Sdu IDENTIFICATION

Electronic Passport

SECURITY TARGET LITE
for
Sdu ICAO eMRTD

Certification ID: BSI-DSZ-CC-0383

Version 1.0.0

standard

File	: SDU_ICAO_ST_Lite 1.0.0.doc	Date: 26 March 2007
Author	: Sdu Identification	Classification: standard

Document Revision History

Version	Date	Author	Description
1.0.0	15/03/2007	Sdu	Public Release

Contents

Tables

1 ST Introduction

1.1 ST reference

TOE:	Sdu ICAO eMRTD
TOE Version:	1.0
Document ID:	8828-9 Security Target Lite
ST Title:	Security Target Lite for Sdu ICAO eMRTD
Version Number:	1.0.0
Date:	26 March 2007
Status:	public release
CC Version:	2.1 (with Final Interpretation of CCIMB as of 04.04.2005)
Assurance Level:	EAL4+ ADV_IMP.2 and ALC_DVS.2.
SOF Level:	SOF-high
Certification ID:	BSI-DSZ-CC-0383

1.2 ST Overview

The Security Target defines the environment, security objectives, requirements and Security Functions for the Sdu ICAO eMRTD based on the Machine Readable Travel Document with "ICAO Application", Basic Access Control Protection Profile [22]. This TOE extends the PP by including Active Authentication as specified in [7].

This evaluation is a composite evaluation with underlying platform being the Philips P531G072V0Q (JCOP 31, v2.2). The certification number for the underlying platform is: BSI-DSZ-CC-0294.

1.3 Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant. The evaluation level is EAL4 augmented by ADV_IMP.2 and ALC_DVS.2. The TOE fully implements the Machine Readable Travel Document with "ICAO Application" Basic Access Control Protection Profile, version 1.0, BSI-PP-0017 [22]. The functionality of the TOE extends that contained in the Protection Profile, by including Active Authentication.

2 TOE Description

Parts of this section have been changed from the PP. These are denoted by **bold text**.

2.1 TOE definition

The Target of Evaluation (TOE) is the Sdu ICAO eMRTD. The 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].

The TOE [Sdu ICAO eMRTD] comprises of

- The Philips P531G072V0Q, comprising of
  - The Philips P5CD072V0Q including 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;
  - JCOP 31 v2.2, the IC Embedded Software (operating system);
- Sdu eMRTD LDS Applet v1.2.3, the MRTD application; and

the associated guidance documentation.

For this TOE, only one application will be present on the IC, namely the MRTD Application. The TOE utilises the evaluation of the underlying platform, which includes the Phillips chip, the IC Dedicated Software, and the JCOP 31 v2.2.

2.2 TOE usage and security features for operational use

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 ensure the authenticity of the data of genuine MRTD's. The receiving State trust a genuine MRTD of a issuing State or Organization.

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 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[1];

(4) the other data according to LDS (DG5 to DG16); and

(5) the Document security object.

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

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.

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. The TOE can optionally demonstrate that the MRTD data is contained on the intended chip by using an RSA signature (Active Authentication).

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.

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 Extended Access Control as optional security mechanisms.

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].

[1] These additional biometric reference data are optional.

2.3 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases.

Phase 1 "Development"

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

The **Operating System** 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) **and the guidance documentation associated with this TOE component. The application developer uses the guidance documentation for the Operating System and develops** the MRTD application and the guidance documentation associated with **this** TOE component.

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" [2]

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.

The MRTD is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 "Personalization of the MRTD"

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 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. For this TOE, the Active Authentication Keys are generated by the Personalization Agent and injected into the TOE, also as part of step (iv).

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

[2] The TOE will be delivered to the Personalization agent at the completion of this Phase. The end of this phase is the boundary of this evaluation.

(together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Phase 4 "Operational Use"[3]

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.

[3] It will not be possible to add or modify the MRTD once it is in the Operational Phase. This includes configuring BAC. [Application Note 2]

3 TOE Environment

3.1 Introduction

3.1.1 Assets

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

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.

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.

3.1.2 Subjects

This protection profile considers the following subjects:

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.

MRTD Holder

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

Traveller

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

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].

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)[4] 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.

The following inspection system is added by the ST author.

The **Active Authentication Inspection System** (AAIS) implements Active Authentication in addition to Passive Authentication. It may or may not implement the Basic Access Control Mechanism and/or the Extended Access Control Mechanism. If Biometric Data is included on the passport, it is authorized by the issuing State or Organization to read the optional biometric reference data. Note that Active Authentication does not require Access Control greater than standard MRTD data, as the only additional accessible data is a public key.

