Agence Nationale des titres sécurisés

ANTS

Protection Profile

Machine Readable Travel Document

SAC (PACE V2) Supplemental Access Control

Date de publication : 21 September 2010
Référence : PP-MRTD-SAC/PACE V2
Version : 1.00

Table of Content

1 PP Introduction

1.1 PP reference

1	Title:	Protection Profile — Machine Readable Travel Document - SAC/PACE V2 Access Control
	Sponsor:	Agence Nationale des titres sécurisés – ANTS
	Editor	Agence Nationale des titres sécurisés – ANTS
	CC Version:	3.1 (Revision 3)
	Assurance Level:	The minimum assurance level for this PP is EAL4 augmented.
	General Status:	Official document
	Version Number:	1.00
	Registration:	
	Keywords:	ICAO, machine readable travel document, PACE V2 access control

1.2 TOE Overview

2 The protection profile defines the security objectives and requirements for the chip implementing the Supplemental Access Control as described in [20] in contact and/or in contactless interface. In particular, it may apply (not limited to), to the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security method PACE V2 Access Control specified in [20]. PACE V2 replaces BAC Access Control specified in [6].
In a transition period and for legacy reasons, some products claiming this PP may also wish to support BAC when they are connected to a BIS.

TOE definition

3 The Target of Evaluation (TOE) is the integrated circuit chip programmed according to the Logical Data Structure (LDS) and providing the PACE V2 Access Control according to [20].

4 The TOE comprises

- the circuitry of the MRTD's chip (the integrated circuit, IC)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application and
- the associated guidance documentation.

5 The ST writer may include other components within the TOE

TOE usage and security features for operational use

6 A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this protection profile contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ), (iii) the CAN for visual and machine reading using OCR methods on the data page and (iv) data elements on the MRTD's chip

according to LDS for machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State or Organization trusts a genuine MRTD of an issuing State or Organization.

7 For this protection profile the MRTD is viewed as unit of

(a) the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
  (1) the biographical data on the biographical data page of the passport book,
  (2) the printed data in the Machine-Readable Zone (MRZ) and
  (3) the printed portrait.

(b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [6] as specified by ICAO on the integrated circuit. It presents readable data including (but not limited to) personal data of the MRTD holder
  (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  (2) the digitized portraits (EF.DG2),
  (3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]
  (4) the other data according to LDS (EF.DG5 to EF.DG16) and
  (5) the Document security object.

8 The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

9 The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [6]. These security measures include the binding of the MRTD's chip to the passport book.

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

11 The ICAO defines the baseline security methods Passive Authentication Access Control to the logical MRTD, Active Authentication of the MRTD's chip, and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [6]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment. The ICAO defines the advanced security method PACE V2 Access Control to the logical MRTD in [20].

12 This protection profile addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the PACE V2 Access Control Mechanism. The PACE V2 Access Control Mechanism replaces the BAC Access Control Mechanism. It offers a higher security level as explained in [20].This protection profile does not address the Active Authentication and the Extended Access Control. They are optional security mechanisms.

---

[1] These additional biometric reference data are optional.

13 The PACE V2 Access Control is a security feature which is mandatory in the TOE. The inspection system (i) reads optically the MRTD or the CAN, (ii) authenticates itself as inspection system by means of Document PACE V2 Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [20].

TOE life cycle

14 The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [17], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

Phase 1 "Development"

15 (Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

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

17 The manufacturing documentation of the IC including the IC Dedicated Software and the IC Embedded Software (operating system) is securely delivered to the IC manufacturer. The IC Embedded Software to be loaded by the MRTD manufacturer, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase 2 "Manufacturing"

18 (Step3) 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 loaded by the IC manufacturer. 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.

19 (Step4) The MRTD manufacturer combines the IC with hardware for the physical interface in the passport book.

20 (Step5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD's chips with pre-personalization Data.

21 **Application Note1:** Creation of the application implies:

- For file based operating systems: the creation of MF and ICAO.DF
- For JavaCard operating systems: the Applet instantiation.

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

Phase 3 "Personalization of the MRTD"

23 (Step6) The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object.

24 The signing of the Document security object by the Document Signer [6] 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.

25 **Application note 2:** The TSF data (data for the operation of the TOE upon which the enforcement of the SFR relies; cf. [1] §97) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the PACE V2 Authentication Control Key. TSF data also include the source code.

26 **Application note 3:** This protection profile distinguishes between the Personalization 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 [6]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

Phase 4 “Operational Use”

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

28 **Application note 4:** The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.

