Security Target lite -
Machine Readable Travel Document
with ICAO Application and Basic Access Control
MTCOS Pro 2.0 ICAO / P5CD072V0Q

MaskTech GmbH

Document number: BSI-DSZ-CC-0384, ST-lite, Version 1.0

Created by: Matthias Brüstle

Date: 2006-10-27

Signature:

Released by Management

Date:

Signature:

Change history

Version	Date	Reason	Remarks
1.0	2006-10-27	First Version of ST-liste based on ST	

Table of Content

1 Introduction

1.1 ST identification

Title:	Security Target lite — Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-ST)
Version:	1.0, 2006-10-27
Editors:	Matthias Brüstle, MaskTech GmbH
Compliant to:	Common Criteria Protection Profile – Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.0, BSI-PP-0017
CC Version:	2.3
Assurance Level:	The assurance level for this ST is EAL4 augmented.
General Status:	Submitted for evaluation
Hardware:	Philips P5CD072V0Q
TOE version:	MTCOS Pro 2.0 ICAO
Keywords:	ICAO, machine readable travel document

1.2 ST Overview

1 The aim of this document is to describe the Security Target for the Machine Readable Travel Document (MRTD) chip with the ICAO Application and Basic Access Control on the MaskTech MTCOS Standard operating system.

2 The Security Target defines the security objectives and requirements for the contactless chip based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the Technical reports of the ICAO New Technology Working Group.

3 MTCOS Standard is a fully interoperable multi-application smart card operating system compliant to ISO/IEC 7816. It provides secret key cryptography and supports also other applications like e-purses, health insurance cards and access control.

4 The operating system software is implemented on the Philips P5CD072V0Q secure dual-interface controller, which is certified according to CC EAL5 augmented. This means, that the TOE consists of software and hardware.

5 The assurance level for the TOE is CC EAL4 augmented.

6 The minimum strength level (SOF) for the TOE security functions is high.

1.3 CC Conformance

7 This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, August 2005, version 2.3, CCMB-2005-08-001

- Common Criteria for Information Technology Security Evaluation, Part 2: Security function requirements, August 2005, version 2.3, CCMB-2005-08-002

- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, August 2005, version 2.3, CCMB-2005-08-001

as follows

- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2 and ALC_DVS.2.

2 TOE Description

2.1 System Type

2.1.1 Machine Readable Travel Documents

8 (This description is taken from the corresponding Protection Profile [16] and should be used as a general introduction to MRTDs.)

9 The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [6] and providing the Basic Access Control according to the ICAO document [7].

10 The TOE comprises of
- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors,
- 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.

TOE usage and security features for operational use

11 State or organisation issues MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveller 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) 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 trust a genuine MRTD of a issuing State or Organization.

12 For this security target 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 contactless integrated circuit. It presents over the logical interface of APDUs contactless readable data including (but not limited to) personal data of the MRTD holder
  (1) the digital Machine Readable Zone Data (digital MRZ data, DG1),
  (2) the digitized portraits (DG2),
  (3) the optional biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both
  (4) the other data according to LDS (DG5 to DG16) and
  (5) the Document security object.

13 The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and its data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the document number.

14 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 organisational security measures (e.g. control of materials, personalization procedures) [8]. These security measures include the binding of the MRTD's chip to the passport book.

15 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.

16 The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of additional biometrics as optional security measure in the ICAO Technical report [7]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

17 This security target 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 Basic Access Control Mechanism. This security target does not address the Active Authentication and the Extended Access Control as optional security mechanisms.

18 The Basic Access Control is a security feature which shall be mandatory supported by the TOE but may be disabled by the Issuing State or Organization. The inspection system (i) reads the printed data in the MRZ, (ii) authenticates themselves as inspection system by means of keys derived from MRZ data. 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 [7], Annex E, and [6].

TOE life cycle

19 The TOE life cycle is described in terms of the four life cycle phases similar to the PP. The phase 2 is split into multiple steps.

Phase 1 “Development”

20 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.

21 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.

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

Phase 2 “Manufacturing”

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

24 The MRTD manufacturer (i) adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary, (ii) creates the MRTD application, and (iii) equips MRTD’s chip with Pre-personalization Data and (iv) packs the IC with hardware for the contactless interface in the passport book.

25 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.

26 For easier handling this phase is split into:

a) IC manufacturing: Manufacturing of the chip incl. Identification Data by the IC manufacturer.

b) Initialization: The MRTD manufacturer configures the TOE like in a software installation procedure.

c) Pre-personalization: The MRTD manufacturer prepares the TOE for the personalization, e.g. creation of data files.

Phase 3 “Personalization of the MRTD”

27 The personalization of the MRTD includes (i) the survey of the MRTD holder biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional 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) the writing the TSF Data into the logical MRTD and 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 (DG1), (ii) the digitised portrait (DG2), and (iii) the Document security object.

28 The signing of the Document security object by the Document signer [7] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Phase 4 “Operational Use”

29 The term “Operational Use” is not used here and afterwards in the sense of the Common Criteria, but just to describe that here the MRTD is really used by the end-user.

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

2.1.2 Use of TOE

31 The TOE is implemented as a smart card IC, which supports the communication via a contactless interface according to ISO/IEC 14443. It is based on ISO/IEC 7816 commands and is intended to be used inside a MRTD as storage of the digital data and supports Basic Access Control.

32 Because of the support of ISO/IEC 7816 the TOE can be also used as multi-application smart card with applications of health care, e-purse or loyalty.

2.2 Limits of the TOE

2.2.1 Architecture

33 The TOE is an RFID device according to ICAO technical reports [6] and [7] supporting Basic Access Control. It is implemented as an embedded software on a smart card chip, in this case the CC EAL 5+ certified Philips P5CD072V0Q. The TOE is the MTCOS Standard smart card operating system stored in the ROM of the IC, the file system including application data, any configurable and non-volatile parameters and perhaps parts of the operating system stored in EEPROM and the IC itself.

34 The TOE provides following services for MRTDs:

1. Storage of the MRTD data, e.g. data groups and signature.
2. Organization of the data in a file system as dedicated and elementary files.
3. Mutual Authenticate and secure messaging as specified in TrPKI [7] for Basic Access Control.
4. Contactless communication according to ISO/IEC 14443.
5. Protection of data against modification.
6. Protection of the privacy of the passport holder with functions like random UID and Basic Access Control.

35 The TOE life cycle is as defined in the preceding subsection with the addition, that the operating system distinguishes in phase 2 between initialization mode and operational mode. In initialization mode the operating system can be configured with secure messaging protected commands. In this phase also the file system is created. The pre-personalization is done in phase 2 after switching the OS to operational mode. The operating system is in the operational mode until end of life.

3 Security Environment

3.1 Introduction

Assets

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

37 **Logical MRTD Data**
The logical MRTD data consists of the data groups DG1 to DG16 and the Document security object according to LDS [6]. These data are user data of the TOE. The data groups DG1 to DG14 and DG 16 contain personal data of the MRTD holder. The Active Authentication Public Key Info in DG 15 is used by the inspection system for Active Authentication of the chip. The Document security object is used by the inspection system for Passive Authentication of the logical MRTD.

38 An additional asset is the following more general one.

39 **Authenticity of the MRTD's chip**
The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD's holder is used by the traveller to authenticate himself as possessing a genuine MRTD.

Subjects

40 This security target considers the following subjects:

41 **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.

42 **MRTD Holder**
The rightful holder of the MRTD for whom the issuing State or Organization personalised the MRTD.

43 **Traveller**
Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

44 **Personalization Agent**
The agent is acting on the behalf of the issuing State or Organisation 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 and (iv) signing the Document Security Object defined in [6].

45 **Inspection system**
A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder. The **Primary Inspection System** (PIS) (i) contains a terminal for the contactless communication with the MRTD's chip and (ii) does not implement the terminals part of the Basic Access Control Mechanism. The Primary Inspection System can read the logical MRTD only if the Basic Access Control is disabled. The **Basic Inspection System** (BIS) (i) contains a terminal for the contactless communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the printed data in the MRZ or other parts of the passport book providing this information. The **Extended Inspection System** (EIS) in addition to the Basic Inspection System (i) implements the Active Authentication Mechanism, (ii) supports the terminals part of the Extended Access Control Authentication Mechanism and (iii) is authorized by the issuing State or Organization to read the optional biometric reference data.