Terminal

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

Attacker[5]

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

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

[4] This Security Target does not discuss the EIS further because the Extended Access Control is outside the scope, and active authentication is covered by AAIS.

[5] An impostor attacks the inspection system in the TOE IT environment by using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant to the TOE.

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.

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[6] 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. To be considered an Active Authentication Inspection System[7], a Primary Inspection System or Basic Inspection System must be able to verify that the Active Authentication private key (stored on the MRTD IC) matches the Active Authentication public key contained in the logical MRTD using a challenge response mechanism in the TOE, [7] section 2.3.2.

3.3 Threats

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

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

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.

[6] According to [7] the support of (i) the Passive Authentication mechanism is mandatory, and (ii) the Basic Access Control and Active Authentication are optional. In the context of this Security Target the Primary Inspection System does not implement the terminal part of the Basic Access Control. Terminals that do not implement BAC will therefore not able to read the logical MRTD if the logical MRTD is protected by Basic Access Control. The TOE allows the Personalization agent to disable the Basic Access Control for use with these Systems.

[7] An Active Authentication Inspection System, is also either a Primary Inspection System or Basic Inspection System, and must follow the policies defined by the TOE configuration.

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.

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.

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.

The TOE shall avert the threat as specified below.

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.

T.Information_Leakage: Information Leakage from MRTD's chip

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

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the 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).

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 pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

T.Malfunction: Malfunction due to Environmental Stress

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.

T.Clone: Attempt to Clone with public information

An attacker may attempt to clone a valid passport using the MRTD read from the valid passport's IC. If an attacker holds the MRTD IC, they can read both BAC enabled or disabled passports.

3.4 Organisational Security Policies

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).

P.Manufact[8]: 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.

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.

P.Personal_Data: Personal data protection policy[9]

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.

[8] The TOE is complete at the end of Phase 2. The TOE is delivered to the Personalizer prior to the commencement of Phase 3.

[9] The organisational security policy P.Personal_Data is drawn from the ICAO Technical Report [7]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

4 Security Objectives

4.1 Security Objectives for the TOE

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.

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.

OT.AC_Pers:[10] 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.

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.

OT.Data_Conf[11]: 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

[10] The OT.AC_Pers implies that:

1. the data of the LDS groups written during personalization for MRTD holder (at least DG1 and DG2) can not be changed by write access after personalization,
2. the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordantly. **The TOE does not allow a personalization agent to add data to the LDS once it is in the Operational Phase.**

[11] The traveller grants the authorization for reading the personal data in DG1 to DG16 to the inspection system by presenting the MRTD. The MRTD's chip provides read access to this data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication independent on the quality of the Document Basic Access Keys which is defined by the TOE environment and loaded into the TOE by the Personalization Agent. Any attack based on decision of the ICAO Technical Report [7] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective OT.Data_Conf. [Cf. CEM [4], section 8.10.3.4, para. 1625]

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 **so that BAC is disabled**[12] no protection in confidentiality of the logical MRTD is required.

OT.Identification[13]: 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.

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.

OT.Active_Authentication[14]: Protection against MRTD Copying

The TOE must provide the option for Active Authentication. The Active Authentication mechanism ensures that the data is read from the genuine IC and that the chip and data page belong to each other. See [7].

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

[12] This phrase was changed to allow for the possibility that the AAIS will have BAC disabled.

[13] The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the MRTD". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing environment as described in its security objective OD.Material. In the Phase 4 "Operational Use" the TOE is identified by the passport number as part of the printed and digital MRZ. If the TOE allows a Primary Inspection System (i.e. every terminal) to read these data every terminal may identify the TOE. If the TOE is configured to allow a Basic Inspection System only to read these data the OT.Identification forbids the output of any other IC (e.g. integrated circuit serial number ICCSN) or a MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

[14] This Objective is added to the PP to cover active authentication.

OT.Prot_Inf_Leak[15]: 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.

OT.Prot_Phys-Tamper[16]: Protection against Physical Tampering

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

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

with a prior

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

OT.Prot_Malfunction[17]: 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.

[15] This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

[16] In order to meet the security objectives OT.Prot_Phys-Tamper the TOE must be designed and fabricated so that it requires a high 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 such a physical attack. This is addressed by the security objective OD.Assurance.

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

4.2 Security Objectives for the Development and Manufacturing Environment

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.

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

4.3.1 Issuing State or Organization

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

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[18] 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.

OE.Pass_Auth_Sign Authentication 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

[18] If Active Authentication is required, the RSA keys must be injected into the TOE by the Personalizer.

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].

4.3.2 Receiving State or organization

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

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.