29 **Application note 5:** The intention of the PP is to consider 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 Step 3 of this phase 2. However, the security target writer can still extend the evaluation scope and add further steps to be covered by ALC tasks. This will result in shifting the TOE delivery moment within the TOE life cycle. 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. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

2 Conformance Claims

2.1 CC Conformance Claim

30 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009, [3]

as follows

- Part 2 extended,
- Part 3 conformant.

31 The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [4]

has to be taken into account.

2.2 PP Claim,

32 This PP does not claim conformance to any another Protection Profiles.

2.3 Package Claim

33 This PP is conforming to assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [3].

2.4 Conformance rationale

34 Since this PP is not claiming conformance to any other protection profile, no rationale is necessary here.

2.5 Conformance statement

35 This PP requires strict conformance of any ST or PP, which claims conformance to this PP.

3 Security Problem Definition

3.1 Introduction

Assets

36 The assets to be protected by the TOE are the User Data of the MRTD's chip.

37 **Logical MRTD Data**
The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [6]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

38 The TOE described in this protection profile specifies only the PACE V2 mechanisms with resistance against high attack potential granting access to

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

39 The TOE prevents read access to sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG4)[2].

40 A sensitive item is the following more general one.

41 **Authenticity of the MRTD's chip**
The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD.

Subjects

42 This protection profile considers the following subjects:

43 **Manufacturer**
The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

[2] Cf. [18] for details how to access these User data under EAC protection.

44 **Personalization Agent**
The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities (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) and/or the encoded iris image(s) (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial static keys and (iv) signing the Document Security Object defined in [6].

45 **Terminal**
A terminal is any technical system communicating with the TOE through the interface.

46 **Inspection system (IS)**
A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

- The **Basic Inspection System** (BIS) (i) contains a terminal for the communication with the MRTD's chip, (ii) implements the terminals part of the BAC Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the BAC Access Control by optical reading the MRTD or other parts of the passport book providing this information.
- The **Supplemental Inspection System** (SIS) (i) contains a terminal for the communication with the MRTD's chip, (ii) implements the terminals part of the PACE V2 Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the PACE V2 Access Control by optical reading the MRTD or other parts of the passport book providing this information.
- The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism.
- The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

47 **Application note 6**: This protection profile does not distinguish between the SIS, GIS and EIS because the Active Authentication and the Extended Access Control is outside the scope.

48 **MRTD Holder**
The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

49 **Traveler**
Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

50 **Attacker**
A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data, nor the printed CAN), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

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

for the TOE IT environment. It shall be addressed by security measures on the TOE IT environment

3.2 Assumptions

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

53 **A.MRTD_Manufact MRTD manufacturing on step 4 to 6**

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

54 **A.MRTD_Delivery MRTD delivery during step 4 to 6**

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

55 **A.Pers_Agent Personalization of the MRTD's chip in step 6**

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document PACE V2 Access Keys, derived from the MRZ or the CAN, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

56 **A.Insp_Sys Inspection Systems for global interoperability during step 7**

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Supplemental Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the PACE V2 Access Control [20]. The Supplemental Inspection System reads the logical MRTD under PACE V2 Access Control and performs the Passive Authentication to verify the logical MRTD.

57 **Application note 8**: According to [6] the support of the Passive Authentication mechanism is mandatory whereas the PACE V2 Access Control is optional. This PP does not address Primary Inspection Systems therefore the PACE V2, which replaces BAC is mandatory within this PP.

3.3 Threats

58 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.

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

60 **T.Chip_ID** **Identification of MRTD's chip**

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the communication interface. The attacker cannot read and does not know the MRZ data, nor the CAN printed on the MRTD data page in advance.

61 **T.Skimming** **Skimming the logical MRTD**

An attacker imitates the inspection system to read the logical MRTD or parts of it via the communication channel of the TOE. The attacker cannot read and does not know the MRZ data, nor the CAN printed on the MRTD data page in advance.

62 **T.Eavesdropping** **Eavesdropping to the communication between TOE and inspection system**

An attacker is listening to the communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data, or the CAN printed on the MRTD data page but the attacker does not know these data in advance.

Note in case of T.Skimming the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data, nor the CAN printed on the MRTD data page and without a help of the inspection system which knows these data. In case of T.Eavesdropping the attacker uses the communication of the inspection system.

63 **T.Forgery** **Forgery of data on MRTD's chip**

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another chip.

64 **T.Abuse-Func** **Abuse of Functionality**

An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational environment after delivery to MRTD holder.

65 The TOE shall avert the threats as specified below.

66 **T.Information_Leakage Information Leakage from MRTD's chip**

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

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

67 **T.Phys-Tamper Physical Tampering**

An attacker may perform physical probing of the MRTD's chip in order (i) to disclose confidential TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) modify TSF data.

