM, data in EF.SOD), and security attributes (authentication status of terminals, Terminal Authorization). FDP_ACF.1.2 requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD, (2.) the successfully authenticated Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD, and (3.) the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD. FDP_ACF.1.3 requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. FDP_ACF.1.4 requires that he TSF shall explicitly deny access of subjects to objects based on the rules: (1.) A terminal authenticated as CVCA is not allowed to read data in the EF.DG3, (2.) A terminal authenticated as CVCA is not allowed to read data in the EF.DG4, (3.) A terminal authenticated as DV is not allowed to read data in the EF.DG3, (4.) A terminal authenticated as DV is not allowed to read data in the EF.DG4, (5.) Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logi-cal MRTD, (6.) Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD. The authentication mechanism for the Access Control SFP is provided by TSF_Auth_Sym.

- FIA_UAU.5.1/PACE requires that the TSF shall provide the PACE Protocol, Passive Authentication, Terminal Authentication, Secure messaging in MAC-ENC mode, Symmetric Authentication Mechanism based on AES, and the Terminal Authentication Protocol to support user authentication. FIA_UAU.5.2/PACE requires that the TSF shall authenticate any user's claimed identity according to specified rules. TSF_Auth_Sym realizes the symmetric authentication mechanism.
- FMT_MTD.1.1/CVCA_INI requires that the TSF shall restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Date to the Personalization Agent. The authentication mechanism is provided by TSF_Auth_Sym.
- FMT_MTD.1.1/CVCA_UPD requires that the TSF shall restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority. The authentication mechanism is provided by TSF_Auth_Sym.
- FMT_MTD.1.1/DATE requires that the TSF shall restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System. The authentication mechanism is provided by TSF_Auth_Sym.
- FMT_MTD.1.1/CAPK requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. The authentication mechanism is provided by TSF_Auth_Sym.

7.1.6.3 TSF_Auth_Chip

This security functionality manages the capability of the TOE to authenticate itself to the terminal using the Chip Authentication Protocol (EAC). TSF_Auth_Chip covers the following SFRs:

- FIA_UID.1.1/PACE requires that the TSF shall allow to establish the communication channel, to carry out the PACE Protocol, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to carry out the Chip Authentication Protocol, to carry out the Terminal Authentication Protocol, and to carry out the Active Authentication Mechanism on behalf of the user to be performed before the user is identified. FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights, TSF_Auth the authentication mechanisms.
- FIA_UAU.1.1/PACE requires that the TSF shall allow to establish the communication channel, to carry out the PACE Protocol, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to identify themselves by selection of the authentication key, to carry out the

Chip Authentication Protocol, to carry out the Terminal Authentication Protocol, and to carry out the Active Authentication Mechanism on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. The chip authentication mechanism is provided by TSF_Auth_Chip.

- FIA_UAU.6/EAC requires that the TSF shall re-authenticate the user under the condition that each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the Inspection System. The authentication mechanism is provided by TSF_Auth_Chip.
- FIA_API.1.1 requires that the TSF shall provide a Chip Authentication Protocol according to [TR-03110] to prove the identity of the TOE. This is provided by TSF_Auth_Chip.
- FDP_UCT.1/TRM: FDP_UCT.1.1 requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure after Chip Authentication. The authentication mechanism is provided by TSF_Auth_Chip.
- FDP_UIT.1/TRM: FDP_UIT.1.1 requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication. FDP_UIT.1.2 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred after Chip Authentication. The authentication mechanism for the Access Control SFP is provided by TSF_Auth_Chip.

7.1.6.4 TSF_Auth_PACE

This Security Functionality provides the PACE protocol.