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.

OE.Active_Auth[19]: Verification by Active Authentication

An Active Authentication Inspection system performs all the functions of the Passive Authentication Inspection System, and verifies the IC authenticity with an RSA signature generated by the MRTD.

OE.Prot_Logical_MRTD[20]: 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.

[19] This Objective is added to the PP to cover active authentication.

[20] The Primary Inspection System may prevent unauthorized listening to or manipulation of the communication with the MRTD's chip e.g. by a Faraday cage.

4.3.3 MRTD Holder

OE.Secure_Handling[21]: Secure handling of the MRTD by MRTD holder

The holder of a MRTD configured for use with Primary Inspection Systems **or Active Authentication Inspection Systems with BAC disabled**[22] (i.e. MTRD with disabled Basic Access Control) will prevent unauthorized communication of the MRTD's chip with terminals through the contactless interface.

[21] The MRTD holder may prevent unauthorized communication of the MRTD's chip with terminals e.g. by carrying the MRTD in a metal box working as Faraday cage.

[22] Text added to allow for AAIS without BAC.

5 Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements that add or change words are denoted by **bold** text. In cases where words from a CC requirement were deleted, a separate statement indicates the words that were removed.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been included from the PP are denoted as underlined text.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been included from the PP are denoted by showing as underlined text.

Where the PP left the operation open, the ST author has completed the operation. These operations are denoted by showing as **bold underlined text**.

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

Security Requirements included in addition to the Protection Profile include the sentence: "This SFR is provided in addition to the Protection Profile". Iterations are marked as described above. The selections and assignments are marked by **bold underlined text.**

5.1 Security Functional Requirements for the TOE

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

5.1.1 Class FAU Security Audit

5.1.1.1 FAU_SAS.1 Audit storage

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

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)

The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

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

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

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[23].

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

5.1.2.2 FCS_CKM.4 Cryptographic key destruction - MRTD

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

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 **physically overwriting the keys** that meets the following: **none**.

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

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

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

Hierarchical to: No other components.

[23] The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [7], Annex E.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [7], Annex E.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1/MRTD.

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[24].

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

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

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

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 [14] 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

5.1.2.5 FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

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

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]

[24] Note that the TOE Platform provides compliance to FIPS 180-1. The standard for FIPS 180-2 states that the algorithm for SHA-1 did not change from version 1 to version 2. Thus, this SFR is consistent with the TOE platform.

FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.2.6 FCS_COP.1/RSA Cryptographic operation – RSA Signature

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). This SFR is provided in addition to the Protection Profile. This requirement forms part of "Active Authentication."

Hierarchical to: No other com0ponents.

FCS_COP.1.1/ RSA: The TSF shall perform **digital signature generation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024, 1280, 1536 and 1792 Bit** that meet the following: **ISO 9796-2**. **and SHA-1 digest.**

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

5.1.2.7 FCS_RND.1/MRTD Quality metric for random numbers

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

Hierarchical to: No other components.

FCS_RND.1.1/ MRTD: The TSF shall provide a mechanism to generate random numbers that meet **class K3 of [AIS 20] with SOF-high.**

Dependencies: No dependencies.

5.1.3 Class FIA Identification and Authentication

Table 1 provides an overview on the authentication mechanisms used by the TOE and its environment.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [7], Annex E, and [23]
Basic Access Control Authentication Mechanism	FIA_UAU.4/MRTD and FIA_UAU.6/MRTD	FIA_UAU.4/BAC_T and FIA_UAU.6/T	Triple-DES, 112 bit keys and Retail-MAC, 112 bit keys

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [7], Annex E, and [23]
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys

Table 1: Overview of authentication SFRs

5.1.3.1 FIA_UID.1 Timing of identification[25]

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2). The bold text below has been added to allow the use of active authentication when the TOE is configured with BAC disabled.

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 **and perform the SELECT command** in Phase 3 "Personalization of the MRTD"[26],

(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 **and request active authentication** 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.

5.1.3.2 FIA_UAU.1 Timing of authentication

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2). The bold text below has been added to allow the use of active authentication when the TOE is configured with BAC disabled.

[25] In the operation phase the MRTD must not allow anybody to read the ICCSN or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal for communication with more then one RFID. This identifier is randomly selected and will not violate the OT.Identification.

[26] Beside the ATS the Personalization Agent is also able to send a SELECT command in the phase 3 in order to personalise the TOE.

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 **and perform the SELECT command** in Phase 3 "Personalization of the MRTD"[26],

(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 **and request active authentication** 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.

5.1.3.3 FIA_UAU.4/MRTD Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE[27] [28]

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

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.