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

68 **T.Malfunction Malfunction due to Environmental Stress**

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration

function. To exploit these vulnerabilities an attacker needs information about the functional operation.

3.4 Organizational Security Policies

69 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 CC part 1, sec. A.6.3).

70 **P.Manufact** **Manufacturing of the MRTD's chip**

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

71 **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.

72 **P.Personal_Data** **Personal data protection policy**

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)[3] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the PACE V2 Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document PACE V2 Access Keys as defined in [20].

73 **Application note 9:** The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [6]. Note that the Document PACE V2 Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

[3] Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by this Protection Profile.

4 Security Objectives

74 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

75 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.

76 **OT.AC_Pers Access Control for Personalization of logical MRTD**

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [6] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

77 **Application note 10**: The OT.AC_Pers implies that

(1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1, and EF.DG2) can not be changed by write access after personalization,

(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the “Operational Use” phase is optional.

78 **OT.Data_Int Integrity of personal data**

The TOE must ensure the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

79 **OT.Data_Conf Confidentiality of personal data**

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Supplemental Inspection System. The Supplemental Inspection System shall authenticate itself by means of the PACE V2 Access Control based on knowledge of the Document PACE V2 Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Supplemental Inspection System.

80 **OT.Identification Identification and Authentication of the TOE**

The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. The storage of the Pre-

Personalization data includes writing of the Personalization Agent Authentication key(s). In Phase 4 “Operational Use” the TOE shall identify itself only to a successful authenticated Supplemental Inspection System or Personalization Agent.

81 **Application note 11:** The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and/or to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the MRTD”. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 “Operational Use” the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the interface before successful authentication as Supplemental Inspection System or as Personalization Agent.
In a multi-applicative product, data allowing to identify the IC or the MRTD, can be disclosed by other applications. Therefore the ST writer shall check that this objective on the TOE also applies to the other applications.

82 The following TOE security objectives address the protection provided by the MRTD’s chip independent of the TOE environment.

83 **OT.Prot_Abuse-Func Protection against Abuse of Functionality**

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded ICEmbedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

84 **OT.Prot_Inf_Leak Protection against Information Leakage**

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD’s chip

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

85 **Application note 12:** This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

86 **OT.Prot_Phys-Tamper Protection against Physical Tampering**

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

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

with a prior

- reverse-engineering to understand the design and its properties and functions.

87 **OT.Prot_Malfunction Protection against Malfunctions**

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

88 **Application note 13:** A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

4.2 Security Objectives for the Operational Environment

Issuing State or Organization

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

90 **OE.MRTD_Manufact Protection of the MRTD Manufacturing**

Appropriate functionality testing of the TOE shall be used in step 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

91 **OE.MRTD_ Delivery Protection of the MRTD delivery**

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:

  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

92 **OE.Personalization Personalization of logical MRTD**

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

93 **OE.Pass_Auth_Sign Authentication of logical MRTD by Signature**

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [6].

Receiving State or Organization

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

95 **OE.Exam_MRTD Examination of the MRTD passport book**

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Supplemental Inspection System (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the PACE V2 Access Control [20].

96 **OE.Passive_Auth_Verif Verification by Passive Authentication**

The border control officer of the receiving State uses the inspection system to verify the traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

97 **OE.Prot_Logical_MRTD Protection of data from the logical MRTD**

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under PACE V2 Access Control will use inspection systems which implement the terminal part of the PACE V2 Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Supplemental Inspection Systems).

4.3 Security Objective Rationale

98 The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				x											
T.Skimming			x												
T.Eavesdropping			x												
T.Forgery	x	x					x					x	x	x	
T.Abuse-Func					x						x				
T.Information_Leakage						x									
T.Phys-Tamper							x								
T.Malfunction								x							
P.Manufact				x											
P.Personalization	x			x							x				
P.Personal_Data		x	x												
A.MRTD_Manufact									x						
A.MRTD_Delivery										x					
A.Pers_Agent											x				
A.Insp_Sys													x		x

Table 1: Security Objective Rationale

99 The OSP **P.Manufact** “Manufacturing of the MRTD’s chip” requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by **OT.Identification**.

100 The OSP **P.Personalization** “Personalization of the MRTD by issuing State or Organization only” addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD”, and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD”. Note the manufacturer equips the TOE with the Personalization Agent Authentication 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 management of TSF to the Personalization Agent.

101 The OSP **P.Personal_Data** "Personal data protection policy" requires the TOE (i) to support the protection of the confidentiality of the logical MRTD by means of the PACE V2 Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives **OT.Data_Int** "Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT.Data_Conf** "Confidentiality of personal data" describes the protection of the confidentiality.

