Security Targets

For

Apollo OS e-Passport V1.0

A Product of

SCsquare Ltd.

Version: 1.03
Date: 14.07.2009
Doc. ID ST- 1
File Name: Apollo OS V3.17 Security Target CC EAL 4+ V1.03
Author(s): Ilanit Avioz
Certif. ID: ITC-8194

Table of Contents

1. ST Introduction

1.1. ST Identification

ST identification	Title	Security Target for Apollo OS e-Passport V1.0 a product of SCSquare Ltd
	Version	1.03
	Publication Date	14 July 2009
	Author	Ilanit Avioz
TOE	Identity	Apollo OS e-Passport V1.0
	Version	1.0
Common Criteria	Version	2.3
Additional information	Assurance Level	EAL4 augmented with ADV_IMP.2, ALC_DVS.2
	Strength of Functions	SOF high
	PP conformance	BSI-PP-0017
	Related Hardware	SLE66CLX800PE

1.2. ST Overview

The aim of this document is to describe the Security Target for the Machine Readable Travel Document (MRTD) chip with the ICAO application and Basic Access Control on the Apollo OS operation system.

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

The Apollo OS is a fully interoperable multi-application smart card operating system compliant to ISO/IEC 7816. It provides a comprehensive end-to-end solution, offering the fastest and most powerful security available.

The Operating system software is implemented on the Infineon SLE66CLX800PE, which is certified according to CC EAL5 augmented (EAL5+) with components ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 (certificate number BSI-DSZ-CC-0399-2007).

The assurance level for the TOE is CC EAL4+ (see Section 1.3).

The TOE follows the composite evaluation aspects (see also [CCDB])

1.3. CC Conformance

This security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, August 2005, version 2.3, CCMB-2005-08-001 [CC-1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, August 2005, version 2.3, CCMB-2005-08-002 [CC-2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, August 2005, version 2.3, CCMB-2005-08-003 [CC-3],

  Including the
- Final Interpretation of CCIMB as of 04.04.2005 as follows:
- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2, ALC_DVS.2.

2. TOE Description

2.1. TOE definition

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

- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors,
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application and
- The associated guidance documentation.