[27] All listed authentication mechanisms uses a challenge of 8 Bytes freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt: the Basic Access Control Authentication Mechanism uses RND.ICC [7], and the Authentication Mechanism based on Triple-DES shall use a Challenge as well.

[28] The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [7]. In the first step the terminal authenticates themselves to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop the communication with the terminal not successfully authenticated in the first step of the protocol to fulfil the security objective OT.Identification and to prevent T.Chip_ID.

5.1.3.4 FIA_UAU.5 Multiple authentication mechanisms[29]

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

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.

5.1.3.5 FIA_UAU.6/MRTD Re-authenticating – Re-authenticating of Terminal by the TOE[30]

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

[29] Depending on the authentication methods used the Personalization Agent holds (i) a pair of a Triple-DES encryption key and a retail-MAC key for the Basic Access Control Mechanism specified in [7], or (ii) a Triple-DES key for the Symmetric Authentication Mechanism. The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Note, the successful authenticated Personalization Agent may disable the Basic Access Control Mechanism.

[30] The Basic Access Control Mechanism specified in [7] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC_MRTD for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticate the user for each received command and accept only those commands received from the initially authenticated by means of BAC user.

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.

5.1.4 Class FDP User Data Protection

The instantiations of FDP_ACC.1 are caused by the TSF management according to FMT_MOF.1. The instantiations of FDP_ACF.1 address different SFP.

5.1.4.1 FDP_ACC.1 Subset access control – Primary Access Control

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

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

5.1.4.2 FDP_ACC.1 Subset access control – Basic Access control[31]

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

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

5.1.4.3 FDP_ACF.1 Security attribute based access control – Primary Access Control[32]

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2). The bold text below has been added to allow the use of active authentication.

[31] The Basic Access Control SFP address the configuration of the TOE for usage with Basic Inspection Systems only.

[32] The MRTD access control prevents changes of data groups by write access to the logical MRTD after their creation by the Personalization Agent (i.e. no update of successful written data in the data groups DG1 to DG16). The Passive Authentication Mechanism detects any unauthorised changes.

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 **and request active authentication**.

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

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

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (Common Criteria Part 2). The bold text below has been added to allow the use of active authentication.

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 **and request active authentication**.

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

5.1.4.5 FDP_ITC.1 Import of user data without security attributes

The TOE shall meet the requirement “Cryptographic operation (FDP_ITC.1)” as specified below (Common Criteria Part 2). This SFR is provided in addition to the Protection Profile. This requirement forms part of “Active Authentication.”

Hierarchical to: No other components.

FDP_ITC.1.1 — The TSF shall enforce the **Basic Access Control SFP or Primary Access Control SFP** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 — The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **none.**

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

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

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

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]

5.1.4.7 FDP_UIT.1/MRTD Data exchange integrity - MRTD

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

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]

5.1.5 Class FMT Security Management

5.1.5.1 FMT_MOF.1 Management of functions in TSF

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

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to enable and disable[33] the functions TSF Basic Access Control to Personalization Agent.

Dependencies: No Dependencies

5.1.5.2 FMT_SMF.1 Specification of Management Functions

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

Hierarchical to: No other components.

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

1. Initialization,
2. Personalization,
3. Configuration.

Dependencies: No Dependencies

5.1.5.3 FMT_SMR.1 Security roles

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

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.

[33] Note that disabling BAC for the user does not prevent the personalization agent using this function in the personalization phase. But if the BAC is disabled for the user, also the BAC Authentication Mechanism is disabled.

Dependencies[34]**:** FIA_UID.1 Timing of identification.

5.1.5.4 FMT_LIM.1 Limited capabilities

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

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.

5.1.5.5 FMT_LIM.2 Limited availability

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

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.

[34] Updated to reflect wording from CC Part 2.

5.1.5.6 FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data[35]

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.

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

5.1.5.7 FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data[36]

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.

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

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

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. The bold text below has been added to allow the use of active authentication.

[35] The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Authentication Key.

[36] According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE restricts the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once to the operating system and also to the java application [to allow access to the data in Phase 3] and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides an unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". The external read access to the Initialization Data and the Pre-personalization Data is blocked in the usage phase. The MRTD Manufacturer will write the Pre-personalization Data.

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write the Document Basic Access Keys **and the Active Authentication Keys** to the Personalization Agent.

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

5.1.5.9 FMT_MTD.1/KEY_READ Management of TSF data – Key Read[37]

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. The bold text below has been added to ensure the protection of the active authentication keys.

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read the Document Basic Access Keys, **the Active Authentication Private Key** and Personalization Agent Keys to none.