- FIA_UID.1.1/PACE requires that the TSF shall allow to establish the communication channel, to carry out the PACE Protocol, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to carry out the Chip Authentication Protocol, to carry out the Terminal Authentication Protocol, and to carry out the Active Authentication Mechanism on behalf of the user to be performed before the user is identified. FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights, TSF_Auth_PACE the PACE mechanism.
- FIA_UAU.1.1/PACE requires that the TSF shall allow to establish the communication channel, to carry out the PACE Protocol, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to identify themselves by selection of the authentication key, to carry out the Chip Authentication Protocol, to carry out the Terminal Authentication Protocol, and to carry out the Active Authentication Mechanism on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. The PACE protocol is provided by TSF_Auth_PACE.
- FIA_UAU.5.1/PACE requires that the TSF shall provide the PACE Protocol, Passive Authentication, Terminal Authentication, Secure messaging in MAC-ENC mode, Symmetric Authentication Mechanism based on AES, and the Terminal Authentication Protocol to support user authentication. FIA_UAU.5.2/PACE requires that the TSF shall authenticate any user's claimed identity according to specified rules. TSF_Auth_PACE realizes the PACE protocol.
- FIA_UAU.6/PACE requires that the TSF shall re-authenticate the user under the condition that each command sent to the TOE after successful run of the PACE Protocol shall be verified as being sent by the terminal. This is provided by TSF_Auth_PACE.

7.1.7 TSF_Integrity: Integrity protection

This Security Functionality protects the integrity of internal applet data like the Access control lists. This function makes use of SF.INTEGRITY of the underlying Java Card OS.

TSF_Integrity covers the following SFRs:

- FPT_FLS.1 requires that the TSF shall preserve a secure state when the following types of failures occur: (1) exposure to out-of-range operating conditions where therefore a malfunction could occur, and (2) failure detected by TSF according to FPT_TST.1. This is realized within TSF_Integrity.

7.1.8 TSF_OS: Javacard OS Security Functionalities

The Javacard operation system (part of the TOE) features the following Security Functionalities. The exact description can be found in the Javacard OS security target [ST_SmartCafe]; the realization is partly based on the security functionalities of the certified cryptographic library and the certified IC platform:

- Enforcement of access control (SF.AccessControl)
- Audit functionality (SF.Audit)
- Cryptographic key management (SF.CryptoKey)
- Cryptographic operations (SF.CryptoOperation)
- Identification and authentication (SF.I&A)
- Secure management of TOE resources (SF.SecureManagement)
- Transaction management (SF.Transaction)

Since the applet layer of the TOE is based on the Javacard OS, the realization of all TOE security functionalities and thus the fulfillment of all SFRs has dependencies to TSF_OS. The following items list all SFRs where TSF_OS has an impact above this level:

- FCS_CKM.1/AA requires that the TSF shall provide RSA key generation with cryptographic key sizes 1024, 1280, 1536, 1984, 2048, 4096 bit, or ECDSA key generation with key sizes of 224, 256, 320, 384, 512, or 521 bit. This is realized in the security functionalities provided by TSF_Crypto based on the functionality of TSF_OS.
- FCS_CKM.1/DH_PACE and FCS_CKM.1/CA require that the TSF shall generate cryptographic keys based on ECDH compliant to ISO 15946 with specific domain parameters, meeting [TR-03110], Annex A.1, or DH based on the Diffie-Hellman key derivation protocol compliant to [PKCS#3] and [TR-03110]. This is realized in the security functionalities provided by TSF_Crypto based on the functionality of TSF_OS.
- FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FDP_RIP.1 requires that any previous information about specific keys is made unavailable upon the deallocation of the resource. This is realized in the security functionality provided by TSF_OS.
- FCS_COP.1/PACE_ENC requires that the TSF shall shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm: AES in CBC mode and cryptographic key size 128, 192, 256 bit, or 3DES in CBC mode and cryptographic key size 112 bit. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FCS_COP.1/PACE_MAC requires that the TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm: CMAC and cryptographic key size 128, 192, 256 bit, or Retail-MAC and cryptographic key size 112 bit. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.