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

47 **Attacker**
A threat agent trying (i) to identify and to trace the movement the MRTD's chip remotely (i.e. without knowing or reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

3.2 Assumptions

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

49 A.Pers_Agent Personalization of the MRTD's chip

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Active Authentication Public Key Info (DG15) 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.

50 A.Insp_Sys Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder. The Primary Inspection System for global interoperability contains the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization [7]. The Primary Inspection System performs the Passive Authentication to verify the logical MRTD if the logical MRTD is not protected by Basic Access Control. The Basic Inspection System in addition to the Primary Inspection System implements the terminal part of the Basic Access Control and reads the logical MRTD being under Basic access Control.

3.3 Threats

51 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.

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

53 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 a communication through the contactless communication interface. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

54 **T.Skimming Skimming the logical MRTD**

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

55 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 printed on the MRTD data page but the attacker does not know this 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 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.

56 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 impose on an inspection system by means of the changed MRTD holders 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 an other identity of the traveller. 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 MRTD's to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveller into an other MTRD'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 in an other contactless chip.

57 The TOE shall avert the threat as specified below.

58 T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in TOE operational phase 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 state after delivery to MRTD holder.

59 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.

60 Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to

measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are 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).

61 T.Phys-Tamper Physical Tampering

An attacker may perform physical probing of the MRTD's chip in order (i) to disclose 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) to modify User Data or (iv) to modify TSF data.

The physical tampering may be focused directly on the discloser 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 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 prerequisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

62 T.MalfunctionMalfunction 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 or 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 misuse of administration function. To exploit this an attacker needs information about the functional operation.

3.4 Organisational Security Policies

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

64 P.Manufact Manufacturing of the MRTD's chip

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing. 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.

65 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 digitised 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 authorized agents of the issuing State or Organization only.

66 P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (DG1), the printed portrait and the digitised portrait (DG2), the biometric reference data of finger(s) (DG3), the biometric reference data of iris image(s) (DG4) and data according to LDS (DG5 to DG14, 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 Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [7]. The issuing State or Organization decides (i) to enable the Basic Access Control for the protection of the MRTD holder personal data or (ii) to disable the Basic Access Control to allow Primary Inspection Systems of the receiving States and all other terminals to read the logical MRTD.

4 Security Objectives

67 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

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

69 OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data groups DG1 to DG16, the Document security object according to LDS [6] and the TSF data can be written by authorized Personalization Agents. The logical MRTD data groups DG1 to DG16 and the TSF data can be written only once and can not be changed after personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups DG 3 to DG16 are added. Only the Personalization Agent shall be allowed to enable or to disable the TSF Basic Access Control.

70 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. If the TOE is configured for the use with Basic Inspection Terminals only the TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

71 OT.Data_Conf Confidentiality of personal data

If the TOE is configured for the use with Basic Inspection Systems the TOE must ensure the confidentiality of the logical MRTD data groups DG1 to DG16 by granting read access to terminals successfully authenticated by (i) as Personalization Agent or as (ii) Basic Inspection System. The Basic Inspection System shall authenticate themselves by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

If the TOE is configured for the use with Primary Inspection Systems no protection in confidentiality of the logical MRTD is required.

72 OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification Data in its non-volatile memory. The IC Identification Data must provide an unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". If the TOE is configured for use with Basic Inspection Terminals only in Phase 4 "Operational Use" the TOE shall identify themselves only to a successful authenticated Basic Inspection System or Personalization Agent.

73 OT.Prot_Abuse-Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded Software, (iii) to manipulate Soft-coded Smartcard Embedded 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.

74 The following TOE security objectives address the protection provided by the MRTD's chip independent on the TOE environment.

75 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.

76 OT.Prot_Phys-Tamper Protection against Physical Tampering

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or

- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

- manipulation of the hardware and its security features, as well as

- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

77 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.

4.2 Security Objectives for the Development and Manufacturing Environment

78 OD.Assurance Assurance Security Measures in Development and Manufacturing Environment

The developer and manufacturer ensure that the TOE is designed and fabricated so that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. This includes the use of the Initialization Data for unique identification of the TOE and the pre-personalization of the TOE including the writing of the Personalization Agent Authentication key(s). The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against obvious penetration attacks with low attack potential and against

direct attacks with high attack potential against security function that uses probabilistic or permutational mechanisms.

79 OD.Material Control over MRTD Material

The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, to initialise, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.

4.3 Security Objectives for the Operational Environment

Issuing State or Organization

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

81 OE.Personalization Personalization of logical MRTD

The issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the issuing State or Organisation (i) establish the correct identity of the holder and create biographic data for the MRTD, (ii) enrol 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 (including the digital signature in the Document Security Object). The Personalization Agents enable or disable the Basic Access Control function of the TOE according to the decision of the issuing State or Organization. If the Basic Access Control function is enabled the Personalization Agents generate the Document Basic Access Keys and store them in the MRTD's chip.

82 OE.Pass_Auth_SignAuthentication of logical MRTD by Signature

The Issuing State or Organization must (i) generate a cryptographic secure Country Signing Key Pair, (ii) ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity. The Issuing State or organization must (i) generate a cryptographic secure Document Signing 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 Signing Public Key to receiving States and organizations. The digital signature in the Document Security Object include all data in the data groups DG1 to DG16 if stored in the LDS according to [6].

Receiving State or organization

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

84 OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the Receiving State must examine the MRTD presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD.

85 OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the Receiving State uses the inspection system to verify the traveller 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 Signing Public Key maintaining their authenticity and availability in all inspection systems.

86 OE.Prot_Logical_MRTD Protection of data of the logical MRTD

The inspection system of the receiving State ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems). The receiving State examining the logical MRTD with Primary Inspection Systems will prevent eavesdropping to the communication between TOE and inspection system.

MRTD Holder

87 OE.Secure_Handling Secure handling of the MRTD by MRTD holder

The holder of a MRTD configured for use with Primary Inspection Systems (i.e. MTRD with disabled Basic Access Control) will prevent unauthorized communication of the MRTD's chip with terminals through the contactless interface.

5 Security Requirements

All SFRs contained in the PP are included in this ST. Refinements of the PP SFRs are marked by double underlining.

5.1 Security Functional Requirements for the TOE

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

5.1.1 Class FAU Security Audit

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

90 FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.

Dependencies: No dependencies.

5.1.2 Class Cryptographic Support (FCS)

91 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.

92 FCS_CKM.1/BAC_MRTD Cryptographic key generation – Generation of Document Basic Access Keys by the TOE

Hierarchical to: No other components.

FCS_CKM.1.1/ BAC_MRTD The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [7], Annex E.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

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

94 FCS_CKM.4 Cryptographic key destruction - MRTD

Hierarchical to: No other components.

FCS_CKM.4.1/ MRTD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion of key value that meets the following: FIPS PUB 140-2 [11].

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]
FMT_MSA.2 Secure security attributes

5.1.1.1 Cryptographic operation (FCS_COP.1)

95 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.

96 FCS_COP.1/SHA_MRTD Cryptographic operation – Hash for Key Derivation by MRTD

Hierarchical to: No other components.

FCS_COP.1.1/ SHA_MRTD	The TSF shall perform hashing in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: FIPS 180-2.

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
FMT_MSA.2 Secure security attributes

97 FCS_COP.1/TDES_MRTD Cryptographic operation – Encryption / Decryption Triple DES

Hierarchical to: No other components.

FCS_COP.1.1/ TDES_MRTD	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [12] and [7]; Annex E.

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
FMT_MSA.2 Secure security attributes

98 FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_MRTD	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).

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
FMT_MSA.2 Secure security attributes

5.1.1.2 Random Number Generation (FCS_RND.1)

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

100 FCS_RND.1/MRTD Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1/ MRTD	The TSF shall provide a mechanism to generate random numbers that meet the requirement to provide an entropy of at least 7.95 bit in each byte.

101 Dependencies: No dependencies.

5.1.2 Class FIA Identification and Authentication

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [7], Annex E, and [17]
Basic Access Control Authentication Mechanism	FIA_UAU.4/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/BAC_T, FIA_UAU.6/T	Triple-DES, 112 bit keys, Retail-MAC, 112 bit keys
Symmetric Authentication Mechanism for Personaliza-tion Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys

Table 1: Overview on authentication SFR

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

103 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow

(1) to read the Initialization Data in Phase 2 “Manufacturing”,

(2) to read the ATS in Phase 3 “Personalization of the MRTD”,

(3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,

(4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 “Operational Use”

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.