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

5.1.6 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_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.

5.1.6.1 FPT_EMSEC.1 TOE Emanation

The TOE shall meet the requirement "Subset information flow control (FDP_IFC.1)" as specified below. The bold text below has been added to ensure the protection of the active authentication keys.

Hierarchical to: No other components.

[37] The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys if the Basic Access Control is enabled. Note the Document Basic Access Keys may be used for the Basic Access Control Authentication Mechanism and secure messaging even if the Basic Access Control is disabled.

FPT_EMSEC.1.1 The TOE shall not emit [**variations in power consumption or timing during command execution**] in excess of [**non-useful information**] enabling access to Personalization Agent Authentication Key and **the Active Authentication Private Key**.

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 **the Active Authentication Private Key**.

Dependencies: No other components.

5.1.6.2 FPT_FLS.1 Failure with preservation of secure state

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

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

5.1.6.3 FPT_TST.1 TSF testing

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

Hierarchical to: No other components.

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up (at each power on)** 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.

5.1.6.4 FPT_PHP.3 Resistance to physical attack

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

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.

5.1.6.5 FPT_RVM.1 Non-bypassability of the TSP

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

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.

5.1.6.6 FPT_SEP.1 TSF domain separation

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

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

The SARs for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) augmented by ADV_IMP.2 and ALC_DVS.2.

The minimum strength of function is SOF-high.

This Security Target contains the security functional requirement FCS_RND.1/MRTD with an explicit stated strength of function claim (class K3 of [AIS 20] with SOF-high).

5.3 Security Requirements for the IT environment

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

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.** In each case, the replaced term is "TSF".

5.3.1 Passive Authentication

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.

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

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).

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 the logical 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 Active Authentication Key Generation

This section defines the requirements for the Active Authentication Key Generation. If the passport is to contain Active Authentication Keys, then this requirement is in addition to those on the Passive Authentication Document Signer.

5.3.2.1 FCS_CKM.1/AAKGS Cryptographic key generation – Generation of Active Authentication Keys[38]

The Basic Terminal shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2). This SFR is provided in addition to the Protection Profile. This requirement forms part of "Active Authentication."

[38] The Public RSA key must be inserted in DG 15, in accordance with [7].

Hierarchical to: No other components.

FCS_CKM.1.1/ AAKGS — The **AAKGS** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **none** and specified cryptographic key sizes **RSA: 1024, 1280, 1536 and 1792 Bit** that meet the following: **PKCS#1**.

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

5.3.3 Active Authentication Inspection Systems

This section defines the requirement for the Active Authentication Inspection System. If the TOE is also in the Basic Access Control configuration then the AAIS will need to comply with the Basic Inspection System requirements.

5.3.3.1 FCS_COP.1/AAIS Cryptographic operation – RSA Signature

The Active Authentication Inspection System shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). This SFR is provided in addition to the Protection Profile. This requirement forms part of "Active Authentication."

Hierarchical to: No other components.

FCS_COP.1.1/ AAIS — The **AAIS** shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024, 1280, 1536 and 1792 Bit** that meet the following: **ISO 9796-2 and SHA-1 digest.**

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

5.3.4 Basic Inspection Systems

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.

5.3.4.1 FCS_CKM.1/BAC_BT Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal[39]

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

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

5.3.4.2 FCS_CKM.4/BT Cryptographic key destruction - BT

The Basic Terminal shall meet the requirement "Cryptographic key generation (FCS_CKM.4)" as specified below (Common Criteria Part 2).

Hierarchical to: No other components.

FCS_CKM.4.1/BT: The **Basic Terminal** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwrite or physical deletion** that meets the following: **none**.

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

5.3.4.3 FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal[40]

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.

Hierarchical to: No other components.

[39] The terminals derive the Document Basic Access Keys from the second line of the printed MRZ data by the algorithm described in [7], 3.2.2 and Annex E.1, use them to generate the Document Basic Access Keys. The Personalization Agent downloads these keys to the MRTD's chip as TSF data for FIA_UAU.4/BAC_MRTD.

[40] This SFR requires the terminal to implement the hash function SHA-1 for the cryptographic primitive to generate the Document Basic Access Keys according to FCS_CKM.1/BAC_BT.

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

5.3.4.4 FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal[41]

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.

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

5.3.4.5 FCS_COP.1/MAC_BT Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal[42]

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.

Hierarchical to: No other components.

[41] This SFR requires the Basic Terminal to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The key is agreed between the TOE and the terminal during the execution of the Basic Access Control Authentication Mechanism. The key size of 112 bit is chosen to resist attacks with high attack potential.