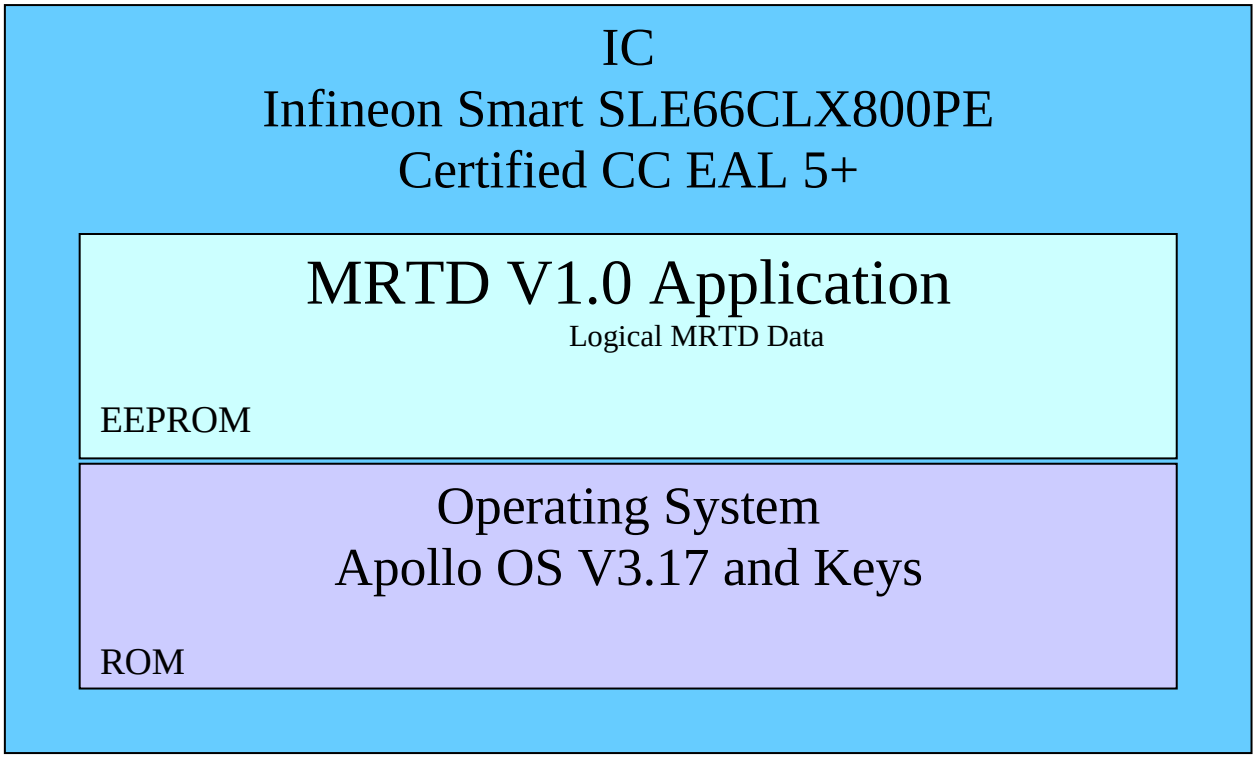

Figure 1: TOE description

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 ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an 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 [LDS] 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, EF.DG1),

   (2) the digitized portraits (EF.DG2),

   (3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]

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

   (5) the Document security object

[1] These additional biometric reference data are optional

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) [SSMR]. 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 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 sensitive biometrics as optional security measure in the ICAO technical report [PKI].
The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of 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 Active Authentication and 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 Organisation. The inspection system

i. Reads the printed data in the MRTD,
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 ([PKI], Annex E, and [LDS]).