102 The threat **T.Chip_ID** "Identification of MRTD's chip" addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the communication interface. This threat is countered as described by the security objective **OT.Identification** by PACE V2 Access Control.

103 The threat **T.Skimming** "Skimming digital MRZ data or the digital portrait" and **T.Eavesdropping "**Eavesdropping to the communication between TOE and inspection system" address the reading of the logical MRTD trough the interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective **OT.Data_Conf** "Confidentiality of personal data" through PACE V2 Access Control.

104 The threat **T.Forgery** "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRTD passport book according to **OE.Exam_MRTD** "Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign "**Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif** "Verification by Passive Authentication".

105 The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks using the MRTD's chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality". Additionally this objective is supported by the security objective for the TOE environment: **OE.Personalization** "Personalization of logical MRTD" ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

106 The threats **T.Information_Leakage** "Information Leakage from MRTD's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak** "Protection against Information Leakage", **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot_Malfunction** "Protection against Malfunctions".

107 The assumption **A.MRTD_Manufact** “MRTD manufacturing on step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_Manufact** “Protection of the MRTD Manufacturing” that requires to use security procedures during all manufacturing steps.

108 The assumption **A.MRTD_ Delivery** “MRTD delivery during step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_ Delivery** “Protection of the MRTD delivery” that requires to use security procedures during delivery steps of the MRTD.

109 The assumption **A.Pers_Agent** “Personalization of the MRTD’s chip” is covered by the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD” including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

110 The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objectives for the TOE environment **OE.Exam_MRTD** “Examination of the MRTD passport book”. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** “Protection of data from the logical MRTD” will require the Supplemental Inspection System to implement the PACE V2 Access Control and to protect the logical MRTD data during the transmission and the internal handling.

5 Extended Components Definition

111 This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [16], other components are defined in this protection profile.

5.1 Definition of the Family FAU_SAS

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

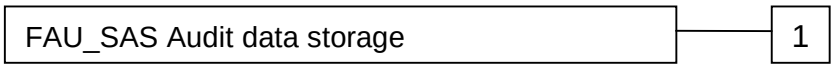
113 The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behavior

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

Component leveling



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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.2 Definition of the Family FCS_RND

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

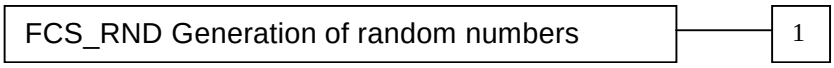
115 The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3 Definition of the Family FMT_LIM

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

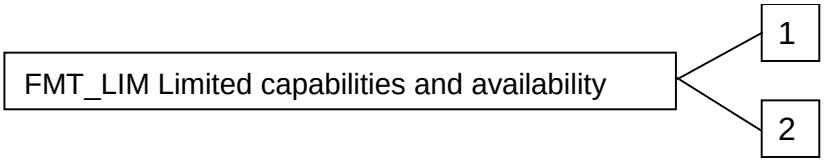
117 The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behavior

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

Component leveling:



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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

118 To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

119 The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: *Limited capability and availability policy*].

120 The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].

121 **Application note 14**: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

5.4 Definition of the Family FPT_EMSEC

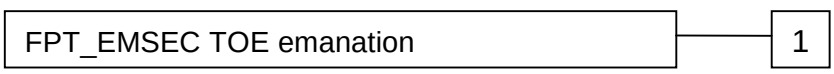
122 The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena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

123 The family “TOE Emanation (FPT_EMSEC)” is specified as follows.

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6 Security Requirements

124 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 [1] of the CC. Each of these operations is used in this PP.

125 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in bold text and the added/changed words are in bold text. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

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

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

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

6.1 Security Functional Requirements for the TOE

129 This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

6.1.1 Class FAU Security Audit

130 The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

131 **FAU_SAS.1 Audit storage**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer[4] with the capability to store the IC Identification Data [5] in the audit records.

4 [assignment: *authorised users*]

5 [assignment: *list of audit information*]

132 **Application note 15:** The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.1.2 Class Cryptographic Support (FCS)

133 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.

134 **FCS_CKM.1 Cryptographic key generation – Generation of Document V2 Session Keys by the TOE**

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 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] [6] and specified cryptographic key sizes [*assignment: cryptographic key sizes*][7] that meet the following: [20], normative appendix 5[8].

135 **Application note 16:** The TOE is equipped with the Document PACE V2 Access Key generated and downloaded by the Personalization Agent. The PACE V2 Access Control Authentication Protocol described in [20], produces agreed parameters to generate the ENC and the MAC session keys for secure messaging. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

6 [*assignment: cryptographic key generation algorithm*]

7 [*assignment: cryptographic key sizes*]

8 [assignment: *list of standards*]

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

137 **FCS_CKM.4 Cryptographic key destruction - 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.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

138 **Application note 17:** The TOE shall destroy the encryption key and the MAC message authentication keys for secure messaging.