[42] This SFR requires the terminal to implement the cryptographic primitive for secure messaging with message authentication code over the transmitted data. The key is agreed or defined as the key for secure messaging encryption. The key size of 112 bit is chosen to resist attacks with high attack potential.

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

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

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

Hierarchical to: No other components.

FCS_RND.1.1/BT	The **Basic Terminal** shall provide a mechanism to generate random numbers that meets **SOF-High**.

Dependencies: No dependencies.

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

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

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[43].

Dependencies: No dependencies.

5.3.4.8 FIA_UAU.6/BT Re-authentication - Basic Terminal[44]

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

Hierarchical to: No other components.

[43] The Basic Access Control Authentication Mechanism [7] uses a challenge RND.IFD freshly and randomly generated by the terminal to prevent reuse of a response generated by a MRTD's chip and of the session keys from a successful run of authentication protocol.

[44] The Basic Access Control Mechanism specified in [7] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The terminal checks by secure messaging in MAC_ENC mode each MRTD's chip response to a command based on Retail-MAC whether it was sent by the successfully authenticated MRTD's chip. The authentication fails if any response is received with incorrect message authentication code.

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[45].

Dependencies: No dependencies.

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

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

Hierarchical to: No other components.

FDP_UCT.1.1/BT The **Basic Terminal** shall enforce the BT part of 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]

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

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

Hierarchical to: No other components.

FDP_UIT.1.1/BT The **Basic Terminal** shall enforce the BT part of 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 94 has occurred.

[45] The Basic Access Control SFP of the TOE requires to protect the User Data by access control (cf. FDP_ACC.1/BASIC and FDP_ACF.1/BASIC) and by secure messaging (cf. FDP_UCT.1/MRTD and FDP_UIT.1/MRTD) for the communication between the TOE and the Basic Terminal. This secure messaging requires the Basic Terminal to support the protection of the TOE data by decryption and checking MAC and to protect its own data by secure messaging as well. The SFP of the Basic Terminal drawn from the TOE "Basic Access Control SFP" is named "BT part of Basic Access Control SFP" and the related SFR is described by FDP_UCT.1/BT and FDP_UIT.1/BT corresponding to FDP_UCT.1/MRTD and FDP_UIT.1/MRTD of the communication partner (i.e. the TOE). Note the Basic Terminal does not enforce any named access control policy or information control policy to be defined by FDP_ACC and FDP_ACF or FDP_IFC and FDP_IFF families (respectively). The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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]

5.3.5 Personalization Terminals

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.

5.3.6 FIA_API.1/SYM_PT Authentication Proof of Identity - Personalization Terminal Authentication with Symmetric Key[46]

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

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.

[46] The Symmetric Authentication Mechanism for Personalization Agents is intended to be used in a high secure personalization environment only. It uses the symmetric cryptographic Personalization Agent Authentication Secret key of 112 bits to encrypt a challenge of 8 Bytes with Triple-DES which the terminal receives from the MRTD's chip e.g. as response of a GET CHALLENGE. The answer may be sent by means of the EXTERNAL AUTHENTICATE command according to ISO 7816-4 [24] command. In this case the communication may be performed without secure messaging (note that FIA_UAU.5.2 requires secure messaging only after run of Basic Access Control Authentication).

6 Security Functions and Assurance Measures

6.1 SF.ACCESS

The TOE implements two access control policies to ensure appropriate access to user data, namely Primary Access Control and Basic Access Control. These policies are mutually exclusive, and the policy used by the TOE is configured by the Personalization agent in accordance with SF.MANAGEMENT. The TOE must be configured to apply one of these policies. The TOE applies the policies in Phase 3 and Phase 4. The policies are described below.

Primary Access Control

The Primary Access Control policy controls access to the User Data (DG1 to DG16, and the SOD) for the Personalization Agent and all other terminals. Any terminal[47] can read the User Data or use the active authentication keys, however only the Authenticated Personalization Agent may write User Data. The User Data can not be written, deleted or modified in Phase 4 “Operational Use”.

Basic Access Control

The Basic Access Control policy controls access to the User Data (DG1 to DG16, and the SOD) for the Personalization Agent, Basic Inspection System and all other terminals. The Authenticated Personalization Agent may write or read User Data. The authenticated Basic Inspection System is allowed to read data or use the active authentication keys. Other terminals may not read User Data. The User Data can not be written, deleted or modified in Phase 4 “Operational Use”. When the TOE is in the BAC configuration, this policy will ensure that the communication is protected by Secure Messaging (SF.CRYPTO) to protect and detect errors arising from modification, deletion, insertion and replay. Secure Messaging protects the transmission and receipt of objects from unauthorised disclosure.