2.3. TOE life cycle

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

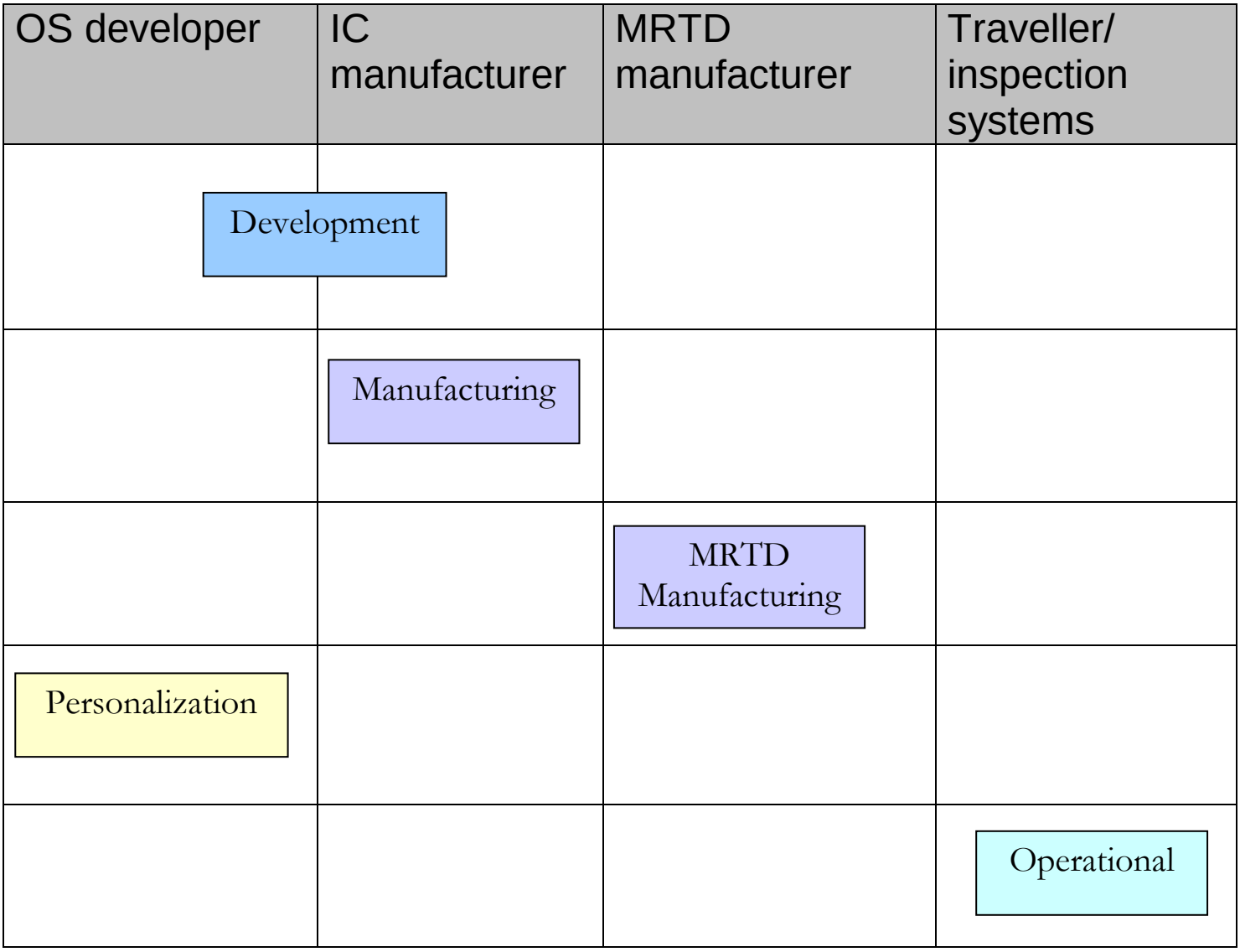

Figure 2: TOE life cycle

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

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 manufacturer

i. add the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary,
ii. Packs the IC with hardware for the contactless interface in the passport book
iii. Send the inlay to the MRTD manufacturer

"**Pre-Personalization**"

The MRDT manufacturer

a. creates the MRTD application, and
b. equips MRTD's chip with Pre-personalization Data and
c. the personalization key

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent.
The personalization key is delivered in a secure channel to the personalization agent using PGP (the key is encrypted using the personalization agent PGP key only). The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

After this phase the TOE is finished.

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.

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

Phase 4 "Operational Use"

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. Security Problem Definition

3.1. Introduction

Assets

The assets to be protected by the TOE include the User Data on 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 [LDS]. 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.
An additional asset is the following more general one.

AUTHENTICITY OF THE MRTD'S CHIP

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

Subjects

This security target 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 [LDS].

INSPECTION SYSTEM

A technical system used by the border control officer of the receiving State

i. examining an MRTD presented by the traveller and verifying its authenticity and

ii. Verifying the traveller as MRTD holder.

The **Primary Inspection System** (PIS)

i. Contains a terminal for the contactless communication with the MRTD's chip and

ii. Does not implement the terminals part of the Basic Access Control Mechanism.

The Primary Inspection System can read the logical MRTD only if the Basic Access Control is disabled.

The **Basic Inspection System** (BIS)

i. Contains a terminal for the contactless communication with the MRTD's chip,
ii. Implements the terminals part of the Basic Access Control Mechanism and
iii. Gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the printed data in the MRZ or other parts of the passport book providing this information.

The **Extended Inspection System** (EIS) in addition to the Basic Inspection System

i. implements the Active Authentication Mechanism,
ii. supports the terminals part of the Extended Access Control Authentication Mechanism and
iii. Is authorized by the issuing State or Organization to read the optional biometric reference data.

This Security Target does not distinguish between the BIS and EIS because the Active Authentication and the Extended Access Control is outside the scope.

TERMINAL

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

ATTACKER

A threat agent trying

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

3.2. Assumptions

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

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.

According to [PKI] the support of (i) the Passive Authentication mechanism is mandatory, and (ii) the Basic Access Control is optional. In the context of this Security Target the Primary Inspection System does not implement the terminal part of the Basic Access Control. It is 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 Primary Inspection Systems.

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 [PKI]. The Primary Inspection System performs the Passive Authentication to verify the logical MRTD if the logical MRTD is not protected by Basic Access Control. The Basic Inspection System in addition to the Primary Inspection System implements the terminal part of the Basic Access Control and reads the logical MRTD being under Basic access Control.

The TOE allows the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems.

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 cannot read and does not know in advance the MRZ data printed on the MRTD data page.

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 cannot 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 holder identity or biometric reference data.
This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the 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 another 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 another 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 attacker needs information about the functional operation.

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 [CC-1], sec. 3.2).

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

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing. The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

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

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

P.Personal_Data **Personal data protection policy**

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (DG1), the printed portrait and the digitized 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 [PKI]. 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.

The organizational security policy P.Personal_Data is drawn from the ICAO Technical Report [PKI]. 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

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

4.1. Security Objectives for the TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data groups DG1 to DG16, the Document Security Object according to LDS [LDS] 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 cannot 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 Confidentiality of personal data

If the TOE is configured for the use with Basic Inspection Systems the TOE must ensure the confidentiality of the logical MRTD data groups DG1 to DG16 by granting read access to terminals successfully authenticated by

i. as Personalization Agent or as

ii. Basic Inspection System.