Dependencies: No dependencies.

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

105 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow

(1) to read the Initialization Data in Phase 2 “Manufacturing”,

(2) to read the ATS in Phase 3 “Personalization of the MRTD”,

(3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,

(4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 “Operational Use”

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.

Dependencies: FIA_UID.1 Timing of identification.

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

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

Hierarchical to: No other components.

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

1. Basic Access Control Authentication Mechanism,

2. Authentication Mechanism based on Triple-DES.

Dependencies: No dependencies.

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

109 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on Triple-DES

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 mechanisms
   (a) the Basic Access Control Authentication Mechanism with the Personalization Agent Keys,
   (b) the Symmetric Authentication Mechanism with the Personalization Agent Key
2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys .

Dependencies: No dependencies.

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

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

Hierarchical to: No other components.

FIA_UAU.6.1/ MRTD The TSF shall re-authenticate the user under the conditions each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

Dependencies: No dependencies.

5.1.3 Class FDP User Data Protection

5.1.3.1 Subset access control (FDP_ACC.1)

112 The TOE shall meet the requirement “Subset access control (FDP_ACC.1)” as specified below (Common Criteria Part 2). The instantiations of FDP_ACC.1 are caused by the TSF management according to FMT_MOF.1.

113 FDP_ACC.1 Subset access control – Primary Access Control

Hierarchical to: No other components.

FDP_ACC.1.1/ PRIM	The TSF shall enforce the Primary Access Control SFP on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD.

Dependencies: FDP_ACF.1 Security attribute based access control

114 FDP_ACC.1 Subset access control – Basic Access control

Hierarchical to: No other components.

FDP_ACC.1.1/ BASIC	The TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD.

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.3.2 Security attribute based access control (FDP_ACF.1)

115 The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (Common Criteria Part 2). The instantiations of FDP_ACC.1 address different SFP.

116 FDP_ACF.1 Security attribute based access control – Primary Access Control

Hierarchical to: No other components.

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

1. Subjects:
   a. Personalization Agent,
   b. Terminals,
2. Objects: data in the data groups DG1 to DG16 of the logical MRTD,
3. security attributes
   a. configuration of the TOE according to FMT_MOF.1

b. authentication status of terminals.

FDP_ACF.1.2/ PRIM: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: in the TOE configuration for use with Primary Inspection Systems

1. the successfully authenticated Personalization Agent is allowed to write the data of the data groups DG1 to DG16 of the logical MRTD,

2. the Terminals are allowed to read the data of the groups DG1 to DG16 of the logical MRTD.

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

FDP_ACF.1.4/ PRIM: The TSF shall explicitly deny access of subjects to objects based on the rule: the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD.

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

117 FDP_ACF.1/Basic Security attribute based access control – Basic Access Control

Hierarchical to: No other components.

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

1. Subjects:

   a. Personalization Agent,

   b. Basic Inspection System,

   c. Terminal,

2. Objects: data in the data groups DG1 to DG16 of the logical MRTD

3. Security attributes

   a. configuration of the TOE according to FMT_MOF.1

   b. authentication status of terminals.

FDP_ACF.1.2/ BASIC: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: in the TOE configuration for use with Basic Inspection Systems only

1. the successfully authenticated Personalization Agent is

allowed to write and to read the data of the data groups DG1 to DG16 of the logical MRTD,

2. the successfully authenticated Basic Inspection System is allowed to read data of the groups DG1 to DG16 of the logical MRTD.

FDP_ACF.1.3/ BASIC	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ BASIC	The TSF shall explicitly deny access of subjects to objects based on the rule: the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD.

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

5.1.3.3 Inter-TSF-Transfer

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

119 FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

FDP_UCT.1.1/ MRTD	The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorised disclosure.

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]

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

121 FDP_UIT.1/MRTD Data exchange integrity - MRTD

Hierarchical to: No other components.

FDP_UIT.1.1/ MRTD	The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.
FDP_UIT.1.2/ MRTD	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

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]

5.1.4 Class FMT Security Management

122 The TOE shall meet the requirement “Management of functions in TSF (FMT_MOF.1)” as specified below (Common Criteria Part 2).

123 FMT_MOF.1 Management of functions in TSF

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to enable and disable the functions TSF Basic Access Control to Personalization Agent.

Dependencies: No Dependencies

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

125 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

a) Initialization,

b) Personalization

c) Configuration.

Dependencies: No Dependencies

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

127 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Primary Inspection System,

4. Basic Inspection System.

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

Hierarchical to: FIA_UID.1 Timing of identification.

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

129 FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.2 Limited availability.

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

131 FMT_LIM.2 Limited availability

Hierarchical to: No other components.

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.

Dependencies: FMT_LIM.1 Limited capabilities.

132 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.

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

Hierarchical to: No other components.

FMT_MTD.1.1/ INI_ENA: The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

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

134 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.

FMT_MTD.1.1/ INI_DIS: The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_WRITE: The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none.

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

5.1.5 Class FPT Protection of the Security Functions

137 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 SFR “Non-bypassability of the TSP (FPT_RVM.1)” and “TSF domain separation (FPT_SEP.1)” together with “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

138 The TOE shall meet the requirement “Subset information flow control (FDP_IFC.1)” as specified below:

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information enabling access to Personalization Agent Authentication Key and none.
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Authentication Key and none.

Dependencies: No other components.

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

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

141 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

(1) exposure to operating conditions where therefore a malfunction could occur,

(2) failure detected by TSF according to FPT_TST.1.

Dependencies: ADV_SPM.1 Informal TOE security policy model

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

143 FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1 The TSF shall run a suite of self tests [*selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*][*assignment: conditions under which self test should occur*] to demonstrate the correct operation of the TSF.

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

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

Dependencies: FPT_AMT.1 Abstract machine testing.

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

145 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

146 The following security functional requirements protect the TSF against bypassing. and support the separation of TOE parts.

147 The TOE shall meet the requirement “Non-bypassability of the TSP (FPT_RVM.1)” as specified below (Common Criteria Part 2).

148 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

149 The TOE shall meet the requirement “TSF domain separation (FPT_SEP.1)” as specified below (Common Criteria Part 2).

150 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2 Security Assurance Requirements for the TOE

151 The 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:

ADV_IMP.2 and ALC_DVS.2.

152 The minimum strength of function is SOF-high.

153 This security target does not contain any security functional requirement for which an explicit stated strength of function claim is required.

5.3 Security Requirements for the IT environment

154 This section describes the security functional requirements for the IT environment using the CC part 2 components.

155 Due to CCIMB Final Interpretation #58 these components are editorial changed to express the security requirements for the components in the IT environment where the original components are directed for TOE security functions. The editorial changes are indicated in **bold**.

5.3.1 Passive Authentication

156 The ICAO, the Issuing States or Organizations and the Receiving States or Organization run a public key infrastructure for the Passive Authentication. This public key infrastructure distributes and protects the Country Signing CA Keys and the Document Signing Keys to support the signing of the User Data (DG1 to DG16) by means of the Document Security Object. The Technical Report [7] describes the requirements to the public key infrastructure for the Passive Authentication.

157 The Document Signer of the Issuing State or Organization shall meet the requirement "Basic data authentication (FDP_DAU.1)" as specified below (Common Criteria Part 2).

158 FDP_DAU.1/DS Basic data authentication – Passive Authentication

Hierarchical to: No other components.

FDP_DAU.1.1/ DS	The **Document Signer** shall provide a capability to generate evidence that can be used as a guarantee of the validity of logical the MRTD (DG1 to DG16) and the Document Security Object.
FDP_DAU.1.2/ DS	The **Document Signer** shall provide Inspection Systems of Receiving States or Organization with the ability to verify evidence of the validity of the indicated information.

Dependencies: No dependencies

5.3.2 Basic Inspection Systems

159 This section describes common security functional requirements to the Basic Inspection Systems and the Personalization Agent if it uses the Basic Access Control Mechanism with the Personalization Agent Authentication Keys. Both are called "Basic Terminals" (BT) in this section.

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

161 FCS_CKM.1/BAC_BT Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal

Hierarchical to: No other components.

FCS_CKM.1.1/ BAC_BT	The **Basic Terminal** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [7], Annex E.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

162 FCS_CKM.4/BT Cryptographic key destruction - BT

Hierarchical to: No other components.

FCS_CKM.4.1/BT The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion of key value that meets the following: FIPS PUB 140-2 [11].