6.2 SF.MANAGEMENT

The TOE will provide management functions in support of initializing, personalizing and configuring the TOE. For this TOE, initialization commands are all those commands required for installing the MRTD applet on the underlying platform (which are provided and controlled by the underlying platform). The Personalization commands are those required to write the User data to the TOE. The configuration command puts the TOE in either Primary Access Control or Basic Access Control “mode”.

6.3 SF.CRYPTO

The TOE will use primitives from the underlying platform to perform the following functions in support of BAC and Secure Messaging:

- generate 112 Bit Document Basic Access Keys according to [7], Annex E.

[47] To protect their data, users are recommended to store their passport in a metal wallet, and only remove for Authorised Inspection Systems when the TOE is configured for Primary Access Control.

- destroy cryptographic keys by overwriting.
- hash data using SHA-1 according to FIPS 180-2.
- secure messaging – Triple-DES in CBC mode encryption and decryption with 112 bit keys in accordance with FIPS 46-3 [14] and [7]; Annex E.
- secure messaging – Retail MAC message authentication code with 112 bit keys in accordance with ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).

The TOE will use primitives from the underlying platform to perform the following functions in support of Active Authentication:

- RSA digital signature generation with 1024, 1280, 1536 and 1792 Bit keys. Digital signature scheme in accordance with ISO 9796-2, and SHA-1 digest.

6.4 SF.AUTH

The TOE maintains the following roles:

- Manufacturer in Phase 2;
- Personalization Agent in Phase 3;
- Based on the configuration, in phase 4, either:
  - Primary Inspection System; or
  - Basic Inspection System.

To interact with the TOE the user must assume one of these roles. Each user must login to assume a role, except when the role is “Primary Inspection System” (i.e. BAC is disabled).

The Manufacturer logs in by presenting the Initialization Keys. More details of this method can be found in [25].

The Personalization agent logs on by using the two Personalization Agent Secret Keys provided by the Manufacturer. The TOE prevents reuse of authentication data by using an authentication scheme based on a challenge authentication method, such as the Basic Access Control Mechanism. The Personalization agent may use the Basic Access Control Authentication Mechanism or the Symmetric Authentication Mechanism based on Triple-DES.

The Basic Inspection System logs on by using the symmetric access keys provided by the Document Basic Access Key Derivation Algorithm. This method derives the symmetric access keys from the MRZ information which is personalized graphically on the MRTD following ICAO specifications. The TOE prevents reuse of authentication data by using the Basic Access Control Mechanism, which is based on challenge-response authentication.

When the Basic Access Control mechanism is being used, the TOE will re-authenticate users for each command sent to the TOE. This is achieved through Secure Messaging, and is inherent in the Secure Messaging protocol.

The only actions allowed by the TOE prior to identification and authentication are:

- reading the Initialization Data in Phase 2 “Manufacturing”,

- reading the ATS and performing the SELECT command in Phase 3 “Personalization of the MRTD”,
- reading the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,
- reading the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 “Operational Use”

Note: the IC Serial Number is not available in the usage phase. The passport is only identifiable by the passport number, which is subject to the SF.AUTH and SF.ACCESS.

This function has a strength of function of SOF-High.

6.5 SF.PLATFORM

The TOE platform provides the following functions. Further details of these functions can be found in [25].

- DES primitives
- destroy cryptographic keys by physically overwriting the keys.
- RSA primitives
- Protection from Emanations
- Limit test function capability and availability
- Limit emissions to a “non-usable” level
- Perform Self-Tests
- Preserve a secure state in the case of exposure or test failure.
- Resist Physical manipulation and probing
- ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
- Maintain Security Domains
- Store IC Identification Data
- Generate random numbers according to [AIS 20] class K3 with SOF-high.

This function has a strength of function of SOF-High.

6.6 Assurance Measures

In the following table the assurance measures of the TOE (documents) are listed. These measures fulfil the requirements from EAL4 augmented by ADV_IMP.2 and ALC_DVS.2.

Component	Assurance Measure / Document
ASE	Security Target (this document)

Component	Assurance Measure / Document
ACM_AUT.1	Configuration Management Documentation
ACM_CAP.4	
ACM_SCP.2	
ADO_DEL.2	Delivery and Operation Documentation
ADO_IGS.1	
ADV_FSP.2	Functional Specification
ADV_HLD.2	High Level Design
ADV_IMP.2	Implementation
ADV_LLD.1	Low Level Design
ADV_RCR.1	Representation Correspondence
ADV_SPM.1	Security Policy Model
AGD_ADM.1	Guidance Documentation
AGD_USR.1	
ALC_DVS.2	Lifecycle Documentation
ALC_LCD.1	
ALC_TAT.1	
ATE_COV.2	Test Documentation
ATE_DPT.1	
ATE_FUN.1	
ATE_IND.2	Part of the evaluation body
AVA_MSU.2	Vulnerability Assessment Documentation
AVA_SOF.1	
AVA_VLA.2	

Table 2: Assurance measures of the TOE

7 PP Compliance

The TOE is compliant with the Machine Readable Travel Document with "ICAO Application" Basic Access Control Protection Profile, version 1.0 [22].