The Basic Inspection System shall authenticate themselves by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

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

The traveler grants the authorization for reading the personal data in DG1 to DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these 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 [PKI] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective OT.Data_Conf

OT.Identification Identification and Authentication of the TOE

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

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.

OT.Prot_Abuse-Func Protection against Abuse of Functionality

The TOE must prevent 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.

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

OT.Prot_Inf_Leak Protection against Information Leakage

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

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

OT.Prot_Phys-Tamper Protection against Physical Tampering

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

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

with a prior

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

OT.Prot_Malfunction Protection against Malfunctions

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

4.2. Security Objectives for the Development and Manufacturing Environment

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

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 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 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 includes all data in the data groups DG1 to DG16 if stored in the LDS according to [LDS].

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.Prot_Logical_MRTD Protection of data of the logical MRTD

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

MRTD Holder

OE.Secure_Handling Secure handling of the MRTD by MRTD holder

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

5. Security Requirements

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of [CC-2]. Each of these operations is used in this security target.
The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements that add or change words are in **bold** text. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.
The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections filled in by the ST author appear as *slanted and 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 made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear as *slanted and underlined text*.

5.1. Security Functional Requirements for the TOE

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

Class FAU Security Audit

The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below.

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
FAU_SAS.1.1	The TSF shall provide the Manufacturer[2] with the capability to store the IC Identification Data[3] in the audit records.
Dependencies:	No dependencies.

The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD’s chip (see FMT_MTD.1/INI_DIS). The security measures in the manufacturing environment assessed under ADO_IGS and ADO_DEL ensure that the audit records will be used to fulfil the security objective OD.Assurance.

[2][assignment: *authorized users*]

[3] [assignment: *list of audit information*]

The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing.

Class Cryptographic Support (FCS)

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

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

Hierarchical to: No other components.

FCS_CKM.1.1/ BAC_MRTD

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[4] and specified cryptographic key sizes 112 bit[5] that meet the following: [PKI] Annex E.[6]

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

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 [PKI], 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 [PKI], Annex E.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1/MRTD.
The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2).

---

[4] [assignment: *cryptographic key generation algorithm*]

[5] [assignment: *cryptographic key sizes*]

[6] [assignment: *list of standards*]

FCS_CKM.4 Cryptographic key destruction - MRTD
Hierarchical to: No other components.

FCS_CKM.4.1/ MRTD

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with zeros or random data*[7] that meets the following: *none*[8].

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

The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging after closing the secure channel or power off.

CRYPTOGRAPHIC OPERATION (FCS_COP.1)

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

FCS_COP.1/SHA_MRTD Cryptographic operation – Hash for Key Derivation by MRTD
Hierarchical to: No other components.

FCS_COP.1.1/ SHA_MRTD

The TSF shall perform hashing[9] in accordance with a specified cryptographic algorithm SHA-1[10] and cryptographic key sizes none[11] that meet the following: FIPS 180-2[12].

---

[7] [assignment: *cryptographic key destruction method*]

[8] [assignment: *list of standards*]

[9] [assignment: *list of cryptographic operations*]

[10] [assignment: *cryptographic algorithm*]

[11] [assignment: *cryptographic key sizes*]

[12] [assignment: *list of standards*]

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

The TOE implements the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4/BAC_MRTD) according to [PKI].

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

Hierarchical to: No other components.

FCS_COP.1.1/ TDES_MRTD

The TSF shall perform secure messaging – encryption and decryption[13] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[14] and cryptographic key sizes 112 bit[15] that meet the following: FIPS 46-3 [FIPS] and [PKI] Annex E[16].

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

The TOE implements the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/BAC_MRTD and FIA_UAU.4/BAC_BT. Note the Triple-DES in CBC mode with zero initial vector include also the Triple-DES in ECB mode for blocks of 8 byte used to check the authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

Hierarchical to: No other components.

[13] [assignment: list of cryptographic operations]

[14] [assignment: cryptographic algorithm]

[15] [assignment: cryptographic key sizes]

[16] [assignment: list of standards]

FCS_COP.1.1/MAC_MRTD

The TSF shall perform secure messaging – message authentication code[17] in accordance with a specified cryptographic algorithm Retail MAC[18] and cryptographic key sizes 112 bit[19] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[20].