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]
FMT_MSA.2 Secure security attributes

163 The Basic Terminal 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 Basic Terminal.

164 FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/SHA_BT The **Basic Terminal** shall perform hashing in accordance with a specified cryptographic algorithms SHA-1 and cryptographic key sizes none that meet the following: FIPS 180-2.

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
FMT_MSA.2 Secure security attributes

165 FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/ENC_BT The **Basic Terminal** shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2).

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
FMT_MSA.2 Secure security attributes

166 FCS_COP.1/MAC_BT Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_BT: The **Basic Terminal** shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail-MAC and cryptographic key sizes 112 bit that meet the following: FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2).

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
FMT_MSA.2 Secure security attributes

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

168 FCS_RND.1/BT Quality metric for random numbers - Basic Terminal

Hierarchical to: No other components.

FCS_RND.1.1/BT: The **Basic Terminal** shall provide a mechanism to generate random numbers that meets the requirement to provide an entropy of at least 7.95 bit in each byte.

Dependencies: No dependencies.

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

170 FIA_UAU.4/BT Single-use authentication mechanisms – Basic Terminal

Hierarchical to: No other components.

FIA_UAU.4.1/BT: The **Basic Terminal** shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism.

Dependencies: No dependencies.

171 The Basic Terminal shall meet the requirement “Re-authentication (FIA_UAU.6)” as specified below (Common Criteria Part 2).

172 **FIA_UAU.6/BT Re-authentication - Basic Terminal**

Hierarchical to: No other components.

FIA_UAU.6.1/BT The **Basic Terminal** shall re-authenticate the user under the conditions each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

Dependencies: No dependencies.

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

174 FDP_UCT.1/BT Basic data exchange confidentiality - Basic Terminal

Hierarchical to: No other components.

FDP_UCT.1.1/BT The **Basic Terminal** shall enforce the Basic Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorised disclosure.

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]

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

176 FDP_UIT.1/BT Data exchange integrity - Basic Terminal

Hierarchical to: No other components.

FDP_UIT.1.1/BT The **Basic Terminal** shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.

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

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]

5.3.3 Personalization Terminals

177 The TOE supports different authentication and access control mechanisms which may be used for the Personalization Agent depending on the personalization scheme of the Issuing State or Organization:

(1) The Basic Access Control Mechanism which may be used by the Personalization Agent with a Personalization Agent Secret Key Pair. The Basic Access Control

Mechanism establishes strong cryptographic keys for the secure messaging to ensure the confidentiality by Triple-DES and integrity by Retail-MAC of the transmitted data. This approach may be used in a personalization environment where the communication between the MRTD's chip and the personalization terminal may be listen or manipulated.

(2) In a centralized personalization scheme the major issue is high productivity of personalization in a high secure environment. In this case the personalization agent may wish to reduce the protocol to symmetric authentication of the terminal without secure messaging. Therefore the TOE and the Personalization Terminal support a simple protocol as requested by the SFR FIA_UAU.4/MRTD and FIA_API.1/SYM_PT.

178 The Personalization Terminal shall meet the requirement "Authentication Prove of Identity (FIA_API)" as specified below (Common Criteria Part 2 extended).

179 FIA_API.1/SYM_PT Authentication Proof of Identity - Personalization Terminal Authentication with Symmetric Key

Hierarchical to: No other components.

FIA_API.1.1/ SYM_PT	The **Personalization Terminal** shall provide a Authentication Mechanism based on Triple-DES to prove the identity of the Personalization Agent.

Dependencies: No dependencies.

6 TOE Summary Specification

180 This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

6.1 TOE Security Functions

181 This chapter gives the overview description of the different TOE Security Functions composing the TSF.

182 In the following table all TOE Security Functions with a SOF claim are listed. The assessment of cryptographic algorithms is not part of this CC evaluation.

TOE Security Function	*SOF claim*	*Description*
F.RNG	high	Random numbers can be analyzed with probabilistic methods.
F.HW_DES	high	The quality can be analyzed with probabilistic methods on side-channels.
F.Identifcation_Authentication	high	The mechanism for identification/authentication of the roles is probabilistic.
F.Secure_Messaging	high	The mechanism for identification/authentication and confidentiality of communication is

TOE Security Function	*SOF claim*	*Description*
		probabilistic.

183

6.1.1 TOE Security Functions from Hardware (IC)

184 Some SFs have additional information appended.

6.1.1.1 F.RNG – Random Number Generator

185 The random number generator continuously produces random numbers with a length of one byte. The TOE implements the F.RNG by means of a physical hardware random number generator working stable within the limits guaranteed by F.OPC (operational conditions).

186 The TSF provides a hardware test functionality that can be used by the Smartcard Embedded Software to detect faults in the hardware implementing the random number generator.

187 According to AIS31 the random number generator claims the fulfilment of the requirements of functionality class P2. This means that the random number generator is suitable for generation of signature key pairs, generation of session keys for symmetric encryption mechanisms, random padding bits, zero-knowledge proofs and generation of seeds for DRNGs.

188 Addition:

189 These random numbers are used in:

- the anticollision phase of the chip in phase 4 to create communication identification data and
- the creation of a session key and authentication nonces.

6.1.1.2 F.HW_DES – Triple-DES Co-processor

190 The TOE provides the Triple Data Encryption Algorithm (TDEA) according to the Data Encryption Standard (DES). F.HW_DES is a modular basic cryptographic function which provides the TDEA algorithm as defined by FIPS PUB 46 by means of a hardware co-processor and supports (a) the 3-key Triple-DEA algorithm according to keying option 1 and (b) the 2-key Triple DEA algorithm according to keying option 2 in FIPS PUB 46-3 [12]. The two/three 56 bit keys (112/168 bit) for the 2-key/3-key Triple DES algorithm shall be provided by the Smartcard Embedded Software. For encryption the Smartcard Embedded Software provides 8 bytes of the plain text and F.HW_DES calculates 8 bytes cipher text. The calculation output is read by the Smartcard Embedded Software. For decryption the Smartcard Embedded Software also provides 8 bytes of cipher text and F.HW_DES calculates 8 bytes plain text. The calculation output is read by the Smartcard Embedded Software.

191 Addition:

192 This SF is used in all cases where DES/3DES is used.

6.1.1.3 F.OPC – Control of Operating Conditions

193 The function F.OPC ensures the correct operation of the TOE (functions offered by the micro- controller including the standard CPU as well as the Triple-DES co-processor, AES co-processor, the arithmetic co-processor, the memories, registers, I/O interfaces and the other system peripherals) during the execution of the IC Dedicated Support Software and Smartcard Embedded Software. This includes all specific security features of the TOE which are able to provide an active response.

194 The TOE ensures its correct operation and prevents any malfunction using the following sub- functions: filtering of power supply and clock input as well as monitoring of power supply, the frequency of the clock and the temperature of the chip by means of sensors. There are multiple sensors for the different ISO 7816 supply voltage classes and the contact-less operation mode. Light sensors are distributed over the chip surface and used to detect light attacks. The thresholds allowed for these parameters are defined within the range where the TOE ensures its correct operation. Additionally to the light sensors the EEPROM provides two functions to detect light attacks. The Smartcard Embedded Software can select one function and also disable both functions of the EEPROM detection function.

195 Specific functional units of the TOE are equipped with special circuitry to detect a number of single fault injection attacks: The Program Counter, the stack pointer, the logic that implements the PSWH register, the DES co-processor and the FameXE co-processor.

196 If one of the monitored parameters is out of the specified range, either (i) a reset is forced and the actual running program is aborted or (ii) an exception is raised which interrupts the program flow and allows a reaction of the Smartcard Embedded Software. A reset is forced by the sensors for voltage, frequency, temperature and light. An exception is forced by the EEPROM light detector and the single fault injection detection circuitry. If the TOE is reset all components of the TOE are initialised with their reset values. In addition the TOE provides a reset cause indicator to the Smartcard Embedded Software. In the case an exception is raised an indicator for the reason of the exception is provided.

197 Before TOE delivery the Test Mode is disabled. In all other modes except the Test Mode the TOE enables the sensors automatically when operated. Furthermore the TOE prevents that the Smartcard Embedded Software disables the sensors. The assignment which sensor raises an exception or forces a reset is hard-wired and cannot be changed by software.

198 In addition, the TOE controls the specified range of the stack pointer. The stack pointer and the control logic is implemented threefold for the User Mode, System Mode and Super System Mode (comprising Boot Mode, Test Mode and Mifare Mode). In case the specified limits are reached an exception is generated.