6.1.2.1 Cryptographic operation (FCS_COP.1)

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

140 **FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation**

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/ SHA The TSF shall perform hashing [9] in accordance with a specified cryptographic algorithm [selection: *SHA or other approved algorithms*] [10] and cryptographic key sizes none [11] that meet the following: [selection: *FIPS 180-2 or other approved standards*] [12].

141 **Application note 18:** This SFR requires the TOE to implement the hash function for the cryptographic primitive of the PACE V2 Access Control Authentication Mechanism (see also FIA_UAU.4) c.

9 [assignment: *list of cryptographic operations*]

10 [assignment: *cryptographic algorithm*]

11 [assignment: *cryptographic key sizes*]

12 [assignment: *list of standards*]

142 **FCS_COP.1/ENC Cryptographic operation – Symmetric Encryption / Decryption**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ ENC: The TSF shall perform secure messaging (PACE V2) – encryption and decryption [13] in accordance with a specified cryptographic algorithm [assignment: *Cryptographic algorithm*] [14] and cryptographic key sizes [assignment: *Cryptographic key sizes*] [15] that meet the following: [assignment: *list of cryptographic operations*][16].

143 **Application note 19:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the PACE V2 Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4. See also [20].

144 **FCS_COP.1/AUTH Cryptographic operation – Authentication**

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/ AUTH: The TSF shall perform symmetric authentication – encryption and decryption [17] in accordance with a specified cryptographic algorithm [selection: *Triple-DES, AES*] [18] and cryptographic key sizes [selection: *112, 128, 168, 192, 256*] bit[19] that meet the following: [selection: *FIPS 46-3 [9], FIPS 197 [12]*][20].

145 **Application note 20:** This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

146 **FCS_COP.1/MAC Cryptographic operation – MAC**

---

13 [assignment: *list of cryptographic operations*]

14 [assignment: *cryptographic algorithm*]

15 [assignment: *cryptographic key sizes*]

16 [assignment: *list of standards*]

17 [assignment: *list of cryptographic operations*]

18 [assignment: *cryptographic algorithm*]

19 [assignment: *cryptographic key sizes*]

20 [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]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ MAC: The TSF shall perform secure messaging – message authentication code [21] in accordance with a specified cryptographic algorithm [selection: *DES or AES Retail-MAC, CMAC or other approved algorithms*] [22] and cryptographic key sizes [assignment: *Cryptographic key sizes*] [23] that meet the following: [selection: ISO9797-1, SP800-38b, or other approved *standards*] [24].

147 **Application note 21:** 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 the PACE V2 Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4. The authorized cryptographic algorithms and key sizes are specified in [20].

6.1.2.2 Random Number Generation (FCS_RND.1)

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

149 **FCS_RND.1 Quality metric for random numbers**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

150 **Application note 22:** This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

21 [assignment: *list of cryptographic operations*]

22 [assignment: *cryptographic algorithm*]

23 [assignment: *cryptographic key sizes*]

24 [assignment: *list of standards*]

6.1.3 Class FIA Identification and Authentication

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

152 **FIA_UID.1 Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read the random identifier and the file CardAccess in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier and the file CardAccess in Phase 4 “Operational Use”[25]

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

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

153 **Application note 23:** The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document PACE V2 Access Keys) the user role Supplemental Inspection System is created by writing the Document PACE V2 Access Keys. The Supplemental Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document PACE V2 Access Key to authenticate the user as Supplemental Inspection System.

154 **Application note 24:** In the “Operational Use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Supplemental Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’s chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

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

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

156 **FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 "Manufacturing",
2. to read the random identifier and the file CardAccess in Phase 3 "Personalization of the MRTD",
3. to read the random identifier and the file CardAccess in Phase 4 "Operational Use"[26]

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

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

157 **Application note 25:** The Supplemental Inspection System and the Personalization Agent authenticate themselves.

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

159 **FIA_UAU.4 Single-use authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. PACE V2 Access Control Authentication Mechanism,
2. Authentication Mechanism based on [selection: *Triple-DES, AES or other approved algorithms*][27].

160 **Application note 26:** 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.

161 **Application note 27:** The PACE V2 Access Control Mechanism is a mutual device authentication mechanism defined in [20]. The last step of this mutual authentication may allow a unique identification of the MRTD's chip. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

---

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

27 [assignment: *identified authentication mechanism(*s)]

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

163 **FIA_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

1. PACE V2 Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on [selection: *Triple-DES, AES*] [28]

to support user authentication.