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

This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/BAC_MRTD and FIA_UAU.4/BAC_MRTD.

RANDOM NUMBER GENERATION (FCS_RND.1)

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

FCS_RND.1/MRTD Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1/ MRTD

The TSF shall provide a mechanism to generate random numbers that meet *functional class P2 with SOF-high of AIS31* [21].

Dependencies: No dependencies.

The TOE generates random numbers used for the authentication protocols as required by FIA_UAU.4/BAC_MRTD.

---

[17] [assignment: *list of cryptographic operations*]

[18] [assignment: *cryptographic algorithm*]

[19] [assignment: *cryptographic key sizes*]

[20] [assignment: *list of standards*]

[21] [assignment: *list of standards*]

Class FIA Identification and Authentication

The Table 1 provides an overview on the authentication mechanisms used.

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

Table 1 - Overview on authentication SFR

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

FIA_UID.1 **Timing of identification**
Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow

1) to read the Initialization Data in Phase 2 "Manufacturing",
2) to read the ATS in Phase 3 "Personalization of the MRTD",
3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 "Operational Use",
4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System s in Phase 4 "Operational Use"[22]

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.

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

The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. If the TOE is configured for use with Primary Inspection System s any terminal is assumed as Primary Inspection System and is allowed to read the logical MRTD. If the TOE is configured for use with Basic Inspection Systems only the Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System according to the SFR FIA_UAU.4/MRTD.

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.
The Chip ID is constant in the manufacturing and pre-personalization phases as part of the pre-personalization the Chip ID is changed to random ID.
When the identifier is randomly selected it will not violate the OT.Identification.

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

FIA_UAU.1 **Timing of authentication**
Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow

1) to read the Initialization Data in Phase 2 “Manufacturing”,
2) to read the ATS in Phase 3 “Personalization of the MRTD”,
3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,
4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System s in Phase 4 “Operational Use”[23]

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

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

The Primary Inspection System does not authenticate them. Only the Basic Inspection System and the Personalization Agent authenticate themselves

FIA_UAU.4/MRTD Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
Hierarchical to: No other components.

FIA_UAU.4.1/ MRTD The TSF shall prevent reuse of authentication data related to
1) Basic Access Control Authentication Mechanism,
2) Authentication Mechanism based on Triple-DES[24].

Dependencies: No dependencies.
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 [PKI], and the Authentication Mechanism based on Triple-DES shall use a Challenge as well.
The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [PKI]. 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

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

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

FIA_UAU.5 **Multiple authentication mechanisms**
Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide
1) Basic Access Control Authentication Mechanism
2) Symmetric Authentication Mechanism based on Triple-DES[25]

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[26].

Dependencies: No dependencies.

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 [PKI], 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

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

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

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.

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

FIA_UAU.6/MRTD Re-authenticating – Re-authenticating of Terminal by the TOE
Hierarchical to: No other components.

FIA_UAU.6.1/MRTD The TSF shall re-authenticate the user under the conditions each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism[27].

Dependencies: No dependencies.

The Basic Access Control Mechanism specified in [PKI] 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.

Class FDP User Data Protection

SUBSET ACCESS CONTROL (FDP_ACC.1)

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

FDP_ACC.1 Subset access control – Primary Access Control

Hierarchical to: No other components.

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

FDP_ACC.1.1/ PRIM

The TSF shall enforce the Primary Access Control SFP[28] on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD[29].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1 Subset access control – Basic Access control
Hierarchical to: No other components.

The data groups DG1 to DG16 of the logical MRTD as defined in [LDS] are the only TOE User data. The Primary Access Control SFP address the TOE usage with Primary Inspection Systems and Basic Inspection Systems independent on the configuration of the TOE.

FDP_ACC.1.1/ BASIC

The TSF shall enforce the Basic Access Control SFP[30] on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD[31].

Dependencies: FDP_ACF.1 Security attribute based access control

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

SECURITY ATTRIBUTE BASED ACCESS CONTROL (FDP_ACF.1)

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

[28] [assignment: *access control SFP*]

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

[30] [assignment: *access control SFP*]

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

FDP_ACF.1 Security attributes based access control – Primary Access Control

Hierarchical to: No other components.

FDP_ACF.1.1/PRIM

The TSF shall enforce the Primary Access Control SFP[32] to objects based on the following:

1) Subjects:
   a) Personalization Agent,
   b) Terminals,
2) Objects: data into 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[33].

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 MRTD34.