199 Beside the sensors the security function comprises an additional sensor to check the high voltage for the write process to the EEPROM during every write sequence. The

result of this sensor must be read from a Special Function Register and does not force an automatic event (e.g. exception).

6.1.1.4 F.PHY – Protection against Physical Manipulation

200 The function F.PHY protects the TOE against manipulation of (i) the hardware, (ii) the IC Dedicated Software in the ROM, (iii) the Smartcard Embedded Software in the ROM and the EEPROM, (iv) the application data in the EEPROM and RAM including the configuration data in the security row. It also protects User Data or TSF data against disclosure by physical probing when stored or while being processed by the TOE.

201 The protection of the TOE comprises different features within the design and construction which make reverse-engineering and tamper attacks more difficult. These features comprise dedicated shielding techniques for different components and specific encryption features for the memory blocks. The security function F.PHY supports the efficiency of other security functions.

202 F.PHY also supports the integrity of the EEPROM and the ROM. The EEPROM is able to correct a 1-bit error within each byte. The ROM provides a parity check. The EEPROM corrects errors automatically without user interaction, a ROM parity error forces a reset.

6.1.1.5 F.LOG – Logical Protection

203 The function F.LOG implements measures to limit or eliminate the information that might be contained in the shape and amplitude of signals or in the time between events found by measuring such signals. This comprises the power consumption and signals on the other pads that are not intended by the terminal or the Smartcard Embedded Software. Thereby this security function prevents the disclosure of User Data or TSF data stored and/or processed in the smartcard IC through the measurement of the power consumption and subsequent complex signal processing. The protection of the TOE comprises different features within the design that support the other security functions.

204 The Triple-DES co-processor includes special features to prevent SPA/DPA analysis of shape and amplitude of the power consumption and ensures that the calculation time is independent from any key and plain/cipher text.

205 Specific features as described for the function F.PHY (e.g. the encryption features) and for the function F.OPC (e.g. the filter feature) support the logical protection.

6.1.1.6 F.COMP – Protection of Mode Control

206 The function F.COMP provides a control of the CPU mode for (i) Boot Mode, (ii) Test Mode and (iii) Mifare Mode. This includes the protection of electronic fuses stored in a protected memory area, the so-called "Security Row", and the possibility to store initialisation or pre- personalisation data in the so-called "FabKey Area".

207 The control of the CPU mode according to Boot Mode, Test Mode and Mifare Mode prevents the abuse of test functions after TOE delivery. Additionally it also ensures that features used at boot time to configure the TOE can not be abused. The initial but not user visible CPU mode is the Boot Mode. Hardware circuitry determines whether the

Test Mode is available or not. If it is available, the TOE starts the IC Dedicated Test Software in the Test Mode. Otherwise, the TOE switches to the System Mode the initial user visible CPU mode and starts execution of the Smartcard Embedded Software.

208 The protection of electronic fuses ensures the secure storage of configuration- and calibration data stored in the Test Mode. F.COMP protects CPU mode changes regarding Boot Mode, Test Mode and Mifare Mode in the following way: Switches from Boot Mode to Test Mode or Mifare Mode are allowed, switches from these two modes back to Boot Mode are prevented. The switch to the Test Mode is prevented after TOE delivery, therefore it is permanently disabled. F.COMP also ensures that the Boot Mode is only active during the boot phase of the TOE after every reset and cannot be invoked afterwards. Therefore, once the TOE has left the test phase and every time the TOE has started up, the Mifare Mode is the only CPU mode available when the PSWH.SSM bit is set. All three CPU modes Boot Mode, Test Mode and Mifare Mode are meant with "Super System Mode" and F.COMP controls which mode is used if the PSWH.SSM bit indicates the Super System Mode.

209 The TSF controls access to the Security Row, within the EEPROM memory, accessible at reserved addresses within the memory map. The available EEPROM memory space for the Smartcard Embedded Software is reduced by this area. F.COMP provides three memory areas within the security row that can be used by the Smartcard Embedded Software:

- the User Read Only Area
- the User Write Protected Area and
- the User Write Once Area.

210 The User Read Only Area contains 32 bytes that are read-only for the Smartcard Embedded Software. The User Write Protected area contains 16 bytes that can be write-protected by the Smartcard Embedded Software on demand. The User Write Once Area contains 32 bytes in which each bit independently can be once set to `1' not reset to `0'.

211 F.COMP also provides the FabKey Area in which initialisation or identification data can be stored. The FabKey area does not belong to the Security Row and is not protected by hardware mechanisms.

212 For all areas the initial values are set during chip testing and pre-personalisation. They depend on the choice of the Smartcard Embedded Software developer and are included in the Order Entry Form. The User Write Protected Area and the User Write Once Area are designed to store the identification of a (fully personalised) smartcard or a sequence of events over the life cycle that can be coded by an increasing number of bits set to "one" or protecting bytes, respectively.

213 F.COMP limits the capabilities of the test functions and provides test personnel during phase 2 with the capability to store the identification and/or pre-personalisation data and/or supplements of the Smartcard Embedded Software in the EEPROM. The security function F.COMP maintains the security domain for its own execution that protects it from interference and tampering by untrusted subjects both in the Test Mode and in the

other modes. It also enforces the separation between the security domains of subjects regarding the IC Dedicated Software and the Smartcard Embedded Software.

214 Addition:

215 This SF is used to store the chip identification data in the User Read Only Area.

6.1.2 TOE Security Functions from Embedded Software (ES)

6.1.2.1 F.Access_Control

216 This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. This function consists of following elements:

1. Access to objects is controlled based on subjects, objects and attributes.

2. No access control policy allows reading of any key.

3. Access Control in phase 2b - initialization - enforces initialization policy: Configuration and initialization of the TOE only by the manufacturer or on behalve of him. (See **F.Initialization_Prepersonalization**.)

4. Access Control in phase 2c – pre-personalization – enforces pre-personalization policy: Creation of the ICAO file structure, configuring of access control policy, doing key management and reading of initialization data only by the pre-personalization agent. (See **F.Initialization_Prepersonalization**.)

5. Access Control in phase 3 – personalization – enforces personalization policy: Writing of user data, doing key management, e.g. BAC key, and reading of initialization data only by the personalization agent. (See **F.Personalization**.)

6. Access Control in phase 4 – operation – enforces operational use policy: Read only. Depending on configuration made in phase 2 enforcement of PIS or BIS policy.

6.1.2.2 F.Deactivate_Non_TSF

217 This security function limits the available commands in the different life cycles.

6.1.2.3 F.Identification_Authentication

218 This function provides identification/authentication of user roles:

- Pre-personalization agent
- Personalization agent
- BIS

219 Each of these roles is identified/authenticated with at least one specific key.

220 It uses for this the Basic Access Control [18] authentication method which has following properties:

1. Requires a challenge fetched directly before this function from the TOE.
2. The cryptographic method for confidentiality is Triple-DES/CBC.
3. The cryptographic method for authenticity is DES/Retail MAC.
4. The cryptographic method for key derivation is SHA-1. The SHA-1 algorithm is compliant to FIPS 180-2. [13]

221 Keys in transient memory are overwritten after usage.

222 On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.

223 On success the generated session key is stored for **F.Secure_Messaging**.

6.1.2.4 F.Initialization_Prepersonalization

224 This function is performed by the pre-personalization agent in phases 2b (initialization) and 2c (pre-personalization).

6.1.2.5 F.Personalization

225 This function is performed by the personalization agent in phase 3.

226 The agent does for this function following steps:

- Formatting of all data to be stored on the TOE according to ICAO requirements which are outside the scope of the TOE. The data to be formated includes the index file EF.COM, the data groups – e.g. DG1 with the MRZ – and the passive authentication data with a signature over all data.
- If BIS policy: Deriving of the Basic Access Control key from the Machine Readable Zone data as specified in TrPKI [18] and writing it to the TOE.
- Writing of all the required data to the appropriate files as specified in TrLDS [17].
- Changing the TOE into the end-usage mode for phase 4.

227 Operations on the TOE are regulated according to **F.Access_Control**.

6.1.2.6 F.Retry_Counter

228 The retry counter (RTC) reacts to failed authentication procedures whereby it limits the number of consecutively failed authentication procedures to a specified maximum. When this limit is reached the respective key is blocked against further usage.