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

1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) [selection *: the PACE V2 Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]*],
2. the TOE accepts the authentication attempt as Supplemental Inspection System only by means of the PACE V2 Access Control Authentication Mechanism with the Document PACE V2 Access Keys [29].

164 **Application note 28:** The PACE V2 Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Supplemental Inspection System uses the PACE V2 Access Control Authentication Mechanism with the Document PACE V2 Access Keys.

28 [assignment: *list of multiple authentication mechanisms*]

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

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

166 **FIA_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions :
Failure of MAC verification in a command received by the TOE.[30].

167 **Application note 29:** The PACE V2 Access Control Mechanism specified in [6] includes the 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 MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/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 PACE V2 user.

168 **Application note 30:** Note that in case the TOE should also fulfill [18] the PACE V2 communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the PACE V2 based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the PACE V2 communication but are protected by a more secure communication channel established after a more advanced authentication process.

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

170 **Authentication failure handling (FIA_AFL.1)**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [assignment: *met or surpassed*], the TSF shall [assignment: *list of actions*].

171 **Application note 31:** The ST writer shall perform the open operation in the elements FIA_AFL.1.1 and FIA_AFL.1.2. These assignments should be assigned to ensure especially the strength of authentication function as terminal part of the PACE V2 Access Control Authentication Protocol to resist high attack potential.
The ST writer may consider the following example for such operations and refinement:
FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within

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

range of acceptable values 1 to 10 **consecutive** unsuccessful authentication attempts occur related to PACE V2 authentication protocol.
The refinement by inclusion of the word "consecutive" allows the TSF to return to normal operation of the PACE V2 authentication protocol (without time out) after successful run of the PACE V2 authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the "consecutive unsuccessful authentication attempts" are count independent on power-on sessions but reset to zero after successful authentication only.

6.1.4 Class FDP User Data Protection

6.1.4.1 Subset access control (FDP_ACC.1)

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

173 **FDP_ACC.1 Subset access control – PACE V2 Access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the PACE V2 Access Control SFP [31] on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD [32].

6.1.4.2 Security attribute based access control (FDP_ACF.1)

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

175 **FDP_ACF.1 Basic Security attribute based access control – PACE V2 Access Control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the PACE V2 Access Control SFP[33] to objects based on the following:
1. Subjects:
   a. Personalization Agent,
   b. Supplemental Inspection System,
   c. Terminal,
2. Objects:
   a. data EF.DG1 to EF.DG16 of the logical MRTD,
   b. data in EF.COM,
   c. data in EF.SOD,
3. Security attributes
   a. authentication status of terminals [34].

31 [assignment: *access control SFP*]

32 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

33 [assignment: *access control SFP*]

FDP_ACF.1.2 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 Supplemental Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD [35].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[36].

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

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Supplemental Inspection System is not allowed to read the data in EF.DG3 and EF.DG4. [37].

176 **Application note 32:** The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this protection profile (cf. [18] for details).

6.1.4.3 Inter-TSF-Transfer

177 **Application note 33:** FDP_UCT.1 and FDP_UIT.1 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 authentication of the terminal. The authentication mechanisms as part of PACE V2 Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

179 **FDP_UCT.1 Basic data exchange confidentiality - MRTD**

34 [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

35 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

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

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

Hierarchical to: No other components.

Dependencies: [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]

FDP_UCT.1.1 The TSF shall enforce the PACE V2 Access Control SFP[38] to be able to transmit and receive[39] user data in a manner protected from unauthorised disclosure.

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

181 **FDP_UIT.1 Data exchange integrity - MRTD**

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce the PACE V2 Access Control SFP [40] to be able to transmit and receive [41] user data in a manner protected from modification, deletion, insertion and replay [42] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [43] has occurred.

6.1.5 Class FMT Security Management

182 **Application note 34**: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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

184 **FMT_SMF.1 Specification of Management Functions**

38 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

39 [selection*: transmit, receive*]

40 [assignment: *access control SFP(s) and/or* i*nformation flow control SFP(s)*]

41 [selection*: transmit, receive*]

42 [selection: *modification*, *deletion*, *insertion*, *replay*]

43 [selection: *modification*, *deletion*, *insertion*, *replay*]

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. Personalization,
3. Configuration [44].

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

186 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Supplemental Inspection System [45].

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

187 **Application note 35**: 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.

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

189 **FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

44 [assignment: *list of management functions to be provided by the TSF*]

45 [assignment: *the authorised identified roles*]

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 disclosed or manipulated
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks

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

191 **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 disclosed or manipulated,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.

192 **Application note 36:** 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 provide an optional approach to enforce the same policy.
Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

193 **Application note 37:** 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.