- FCS_COP.1/CA_ENC requires that the TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm: AES and cryptographic key size 128, 192, 256 bit, or 3DES in CBC mode and cryptographic key size 112 bit. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FCS_COP.1/CA_MAC requires that the TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm: CMAC and cryptographic key size 128, 192 and 256 bit, or Retail-MAC and cryptographic key size 112 bit. This is realized by TSF_Crypto using the security functionality provided by TSF_OS.
- FCS_COP.1.1/SIG_VER requires that the TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm: RSASSA-PSS or ECDSA, each with SHA-1, SHA-224, SHA-256, SHA-384, or SHA512 and specified elliptic curves and cryptographic key sizes of 1024, 1280, 1536, 1984, 2048, 4096 bit or 224, 256, 320, 384, 512, or 521 bit, respectively that meet the following: [PKCS1], or [ISO15946]. This is realized within TSF_Crypto and TSF_OS.
- FCS_COP.1/SIG_GEN requires that the TSF shall perform digital signature generation in accordance with RSA or ECDSA and cryptographic key sizes of 1024, 1280, 1536, 1984, 2048, 4096 bit or 224, 256, 320, 384, 512, or 521 bit. This is realized within TSF_Crypto and TSF_OS.
- FCS_RND.1: FCS_RND.1.1 requires that the TSF shall provide a mechanism to generate random numbers that meet the AIS 20 Class DRG.3 quality metric. This is realized within TSF_OS.
- FMT_LIM.1 requires that 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, (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, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed. This is realized by TSF_OS.
- FMT_LIM.2 requires that the TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be manipulated, (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, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed. This is realized by TSF_OS.
- FMT_MTD.1.1/INI_ENA requires that the TSF shall restrict the ability to write the Initialization Data and Prepersonalization Data to the Manufacturer. This is realized by TSF_OS.
- FMT_MTD.1.1/INI_DIS requires that the TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent. This is realized by TSF_OS.
- FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the (1.) PACE passwords the (2.) Chip Authentication Private Key, and the (3.) Personalization Agent Keys to none. This is realized by TSF_OS.
- FPT_EMS.1: FPT_EMS.1.1 requires that the TOE shall not emit variations in power consumption or timing during command execution in excess of non-useful information enabling access to (1) Chip Authentication Session Keys, (2) PACE Session Keys (PACE-KMAC, PACE-KENC), (3) the ephemeral private key ephem SKPICC-PACE, (4) none, (5) Personalization Agent Key(s), (6) Chip Authentication Private Key, (7) Active Authentication Private Key. FPT_EMS.1.2 requires that the TSF shall ensure any users are unable to use the following interface: smart card circuit contacts or contactless interface to gain access to (1) Chip Authentication Session Keys, (2) PACE Session Keys (PACE-KMAC, PACE-KENC), (3) the ephemeral private key ephem SKPICC-PACE, (4) none, (5) Personalization Agent Key(s), (6) Chip Authentication Private Key, (7) Active Authentication Private Key. This is mainly realized by appropriate measures in TSF_OS together with the strict following of the security implementation guidelines of the Javacard platform.

- FPT_FLS.1.1 requires that the TSF shall preserve a secure state when the following types of failures occur: (1) exposure to out-of-range operating conditions where therefore a malfunction could occur, and (2) failure detected by TSF according to FPT_TST.1. This is realized within TSF_OS (together with TSF_Integrity).
- FPT_TST.1.1 requires that the TSF shall run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF. FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data. FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.
- FPT_PHP.3.1 requires that the TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.

7.2 TOE summary specification rationale

This summary specification shows that the TSF and assurance measures are appropriateto fulfill the TOE security requirements.

Each TOE security functional requirement is implemented by at least one security functionality. The mapping of TOE Security Requirements and TOE Security Functionalities isgiven in the following table. If iterations of a TOE security requirement are covered by the same TOE security functionality the mapping will appear only once. The description of the TSF is given in section 7.1.