229 Reasons for authentication failures are e.g.:

- Wrong MAC

- Wrong challenge

230 All administrative keys used in phases 2c and 3 use this SF to limit the consecutively failed authentication procedures to three.

231 The MRZ derived key used for BIS policy must not be protected with this SF as this could introduce practical problems, i.e. accidently blocked and hence unusable passports.

6.1.2.7 F.Secure_Messaging

232 This security function implements a secure communication channel with following parameters:

1. The Secure Messaging is as specified in Basic Access Control.
2. In phases 3 – 4 a session key is used.
3. The cryptographic method for confidentiality is Triple-DES/CBC.
4. The cryptographic method for authenticity is DES/Retail MAC.
5. In a Secure Messaging protected command it must be the method for confidentiality and the method for authenticity present.
6. The initialization vector is changed after each command according to [7].
7. Any non Secure Messaging protected command overwrites the session key and requires new authentication via **F.Identification_Authentication**.
8. Overwrites keys in transient memory after usage.

6.1.2.8 F.Verification

233 This function ensures correct operation.

6.2 Assurance Measures

234 The assurance measures fulfilling the requirements of EAL4 augmented with ADV_IMP.2 and ALC_DVS.2 are:

Assurance Measure	***Description***
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation and startup
ADV_FSP.2	Fully defined external interfaces

Assurance Measure	*Description*
ADV_HLD.2	Security enforcing high-level design
ADV_LLD.1	Implementation of the TSF
ADV_IMP.2	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.2	Validation of analysis
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Independent vulnerability analysis

7 PP Claims

7.1 PP Reference

235 The conformance of this ST to the Common Criteria Protection Profile – Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.0, BSI-PP-0017 is claimed.

7.2 PP Refinements

236 None.

7.3 PP Additions

237 None.

8 Rationale

8.1 Security Objectives Rationale

238 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.Malfunction	OD.Assurance	OD.Material	OE.Personalization	OE.Pass_Auth_Sign	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD	OE.Secure_Handling
T.Chip-ID				x												x
T.Skimming			x													x
T.Eavesdropping			x												x	
T.Forgery	x	x					x					x	x	x		
T.Abuse-Func					x											
T.Information_Leakage						x										
T.Phys-tamper							x									
T.Malfunction								x								
P.Manufact									x	x						
P.Personalization	x								x		x					
P.Personal_Data		x	x													
A.Pers_Agent											x					
A.Insp_Sys													x		x	

Table 1: Security Objective Rationale

239 The OSP **P.Manufact** “Manufacturing of the MRTD’s chip” requires the quality and integrity of the manufacturing process and control the MRTD’s material in the Phase 2 Manufacturing including unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data. The security objective for the TOE environment **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment” address these obligations of the IC Manufacturer and MRTD Manufacturer.

240 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 **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment”. The security objective OT.AC_Pers limits the management of TSF data and the management of TSF (enabling and disabling of the TSF Basic Access Control) to the Personalization Agent.

241 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 Basic 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“ which describes the unconditional protection of the integrity of the stored data and the configurable integrity protection during the transmission. The

security objective OT.Data_Conf “Confidentiality of personal data” describes the protection of the confidentiality as configured by the Personalization Agent acting in charge of the issuing State or Organization.

242 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 contactless communication interface. In case of TOE configuration for use with Basic Inspection Terminals only this threat is countered as described by the security objective **OT.Identification** by Basic Access Control. If the TOE is configured for use with Primary Inspection Systems this threat shall be adverted by the TOE environment as described by **OE.Secure_Handling**.

243 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 contactless interface or listening the communication between the MRTD’s chip and a terminal. In case of TOE configuration for use with Basic Inspection Terminals only this threat is countered by the security objective OT.Data_Conf through Basic Access Control. If the TOE is configured for use with Primary Inspection Systems the threat T.Skimming shall be adverted by the TOE environment according to **OE.Secure_Handling** “Secure handling of the MRTD by MRTD holder” and the threat T.Eavesdropping shall be adverted by **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD”.

244 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 an additional contactless 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”.

245 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. The protection of the TOE against this threat is addressed by the directly related security objective **OT.Prot_Abuse-Func**. The security objective for the TOE environment **OD.Material** “Control over MRTD Material” ensures the control of the MRTD material. The security objectives for the TOE environment **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment” and **OE.Personalization** “Personalization of logical MRTD” ensure 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.

246 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 are 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”.

247 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 and the enabling of security features of the TOE according to the decision of the Issuing State or Organization concerning the Basic Access Control.

248 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”. If the Issuing State of Organization decides to protect confidentiality of the logical MRTD than the security objectives for the TOE environment **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD” will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling. If the Issuing State of Organization decides to configure the TOE for use with Primary Inspection Systems than no protection of the logical MRTD data is required by the inspection system.

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements Rationale

249 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.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1/BAC_MRTD	(x)	x	(x)					
FCS_CKM.4	(x)		x					
FCS_COP.1/SHA_MRTD	x	x	(x)					
FCS_COP.1/TDES_MRTD	x	x	x					
FCS_COP.1/MAC_MRTD	x	x	x					
FCS_RND.1/MRTD	(x)	x	x					
FIA_UID.1			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4/MRTD	x	x	x					
FIA_UAU.5/MRTD	x	x	x					
FIA_UAU.6/MRTD	x	x	x					
FDP_ACC.1/PRIM	x	x						
FDP_ACF.1/PRIM	x	x						
FDP_ACC.1/BASIC	x	x	x					
FDP_ACF.1/BASIC	x	x	x					
FDP_UCT.1/MRTD	x	x	x					
FDP_UIT.1/MRTD	x	x	x					
FMT_MOF.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						
FPT_EMSEC.1	x				x			
FPT_TST.1					x		x	
FPT_RVM.1								x
FPT_FLS.1	x				x		x	
FPT_PHP.3	x				x	x		
FPT_SEP.1							x	x

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

250 The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD and the management of the TSF for Basic Access Control. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/PRIM and FDP_ACF.1/BASIC in the same way: only the successfully authenticated

Personalization Agent is allowed to write the data of the groups DG1 to 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/MRTD and FIA_UAU.5/MRTD. In case the Basic Access Control Authentication Mechanism was used the SFR FIA_UAU.6/MRTD describes the re-authentication and FDP_UCT.1/MRTD and FDP_UIT.1/MRTD the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/BAC_MRTD, FCS_CKM.4, FCS_COP.1/SHA_MRTD, FCS_RND.1/MRTD (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD 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) because the Personalization Agent handles the configuration of the TSF Basic Access Control according to the SFR FMT_MOF.1 and the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data if Basic Access Control is enabled. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

251 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/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/PRIM and FDP_ACF.1/BASIC in the same way: only the Personalization Agent is allowed to write the data of the groups DG1 to DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups DG1 to 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).

If the TOE is configured for the use with Basic Inspection Terminals only by means of FMT_MOF.1 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. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD. The SFR FIA_UAU.6/MRTD, 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/BAC_MRTD, FCS_COP.1/SHA_MRD, FCS_RND.1/MRTD (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys.

252 The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups DG1 to DG16 if the TOE is configured for the use with Basic Inspection Systems by means of FMT_MOF.1. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. The read access to the logical MRTD data is defined by the FDP_ACC.1/BASIC and FDP_ACF.1.2/BASIC: only the

successful authenticated Personalization Agent and the successful authenticated Basic Inspection System are allowed to read the data of the logical MRTD. The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA_UAU.4/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5/MRTD enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6/MRTD requests secure messaging after successful authentication of the terminal with Basic 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/TDES_MRTD and FCS_COP.1/MAC_MRTD (cf. the SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD). (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode. The SFR FCS_CKM.1/BAC_MRTD, FCS_CKM.4, FCS_COP.1/SHA_MRTD and FCS_RND.1/MRTD 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 Basic Access Keys.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5/MRTD requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging. If the TOE is configured for the use with Primary Inspection Systems, no protection in confidentiality of the logical MRTD is needed to ensure.

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

Furthermore, if the TOE is configured for use with Basic Inspection Terminals the TOE shall identify themselves only to a successful authenticated Basic 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. The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their use 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 Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt.

254 The security objective **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality” is ensured by (i) 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, (ii) the SFR FPT_RVM.1 which prevents by monitoring the bypass and deactivation of security features or functions of the TOE, and (iii) the SFR FPT_SEP.1 which prevents change or explore security features or functions of the TOE by means of separation the other TOE functions.

255 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.