8 Extended Components Definition

This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [20], other components are defined in this protection profile.

8.1 Definition of the Family FAU_SAS

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

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

8.1.1 FAU_SAS Audit data storage

Family behaviour

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

Component leveling

FAU_SAS Audit data storage 1

FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1 There are no management activities foreseen.
Audit:	FAU_SAS.1 There are no actions defined to be auditable.

8.1.1.1 FAU_SAS.1 Audit storage

Hierarchical to:	No other components.
FAU_SAS.1.1	The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.
Dependencies:	No dependencies.

8.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component

FCS_RND is not limited to generation of cryptographic keys as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

8.2.1 FCS_RND Generation of random numbers

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

Family behaviour

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

Component leveling:

FCS_RND Generation of random numbers 1

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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

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

Dependencies: No dependencies.

8.3 Definition of the Family FIA_API

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

The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter Explicitly stated IT security requirements (APE_SRE)) form a TOE point of view. Note that this protection profile uses this explicit stated

SFR for the personalization terminal in the IT environment only. Therefore the word "TSF" is substituted by the word "Personalization terminal".

8.3.1 FIA_API Authentication Proof of Identity

Family behaviour

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

Component leveling:

FIA_API Authentication Proof of Identity 1

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT:

Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable .

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

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

Dependencies: No dependencies.

8.4 Definition of the Family FMT_LIM

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

8.4.1 FMT_LIM Limited capabilities and availability

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

Family behaviour

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

Component leveling:

FMT_LIM Limited capabilities and availability1 2

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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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

8.4.1.1 FMT_LIM.1 Limited capabilities

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

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 [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.2 Limited availability.

8.4.1.2 FMT_LIM.2 Limited availability

The TOE Functional Requirement "Limited availability (FMT_LIM.2)" is specified as follows.

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 [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.1 Limited capabilities.

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

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

or conversely

(ii) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

The combination of both requirements shall enforce the policy.

8.5 Definition of the Family FPT_EMSEC

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE

shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [2].

The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC TOE emanation 1

FPT_EMSEC.1	TOE emanation has two constituents:
FPT_EMSEC.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMSEC.1.2	Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

8.5.1 FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

Dependencies: No other components.

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.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data. This data is copied to the Application to allow the personalizer to trace chips. It is not available in Phase 4.
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.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
Biographical data (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]

Term	Definition
Country Signing CA Certificate (CCSCA)	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) 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 KENC) and message authentication (key KMAC) 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 (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [7]
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [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]

Term	Definition
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 (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.

Term	Definition
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) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, DG1), (3) the digitized portraits (DG2), (4) the biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both and (5) 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]

Term	Definition
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 - 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.

Term	Definition
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.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.

Term	Definition
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
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

Term	Definition
	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.

9.1 Acronyms

Acronym	Term
SFR	Security functional requirement
TOE	Target of Evaluation
SAR	Security assurance requirements
TSF	TOE security functions
CC	Common Criteria
OSP	Organisational security policy
PIS	Primary Inspection System
BIS	Basic Inspection System
PT	Personalization Terminal
n.a.	Not applicable
AAKGS	Active Authentication Key Generation System

10 References

10.1 Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1, August 1999

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1, August 1999

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1, August 1999

[4] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999

[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

10.2 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)

[11] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version – 0.42 - Draft, August, 2004, Dr. Kügler, BSI

10.3 Cryptography

[12] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, Bonn, 10.8.2004 (Zieldatum der Veröffentlichung ist Januar 2005)

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

[14] 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 Bundesamt für Sicherheit in der Informationstechnik page 73 of 74 Version 1.0, 18th August 2005 Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control

[15] 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

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

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

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

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

10.4 Protection Profiles

[20] 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

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

[22] Machine Readable Travel Document with “ICAO Application” Basic Access Control Protection Profile, version 1.0, August 18th, 2005

10.5 Other

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

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

[25] SECURITY TARGET Philips P531G072V0Q (JCOP 31, v2.2) on Philips P5CT072V0P, Secure Smart Card Controller, v1.6.