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth	TSF_Integrity	TSF_OS
FAU_SAS.1		x						
FCS_CKM.1/AA				x				x
FCS_CKM.1/CA				x				x
FCS_CKM.1/DH_PACE				x				x
FCS_CKM.4				x				x
FCS_COP.1/CA_ENC				x				x
FCS_COP.1/CA_MAC				x				x
FCS_COP.1/PACE_ENC				x				x
FCS_COP.1/PACE_MAC				x				x
FCS_COP.1/SIG_VER				x				x
FCS_COP.1/SIG_GEN				x				x
FCS_RND.1								x
FIA_UID.1/PACE	x			x		x		
FIA_UAU.1/PACE	x					x		

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth	TSF_Integrity	TSF_OS
FIA_UAU.4/PACE	x							
FIA_UAU.5/PACE	x			x	x	x		
FIA_UAU.6/PACE	x					x		
FIA_UAU.6/EAC	x					x		
FIA_AFL.1/PACE	x							
FIA_API.1						x		
FIA_API.1/AA				x				
FDP_ACC.1/TRM	x					x		
FDP_ACF.1/TRM	x					x		
FDP_RIP.1				x				x
FDP_UCT.1/TRM	x					x		
FDP_UIT.1/TRM	x				x	x		
FMT_SMF.1		x						
FMT_SMR.1/PACE	x	x						
FMT_LIM.1	x	x						x
FMT_LIM.2	x	x						x
FMT_MTD.1/INI_ENA								x
FMT_MTD.1/INI_DIS								x
FMT_MTD.1/CVCA_INI	x	x				x		
FMT_MTD.1/CVCA_UPD	x	x				x		
FMT_MTD.1/DATE	x	x				x		
FMT_MTD.1/AA	x	x	x					
FMT_MTD.1/CAPK	x	x	x			x		
FMT_MTD.1/KEY_READ	x		x					x
FMT_MTD.1/PA	x	x	x					
FMT_MTD.3						x		
FPT_EMS.1								x
FPT_FLS.1							x	x
FPT_TST.1								x
FPT_PHP.3								x
FTP_ITC.1/PACE	x				x	x		

Table 15: Mapping of TOE Security Requirements and TOE Security Functionalities. Please note that TSF_Auth is a generic classification containing TSF_Auth_Term, TSF_Auth_Sym, TSF_Auth_Chip, and TSF_Auth_PACE.

8 References

In the following tables, the references used in this document are summarized.

Common Criteria

[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017; CCMB-2017-04-001.
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-002.
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-003.
[CC_4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017; CCMB-2017-04-004.

Protection Profiles

[PP0056v2]	Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), Version 1.3.2, 5.12.2012, BSI-CC-PP-0056-V2-2012, Bundesamt für Sicherheit in der Informationstechnik.
[PP0068v2]	Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22.7.2014, BSI-CC-PP-0068-V2-2011-MA-01, Bundesamt für Sicherheit in der Informationstechnik.
[PP0084]	Security IC Platform Protection Profile, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014.
[PP0055]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March 2009.
[PP_Javacard]	Java Card System - Open Configuration Protection Profile, April 2020, Version 3.1, Oracle Corporation

TOE and Platform References

[ST_SmartCafe]	SmartCafe Expert 8.0 C2 Veridos Security Target, Version 4.2/Status 03.08.2023
[ZertSmartCafe]	Certification Report SmartCafé Expert 8.0 C2, NSCIB-CC-2300005-01-CR, 24 May 2023 with Assurance Continuity Maintenance Report SmartCafé Expert 8.0 C2, NSCIB-CC-2300005-01-MA, 18 September 2023.
[ST_IC]	Security Target BSI-DSZ-CC-1107-V3-2022 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11, Security Target Lite, v4.3.1, 2022-05-10, Infineon
[ZertIC]	Certification report BSI-DSZ-CC-1107-V3-2022 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h,

	IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0 & 80.306.16.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACL v3.33.003 and v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and guidance from Infineon Technologies AG, 16.5.2022, BSI
[Guidance_PRE]	Veridos Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC); Preparation Guidance (AGD_PRE). For the exact version please refer to the certification report.
[Guidance_OPE]	Veridos Suite v4.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC); Operational Guidance (AGD_PRE). For the exact version please refer to the certification report.
[Guidance_GEN]	Veridos Suite v4.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications; Guidance Manual. For the exact version please refer to the certification report.
[GP_CIC]	GlobalPlatform Card Common Implementation Configuration Version 1.0, February 2014
[AGD_PRE]	Preparative Procedures SmartCafe Expert 8.0 C2, Tbd.