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

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write [46] the Initialization Data and Pre-personalization Data [47] to the Manufacturer [48].

196 **Application note 38:** The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Authentication Key.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to disable read access for users to [49] the Initialization Data [50] to the Personalization Agent [51].

198 **Application note 39:** According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

199 **FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write**

---

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

47 [assignment: *list of TSF data*]

48 [assignment: *the authorised identified roles*]

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

50 [assignment: *list of TSF data*]

51 [assignment: *the authorised identified roles*]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write [52] the Document PACE V2 Access Keys [53] to the Personalization Agent [54].

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read [55] the Document PACE V2 Access Keys and Personalization Agent Keys [56] to none [57].

201 **Application note 40**: The Personalization Agent generates, stores and ensures the correctness of the Document PACE V2 Access Keys.

6.1.6 Class FPT Protection of the Security Functions

202 The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.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 “TSF testing (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 functions.

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

204 **FPT_EMSEC.1 TOE Emanation**

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMSEC.1.1	The TOE shall not emit [*assignment: types of emissions*] in excess of

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

53 [assignment: *list of TSF data*]

54 [assignment: *the authorised identified roles*]

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

56 [assignment: *list of TSF data*]

57 [assignment: *the authorised identified roles*]

[assignment: *specified limits*] enabling access to Personalization Agent Authentication Key(s) [58] and [assignment: *list of types of user data*].

FPT_EMSEC.1.2 The TSF shall ensure any unauthorized users [59] are unable to use the following interface smart card circuit contacts [60] to gain access to Personalization Agent Authentication Key(s) [61] and [assignment: *list of types of user data*].

205 **Application note 41**: The ST writer shall perform the operation in FPT_EMSEC.1.1 and FPT_EMSEC.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. 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.

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

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

208 **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 **[62]**.

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

210 **FPT_TST.1 TSF testing**

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up,*

58 [assignment: *list of types of TSF data*]

59 [assignment: *type of users*]

60 [assignment: *type of connection*]

61 [assignment: *list of types of TSF data*]

62 [assignment: *list of types of failures in the TSF*]

periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF[63].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data[64].

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

211 **Application note 42**: The ST writer shall perform the operation in FPR_TST.1.1. If the MRTD's chip uses state of the art smart card technology it will run the some self tests at the request of the authorized 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 "authorized user" Manufacturer in the Phase 2 Manufacturing. Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 "Operational Use", e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.

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

213 **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 [65] to the TSF [66] by responding automatically such that the SFRs are always enforced.

214 **Application note 43**: 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.

215 **Application note 44**: The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

---

63 [selection: *[assignment: parts of TSF], the TSF*]

64 [selection: *[assignment: parts of TSF], TSF data*]

65 [assignment: *physical tampering scenarios*]

66 [assignment: *list of TSF devices/elements*]

6.2 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ALC_DVS.2 and AVA_VAN.5.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT:Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Malfuntion	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					
FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_RND.1	x	x	x					
FIA_UID.1			x	x				
FIA_AFL.1			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4	x	x	x					
FIA_UAU.5	x	x	x					
FIA_UAU.6	x	x	x					
FDP_ACC.1	x	x	x					
FDP_ACF.1	x	x	x					
FDP_UCT.1	x	x	x					
FDP_UIT.1	x	x	x					
FMT_SMF.1	x	x	x					
FMT_SMR.1	x	x	x					
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA				x				
FMT_MTD.1/INI_DIS				x				
FMT_MTD.1/KEY_WRITE	x	x	x					
FMT_MTD.1/KEY_READ	x	x	x					
FPT_EMSEC.1	x				x			
FPT_TST.1					x		x	
FPT_FLS.1	x				x		x	
FPT_PHP.3	x				x	x		

Table 2: Coverage of Security Objective for the TOE by SFR

218 The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the

successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the PACE V2 mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [18] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

In case of using the PACE V2 mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document PACE V2 Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

219 The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the PACE V2 mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document PACE V2 Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

220 The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated

Supplemental Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Supplemental Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document PACE V2 Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Supplemental Inspection System only by means of the PACE V2 Access Control Authentication Mechanism with the Document PACE V2 Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with PACE V2 Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document PACE V2 Access Keys.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the PACE V2 Access Control Authentication Mechanism or secure messaging.

221 The security objective **OT.Identification** “Identification and Authentication of the TOE” address the storage of the IC Identification Data uniquely identifying the MRTD’s chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

Furthermore, the TOE shall identify itself only to a successful authenticated Supplemental Inspection System in Phase 4 “Operational Use”. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 “Operational Use” violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD’s chip before successful authentication of the Supplemental Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application note 27). In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

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

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

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT_EMSEC.1,

- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or

- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

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

225 The security objective **OT.Prot_Malfunction** "Protection against Malfunctions" is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

6.3.2 Dependency Rationale

226 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.