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

257 The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstare the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction, and (iii) the SFR FPT_SEP.1 limiting the effects of malfunctions due to TSF domain separation.

258 The following table provides an overview how security functional requirements for the IT environment cover security objectives for the TOE environment. The protection profile describes only those SFR of the IT environment directly related to the SFR for the TOE. It does not state any SFR for the IT environment supporting the security objectives OD.Assurance and OD.Material. The OE.Exam_MRTD uses only security function of the IT environment, i.e. the passive authentication. The security objective OE.Prot_Logical_MRTD is directed to Basic Inspection Systems only which cooperate with the TOE in protection of the logical MRTD.

	OD.Assurance	OD.Material	OE.Personalization	OE.Exam_MRTD	OE.Pass_Auth_Sign	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
Document Signer							
FDP_DAU.1/DS				x	x	x	
Terminal							
FCS_CKM.1/BAC_BT			(x)				x
FCS_CKM.4/BT			(x)				x
FCS_COP.1/SHA_BT			(x)				x
FCS_COP.1/ENC_BT			(x)				x
FCS_COP.1/MAC_BT			(x)				x
FCS_RND.1/BT			(x)				x
FIA_UAU.4/BT			(x)				x
FIA_UAU.6/BT			(x)				x
FDP_UCT.1/BT			(x)				x
FDP_UIT.1/BT			(x)				x
Personalization Agent							
FIA_API.1/SYM_PT			(x)				

Table 3: Coverage of Security Objectives for the IT environment by SFR

259 The security objective **OE.Exam_MRTD** “Examination of the MRTD passport book” requires the inspection system to verify the passport, the security objective **OE.Pass_Auth_Sign** “Authentication of logical MRTD by Signature” requires the issuer to provide Passive Authentication infrastructure and the security objective **OE.Passive_Auth_Verif** “Verification by Passive Authentication” requires the inspection system to verify the digital signature and data. The document signer provides the security function Passive Authentication according to FDP_DAU.1/DS to support the inspection system to verify the logical MRTD.

260 The security objective **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD“ address the protection of the logical MRTD during the transmission and internal handling. The SFR FIA_UAU.4/BT and FIA_UAU.6/BT address the terminal part of the Basic Access Control Authentication Mechanism and FDP_UCT.1/BT and FDP_UIT.1/BT the secure messaging established by this mechanism. The SFR FCS_CKM.1/BAC_BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT and FCS_RND.1/BT are necessary to implement this mechanism. The BIS shall destroy the Document Access Control Key and the secure messaging key after inspection of the MRTD because they are not needed any more (FCS_CKM.4/BT).

261 The **OE.Personalization** “Personalization of logical MRTD” requires the personalization terminal to authenticate themselves to the MRTD’s chip to get the write authorization. This implies to implement the Basic Access Control Authentication Mechanism (SFRs FCS_CKM.1/BAC_BT, FCS_CKM.4/BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT, FCS_RND.1/BT, FIA_UAU.4/BT, FIA_UAU.6/BT, FDP_UCT.1/BT,

FDP_UIT.1/BT) with the Personalization Agent Authentication Keys or support the symmetric authentication protocol according to the SFR FIA_API.1/SYM_PT.

262 For dependency rationale (SFR/SAR) see PP 7.2.2.

8.2.2 TOE Summary Specification Rationale

263 This shows the coverage of the SFRs by TSFs.

	F.RNG	F.HW_DES	F.OPC	F.PHY	F.LOG	F.COMP	F.Access_Control	F.Deactivate_Non_TSF	F.Identification_Authentication	F.Initialization_Prepersonalization	F.Personalization	F.Retry_Counter	F.Secure_Messaging	F.Verification
FAU_SAS.1						x								
FCS_CKM.1/BAC_MRTD											x			
FCS_CKM.4									x				x	
FCS_COP.1/SHA_MRTD									x					
FCS_COP.1/TDES_MRTD		x											x	
FCS_COP.1/MAC_MRTD		x											x	
FCS_RND.1/MRTD	x													
FIA_UID.1							x							
FIA_UAU.1							x							
FIA_UAU.4/MRTD	x												x	
FIA_UAU.5/MRTD									x					
FIA_UAU.6/MRTD													x	
FDP_ACC.1/PRIM							x							
FDP_ACF.1/PRIM							x							
FDP_ACC.1/BASIC							x							
FDP_ACF.1/BASIC							x							
FDP_UCT.1/MRTD													x	
FDP_UIT.1/MRTD													x	
FMT_MOF.1										x	x			
FMT_SMF.1										x	x			
FMT_SMR.1									x					
FMT_LIM.1						x		x						
FMT_LIM.2						x		x						
FMT_MTD.1/INI_ENA						x	x							
FMT_MTD.1/INI_DIS								x			x			
FMT_MTD.1/KEY_WRITE							x							
FMT_MTD.1/KEY_READ							x							
FPT_EMSEC.1		x			x							x		
FPT_FLS.1			x											
FPT_TST.1				x										x
FPT_PHP.3				x										
FPT_RVM.1							x							
FPT_SEP.1						x		x						

Table 4: Coverage of SFRs for the TOE by TSFs.

264 The SFR **FAU_SAS.1** requires the storage of the chip identification data which is addressed in the addition to **F.COMP**.

265 The SFR **FCS_CKM.1/BAC_MRTD** requires the generation of the document Basic Access Control key which is done by the personalization agent in **F.Personalization** (“If BIS policy: Deriving of the Basic Access Control key ...”).

266 The **SFR FCS_CKM.4** requires the destroying of cryptographic keys. This is done in **F.Identification_Authentication** (“Keys in transient memory are overwritten after usage.”) and **F.Secure_Messaging** (“Overwrites keys in transient memory after usage”).

267 The SFR **FCS_COP.1/SHA_MRTD** requires the SHA-1 algorithm which is provided by **F.Identification_Authentication** (Item 4).

268 The SFR **FCS_COP.1/TDES_MRTD** requires Triple-DES in CBC mode for data confidentiality. **F.Secure_Messaging** (Item 3) uses Triple-DES/CBC as specified in the Basic Access Control specification. [7] Triple-DES is used from **F.HW_DES** (See addition there).

269 The SFR **FCS_COP.1/MAC_MRTD** requires Triple-DES in retail-MAC mode for data authenticity. **F.Secure_Messaging** (Item 4) uses Triple-DES/retail-MAC as specified in the Basic Access Control specification. [7] DES and Triple-DES are used from **F.HW_DES** (See addition there).

270 The SFR **FCS_RND.1/MRTD** requires the generation of random numbers which is provided by **F.RNG**. F.RNG produces cryptographically strong random numbers which are used at the appropriate places as written in the addition there.

271 The SFR **FIA_UID.1** requires timing of identification. It is handled by **F.Access_Control** which enforces identification of a role before access is granted (“...only executed after this TSF allowed access.”). Also all policies there besides PIS in phase 4 prevent reading sensitive or user dependent data without user identification.

272 The SFR **FIA_UAU.1** requires timing of authentication. It is handled by **F.Access_Control** which enforces authentication of a role before access is granted (“...only executed after this TSF allowed access.”). Also all policies there besides PIS in phase 4 prevent reading sensitive or user dependent data without user authentication.

273 The SFR **FIA_UAU.4/MRTD** requires the prevention of authentication data reuse. This is fulfilled by using random data from **F.RNG** (“... used in ... the creation of a session key and authentication nonces.”) and by using changing initialization vectors in **F.Secure_Messaging** (Item 6) as specified in the Basic Access Control specification. [7]

274 The SFR **FIA_UAU.5** requires Basic Access Control authentication mechanism and authentication mechanism using Triple-DES. This is provided by **F.Identification_Authentication** (“It uses for this the Basic Access Control authentication method...” and items 2 and 3) as specified in the Basic Access Control specification. [7] The SFR **FIA_UAU.5** also requires the role to be identified with role specific keys. This is done in **F.Identification_Authentication** (“Each of these roles it identified/authenticated with at least one specific key.”).

275 The SFR **FIA_UAU.6/MRTD** requires re-authentication of each command. This is ensured by the enforced method for authenticity in **F.Secure_Messaging** (Item 5).

276 The SFR **FDP_ACC.1/PRIM** requires the enforcement of the PIS access control policy which is done by **F.Access_Control** (Item 6: “Access Control in phase 4 ... enforcement of PIS ...”).