ICAO specifications

[ICAODoc]	ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization
[ICAO_SAC]	International Civil Avation Organisation, ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 11, 2010

Cryptography

[TR-03110]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 20.03.2012[77]
[TR-ECC]	Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.
[ISO7816-4]	ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004
[AIS20]	Anwendungshinweise und Interpretationen zum Schema (AIS); AIS 20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[77] This document version superseded by a newer one, but the one that is cited in the Protection Profile PP0056v2.

[AIS31]	Anwendungshinweise und Interpretationen zum Schema, AIS 31: Funk-tionalitäts-klassen und Evaluationsmethodologie für physikalische Zufalls-zahlengeneratoren, Version 3, Stand:15.05.2013
[ISO14888-3]	ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures withappendix – Part 3: Certificate-based mechanisms, 1999
[FIPS46-3]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S.DEPARTMENT OF COMMERCE/National Institute of Standards and Technlogy
[NIST800-20]	NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999
[FIPS180-2]	Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD(+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/NationalInstitute of Standards and Technology, 2002 August 1
[FIPS180-4]	Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD (SHS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, March 2012
[FIPS197]	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTIONSTANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standardsand Technology, November 26, 2001
[ANSIX9.19]	ANSI X9.19, AMERICAN NATIONAL STANDARD, Financial Institution Retail Message Authentication, 1996
[ANSIX9.62]	AMERICAN NATIONAL STANDARD X9.62-1999: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),September 20, 1998
[ISO9796-2]	ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002
[ISO15946]	ISO/IEC 15946. Information technology – Security techniques – Cryptographic techniques based on elliptic curves, 2002.
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[ISO18013-3]	ISO/IEC 18013-3:2009 Information technology -- Personal identification -- ISO-compliant driving licence -- Part 3: Access control, authentication and integrity validation (2009)
[NIST800-38A]	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A, National Institute of Standards and Technology, December 2001
[NIST800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005
[RFC4493]	Request for Comments: 4493, The AES-CMAC Algorithm, JH. Song et al. University of Washington, Category: Informational, June 2006
[ISO11770-3]	ISO/IEC 11770 Part 3: Information technology- Security techniques - Key management: Mechanisms using asymmetric techniques

[Brainpool]	RFC 5639 ECC Brainpool Standard Curves & Curve Generation, March 2010; available at:http://tools.ietf.org/html/rfc5639
[FIPS186-3]	Digital Signature Standard (DSS) - FIPS PUB 186-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, June 2009.[78]
[PKCS1]	PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note Version 2.1
[TR-03111]	Technical Guideline TR-03111: Elliptic Curve Cryptography; BSI, Version 2.0, 28.6.2012

[78] This document version was superseded by a newer one, but the one that is cited in the Protection Profile PP0056v2.

Glossary

Active authentication	Security mechanism defined in [ICAODoc] 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.
AES	The AES (Advanced Encryption Standard) has been defined as a standard for symmetric data encryption. It is a block cipher with a block length of 128 bit and key lengths of 128, 192 and 256 bit.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Asymmetric cipher	Encryption procedures employing two different keys (in contrast to a symmetric cipher): one publicly known (public key) for data encryption and one key only known to the message receiver (private key) for decryption.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authentication	Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures.
BAC	Basic access control. Security mechanism defined in [ICAODoc] by which means the MTRD's chip proves and the inspection system protects their communication by means of secure messaging.
Basic access keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [ICAODoc]. 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.
Block cipher	An algorithm processing the plaintext in bit groups (blocks). Its alternative is called stream cipher.
CA	Certification authority
Certificate	see digital certificate
Certificate revocation list	A list of revoked certificates issued by a certificate authority
Certification authority	An entity responsible for registering and issuing, revoking and generally managing digital certificates
Country signing CA certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority. The C_{CSCA} is stored in the inspection system.
Country verifying CA	The country specific root of the PKI of Inspection Systems. It creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing country or organization in respect to the protection of sensitive biometric data stored in the MRTD.
CRL	see Certificate Revocation List
Cryptography	In the classical sense, the science of encrypting messages. Today, this notion comprises a larger field and also includes problems like authentication or digital signatures.