227 The table 3 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction,	Fulfilled by FCS_COP.1/ENC and FCS_COP.1/MAC, Fulfilled by FCS_CKM.4
FCS_CKM.4	[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]	Fulfilled by FCS_CKM.1,
FCS_COP.1/SHA	[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, Fulfilled by FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/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, Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[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	justification 1 for non-satisfied dependencies justification 1 for non-satisfied dependencies
FCS_COP.1/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, Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 2 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 3 for non-satisfied dependencies Fulfilled by FDP_ACC.1

SFR	Dependencies	Support of the Dependencies
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 3 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
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
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
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 3: Dependencies between the SFR for the TOE

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

No. 1: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

No. 2: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization 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.2) is necessary here.

No. 3: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS. There is no need for sensitive SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel.

6.3.3 Security Assurance Requirements Rationale

229 The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

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

231 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.

232 The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements.

233 The component AVA_VAN.5 augmented to EAL4 has the following dependencies:
- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing 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 EAL4 assurance package.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

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

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

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

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

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

7 Glossary and Acronyms

Term	Definition
Active Authentication	Security mechanism defined in [6] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control (BAC)	Security mechanism defined in [6] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there). In this PP, BAC is replaced by PACE V2, defined in [20].
PACE V2 /Supplemental Access Control (SAC)	Security mechanism defined in [20] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document PACE V2 Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys, derived from the printed MRZ data, for reading the logical MRTD.
Supplemental Inspection System (SIS)	An inspection system which implements the terminals part of the PACE V2 Access Control Mechanism and authenticates itself to the MRTD's chip using the Document PACE V2 Access Keys, derived from the printed MRZ data or the CAN, for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [6]
biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [6]
Card Access Number (CAN)	Password derived from a short number printed on the front side of the datapage. [20]
Country Signing CA Certificate (C_{CSCA})	Self-signed certificate of the Country Signing CA Public Key (K_{PuCSCA}) issued by CSCA stored in the inspection system.
Document PACE V2 Access Keys	Pair of symmetric 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 [20]. It is drawn from the printed MRZ or CAN of the passport book to authenticate an entity able to read these data.
Document Security	A RFC3369 CMS Signed Data Structure, signed by the Document Signer

Term	Definition
Object (SO_D)	(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 (C_{DS}). [6]
Eavesdropper	A threat agent with high attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [6]
Extended Access Control	Security mechanism identified in [6] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Supplemental Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [6]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [6]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [6]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [6]
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).

Term	Definition
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [6]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [6]
Issuing State	The Country issuing the MRTD. [6]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [6]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [6] as specified by ICAO on the integrated circuit. It presents readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16). (6) EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [6]
Machine readable visa (MRV):	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [6]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [6] It also means the password derived from the MRZ. [20]

Term	Definition
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [6]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [6], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14, EF.DG 16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD PACE V2 Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	An integrated circuit chip programmed according to the Logical Data Structure as specified by ICAOT, [7], p. 14.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
OCR method	Optical character Reading method Machine reading technology used for the document
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
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.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment". [6]
Personalization Agent	The agent acting on the behalf of the issuing State or Organization 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.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD and (ii) by the MRTD's chip

Term	Definition
Authentication Key	to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
Primary Inspection System (PIS)	An inspection system that contains a terminal for the communication with the MRTD's chip and does not implement the terminals part of the PACE V2 Access Control Mechanism. This PP does not support PIS
Receiving State	The Country to which the Traveler is applying for entry. [6]
reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [6]
secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the communication channel of the TOE without knowledge of the printed MRZ data, nor the CAN.
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. [6]
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalisation Agent from the Manufacturer.
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [6]
Verification data	Data provided by an entity in an authentication attempt to prove their identity

Term	Definition
	to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
BIS	Basic Inspection System
CC	Common Criteria
EF	Elementary File
GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number.
MF	Master File
n.a.	Not applicable
OSP	Organizational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
SIS	Supplemental Inspection System
TOE	Target of Evaluation
TSF	TOE security functions

8 Literature

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

[5] Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik

ICAO

[6] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization

[7] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

Cryptography

[8] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[9] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[10] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[11] Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[12] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[13] Certicom Research: SEC 1: Elliptic Curve Cryptography, September 20, 2000, Version 1.0

[14] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998

[15] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2002

Protection Profiles

[16] PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[17] Security IC Platform Protection Profile, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007

[18] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0056, version 1.10, 25th March 2009

Other

[19] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] ICAO TR – Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, March 23, 2010

[21] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004