277 The SFR **FDP_ACF.1/PRIM** requires the enforcement of accesses to objects based on subjects, objects and attributes, which is enforced by **F.Access_Control** (Item 1). The SFR **FDP_ACF.1/PRIM** also requires the enforcement of the rules of the PIS access control pilicy which are there formulated in detail. This is enforced by **F.Access_Control** (Item 6: “Access Control in phase 4 ... enforcement of PIS ...”).

278 The SFR **FDP_ACC.1/BASIC** requires the enforcement of the BIS access control policy which is done by **F.Access_Control** (Item 6: “Access Control in phase 4 ... enforcement of BIS ...”).

279 The SFR **FDP_ACF.1/BASIC** requires the enforcement of accesses to objects based on subjects, objects and attributes, which is enforced by **F.Access_Control** (Item 1)**.** The SFR **FDP_ACF.1/BASIC** also requires the enforcement of the rules of the BIS access control pilicy which are there formulated in detail. This is enforced by **F.Access_Control** (Item 6: “Access Control in phase 4 ... enforcement of BIS ...”)**.**

280 The SFR **FDP_UCT.1/MRTD** requires a TSF for confidentiality in communication provided by the encrypted communication channel in **F.Secure_Messaging**. It does this by enforcing to use a cryptographic method for confidentiality when used. (Item 5)

281 The SFR **FDP_UIT.1/MRTD** requires a TSF for protecting communication against modification provided by the protected communication channel in **F.Secure_Messaging**. It does this by using unique initialization vectors (Item 6) and the cryptographic method for authenticity (Item 4). The send sequence counter makes each command unique while the authenticity method makes it possible to detect any of the listed modifications.

282 The SFR **FMT_MOF.1** requires the restriction of the selection of Basic Access Control to the personalization agent in **F.Personalization.** In fact the choice is already made in **F.Initialization_Prepersonalization**. Later - esp. in phase 4 - this can't be changed anymore. Hence the purpose of the SFR is satisfied.

283 The SFR **FMT_SMF.1** requires management functions to be present which are provided by **F.Initialization_Prepersonalization** and **F.Personalization**.

284 The SFR **FMT_SMR.1** requires the maintenance of user roles. These are managed by **F.Identification_Authentication**. The first list gives the user roles 1, 2 and 4 listed in **FMT_SMR.1**. The role 3 is implicit as it requires no identification/authentication.

285 The SFR **FMT_LIM.1** requires limited capabilities of test functions, which is provided by **F.Deactivate_Non_TSF**. Also the test functions of the hardware part are disabled when the embedded software is running. (**F.COMP**: paragraph “The control of the boot mode ...”)

286 The SFR **FMT_LIM.2** requires limited availability of test functions, which is provided by **F.Deactivate_Non_TSF**. Also the testfunctions of the hardware part are disabled when the embedded software is running. (**F.COMP**: paragraph “The control of the boot mode ...”)

287 The SFR **FMT_MTD.1/INI_ENA** requires writing of initialization data and pre-personalization data to the manufacturer. Writing of pre-personalization and installation data only by the manufacturer is enforced by **F.Access_Control**, which limits these operations to phase 2b and 2c (“Access Control in phase 2b/2c ... ”). Independent of **F.Access_Control** writing of the initialization data is only possible in phase 2a because **F.COMP** (See addition) stores this data in the User Read Only Area which can't be changed afterwards.

288 The SFR **FMT_MTD.1/INI_DIS** requires only the personalization agent to be able to disable reading of the initialization data. This is provided by **F.Deactivate_Non_TSF** and **F.Personalization**.

289 The SFR **FMT_MTD.1/KEY_WRITE** requires the personalization agent to be able to write the Document Basic Access Control keys. This is provided by **F.Access_Control** (“Access Control in phase 3 ... doing key management, e.g. BAC key ...”) allowing the personalization agent in phase 3 to write all necessary data.

290 The SFR **FMT_MTD.1/KEY_READ** requires the Document Basic Access Control keys to never be readable. This is enforced by **F.Access_Control**, which does not allow reading of any key to any role (Item 2).

291 The SFR **FPT_EMSEC.1** requires limiting of emanations. This is provided by **F.HW_DES** (special DES protection) and **F.LOG** (general protection) by the hardware. Additional **F.Retry_Counter** limits the number of possible tries to use management keys which reduces the availability of analyzable data.

292 The SFR **FPT_FLS.1** requires failure detection and preservation of a secure state. **F.OPC** is directly designed for this SFR. It audits continually and reacts to environmental and other problems by bringing it into a secure state.

293 The SFR **FPT_TST.1** requires testing which is provided by **F.Verification**. **F.PHY** tests all EEPROM and ROM content for integrity (“... able to correct a 1-bit error within each byte.” / “... parity check.”).

294 The SFR **FPT_PHP.3** requires resistance to physical attacks. This is provided by **F.PHY** which is provided by the hardware to resist attacks. (“The function F.PHY protects the TOE against manipulation ...” / “... construction which make reverse-engineering and tamper attacks more difficult.”)

295 The SFR **FPT_RVM.1** requires enforcement functions to succeed. This is provided by **F.Access_Control** which enforces first the TSP and then allows execution of the protected functions only on success. (“... which only are only executed after this TSF allowd access.”)

296 The SFR **FPT_SEP.1** requires separation of TSF and Non-TSF data. This is done by disabling Non-TSF functions with **F.Deactivate_Non_TSF**. Also **F.COMP** does protect

the embedded software against test functions of the hardware ("... control of the CPU mode ...").

297 The summary specification rationale obviously shows that the set of IT security functions work together to form a mutually supportive and internally consistent whole satisfying the TOE security functional requirements.

8.2.3 Strength of Function Level Rationale

Due to the requirements of the PP the level for the strength of the TOE´s security functional requirements is claimed as SOF-high. The TOE is considered as a product with critical security mechanisms which only have to be defeated by attackers possessing a high level of expertise, opportunity and resources, and whereby successful attack is judged beyond normal practicability.

9 Glossary and Acronyms

Term	Definition
Active Authentication	Security mechanism defined in [7] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
Audit records	Write-only-once non-volatile memory area of the MRTD's 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	Security mechanism defined in [7] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminal's part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [8]
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. [8]
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 Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [7]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is

Term	Definition
(SO_D)	stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}). [7]
Eavesdropper	A threat agent with moderate 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. [9]
Extended Access Control	Security mechanism identified in [7] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [8]
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. [9]
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. [8]
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. [9]
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveller

Term	Definition
	(the MRTD holder) and verifying its authenticity. [9]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
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 contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder (1) the digital Machine Readable Zone Data (digital MRZ data, DG1), (2) the digitized portraits (DG2), (3) the biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both and (4) the other data according to LDS (DG5 to DG16).
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless 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]
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. [8]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes

Term	Definition
	- 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 DG1 to DG14 and DG 16) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic 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	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [10], 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.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
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. [8]
Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.
Prepersonalization Agent	A part of the manufacturer role acting on the behalf of the issuing State or organisation to configure the TOE before phase 3.
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,

Term	Definition
	(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)	A inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
Receiving State	The Country to which the MRTD holder 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. [8]
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 contactless communication channel of the TOE without knowledge of the printed MRZ data.
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. [9]
traveller	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	MRTD material prepared to produce an personalized MRTD containing an initialised and pre-personalized MRTD's chip.
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 enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. [9]
verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
SFR	Security functional requirement
TOE	Target of Evaluation
SAR	Security assurance requirements
TSF	TOE security functions
CC	Common Criteria

Acronym	Term
OSP	Organisational security policy
PIS	Primary Inspection System
BIS	Basic Inspection System
PT	Personalization Terminal

10 Literature

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 2.3, August 2005

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements; Version 2.3, August 2005

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements; Version 2.3, August 2005

[4] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation methodology, Version 2.3, August 2005

[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] Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

[7] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[8] ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[9] BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 1.9, ICAO TAG MRTD/NTWG, 19 May 2003

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

Cryptography

[11] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, Issued 2001 May 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[12] 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

[13] 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

Protection Profiles

[14] 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

[15] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

[16] Protection Profile — Machine Readable Travel Document with "ICAO Application", Basic Access Control, Version 1.0, BSI-PP-0017, 2005-08-18

Sonstige

[17] Technical Report Advanced Security Mechanisms for Machine Readable Travel Documents, Version 0.8 (final), BSI

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

[19] ISO/IEC 14443-3:2001, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, Part 3: Initialization and anticollision, 2001