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.
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.
DES	(Data Encryption Standard) symmetric 64 bit block cipher, which was developed (first under the name Lucifer) by IBM. The key length is 64 bit of which 8 bit serve for a parity check. DES is the classic among the encryption algorithms, which nevertheless is no longer secure due to its insufficient key length. Alternatives are Triple-DES or the successor AES.
Digital certificate	A data set that identifies the certification authority issuing it, identifies its owner, contains the ower's public key, identifies its operational period, and is digitally signed by the certification authority issuing it.
Digital signature	The counterpart of a handwritten signature for documents in digital format. A digital signature grants authentication, integrity, and non-repudiation. These features are achieved by using asymmetric procedures.
Document verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations
EAC	Extended access control. Security mechanism identified in [ICAODoc]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.
ECC	(Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.
Elliptic curves	A mathematical construction, in which a part of the usual operations applies, and which has been employed successfully in cryptography since 1985.
Fingerprint (digital)	Checksum that can be used to easily determine the correctness of a key without having to compare the entire key. This is often done by comparing the hash values after application of a hash function.
Hash function	A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value. Common hash functions are RIPEMD-160 and SHA-1, each having hash values with a length of 160 bit as well as the MD5, which is still often used today having a hash value length of 128 bit.
Inspection system	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.

Integrity	The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hash-functions, MACs (Message Authentication Codes) or – with additional functionality – digital signatures.
Javacard	A smart card with a Javacard operation system.
Key exchange	The use of symmetric cipher procedures requires that two communication partners decide on one joint key only known to themselves. The difficulty is that for the exchange of such information usually only partially secure channels exist. Additionally, protocols for key exchange must be prepared in such a way that only those pieces of information are exchanged which do not lead to knowledge of the real secret (the key). The most popular protocol of that type is diffie-Hellman, whose presentation in 1976 can be regarded as the birth of public key cryptography.
LDS	Logical data structure. The collection of groupings of data elements stored in the optional capacity expansion technology, defined in [ICAODoc].
MAC	Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy, requires its protection in a suitable way.
MRTD	Machnine-readable travel document. 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.
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.
Non-repudiation	One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered and respective framework conditions need to be provided by pertinent laws.
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.
Passphrase	A long, but memorable character sequence (e.g. short sentences with punctuation) which should replace passwords as they offer more security.
Password	A secret character sequence whose knowledge is to serve as a replacement for the authentication of a participant. A password is usually short to really ensure that an attacker cannot guess the password by trial and error.
Personalization	The process by which the portrait, signature and biographical data are applied to the document.
Personalization agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.

PKI	Cf. Public Key Infrastructure
PP	Protection Profile
Private key	Secret key only known to the receiver of a message, which is used in asymmetric ciphers for encryption or generation of digital signatures.
Pseudo random number	Many cryptographic mechanisms require random numbers (e.g. in key generation). The problem, however, is that it is difficult to implement true random numbers in software. Therefore, so called pseudo-random number generators are used, which then should be initialized with a real random element (the so called *seed*).
Public key	Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures.
Public key infrastructure (PKI)	Combination of hardware and software components, policies, and different procedures used to manage digital certificates.
Random numbers	Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for a software), so called pseudo random numbers are used instead.
Secure messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.
SFR	Security functional requirement.
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.
Smart card	A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (ROM, EEPROM) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). Therefore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.
SOD	Document Security Object (stored in EF.SOD). 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).
ST	Security Target
Stream cipher	Symmetric encryption algorithm which processes the plaintext bit-by-bit or byte-by-byte. The other usually employed class of procedures comprises so called block cipher.
Symmetric cipher	Encryption procedure using the same key for enciphering and deciphering (or, in which these two keys can simply be derived from each other). One distinguishes between block ciphers processing plaintext in blocks of fixed length (mostly 64 or 128 bit) and stream ciphers working on the basis of single characters.

TOE	Target of evaluation.
Travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.
TSF	TOE security functionality.
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template.
X.509	Standard for certificates, CRLs and authentication services. It is part of the X.500 standard of the ITU-T for realization of a worldwide distributed directory service realized with open system.