FDP_ACF.1.3/ PRIM

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[35].

---

[32] [assignment: access control SFP]

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

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

[35] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to

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[36].

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

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 unauthorized changes.

FDP_ACF.1 Security attributes based access control – Basic Access Control
Hierarchical to: No other components.

FDP_ACF.1.1/ BASIC

The TSF shall enforce the Basic Access Control SFP[37] to objects based on the following:

1) Subjects:
   a) Personalization Agent
   b) Primary Inspection System
2) Objects: data into 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[38].

objects]

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

[37] [assignment: *access control SFP*]

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

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[39].

FDP_ACF.1.3/ BASIC

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[40].

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[41].

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

Inter-TSF-Transfer

FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

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

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

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

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD
Hierarchical to: No other components.

FDP_UCT.1.1/ MRTD
The TSF shall enforce the Basic Access Control SFP[42] to be able to transmit and receive[43] objects in a manner protected from unauthorized 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]

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

FDP_UIT.1/MRTD Data exchange integrity - MRTD
Hierarchical to: No other components.

FDP_UIT.1.1/ MRTD
The TSF shall enforce the Basic Access Control SFP[44] to be able to transmit and receive[45] user data in a manner protected from modification, deletion, insertion and replay[46] errors.

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

[43] [selection: *transmit, receive*]

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

[45] [selection: *transmit, receive*]

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

FDP_UIT.1.2/ MRTD

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[47] 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]

Class FMT Security Management

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

FMT_MOF.1 Specification of Management Functions
Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to enable and disable[48] the functions TSF Basic Access Control[49] to Personalization Agent[50].

Dependencies: No Dependencies

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

[48] [selection: *determine the behavior of, disable, enable, modify the behavior of*]

[49] [assignment: *list of functions*]

[50] [assignment: *the authorized identified roles*]

The enabling and disabling the TSF Basic Access Control defines the configuration of the TOE in Phase 3 “Personalization of the MRTD” before use in the phase 4 “Operational Use”:

1. The TOE is configured with Primary Inspection systems when the TSF Basic Access Control is disabled. In this configuration the TOE enforces the Primary Access Control SFP according to FDP_ACC.1/PRIM and FDP_ACF.1/PRIM. In this case the logical MRTD may be read without successful authentication as Basic Inspection System or Personalization Agent.
2. The TOE is configured with Basic Inspection Systems only when the TSF Basic Access Control is enabled. In this configuration the TOE enforces the Basic Access Control SFP according to FDP_ACC.1/BASIC and FDP_ACF.1/BASIC. In this case the reading of the logical MRTD requires successful authentication as Basic Inspection System or Personalization Agent.

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

FMT_SMF.1 **Specification of Management Functions**
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[51].

Dependencies: No Dependencies

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

FMT_SMR.1 **Security roles**
Hierarchical to: No other components.

[51] [assignment: list of security management functions to be provided by the TSF]

FMT_SMR.1.1

The TSF shall maintain the roles
1) Manufacturer,
2) Personalization Agent,
3) Primary Inspection System,
4) Basic Inspection System[52].

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

Hierarchical to: FIA_UID.1 Timing of identification.

The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

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

FMT_LIM.1 Limited capabilities
Hierarchical to: No other components.

[52] [assignment: the authorized identified roles]

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.

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

FMT_LIM.2 **Limited availability**
Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow

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

Dependencies: FMT_LIM.1 Limited capabilities.

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

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/ INI_ENA

The TSF shall restrict the ability to write[53] the Initialization Data and Pre-personalization Data[54] to the Manufacturer[55].

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

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.

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

Hierarchical to: No other components.

[53] [selection: change default, query, modify, delete, clear, [assignment: other operations]]

[54] [assignment: list of TSF data]

[55] [assignment: the authorized identified roles]

FMT_MTD.1.1/ INI_DIS

The TSF shall restrict the ability to disable read access for users to[56] the Initialization Data[57] to the Personalization Agent[58].

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

According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by

i. allowing to write these data only once and

ii. Blocking the role Manufacturer at the end of the Phase 2.

The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides 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”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

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

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_WRITE

The TSF shall restrict the ability to write[59] the Document Basic Access Keys[60] to the Personalization Agent[61].

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

[56] [selection: change default, query, modify, delete, clear, [assignment: other operations]]

[57] [assignment: list of TSF data]

[58] [assignment: the authorized identified roles]

[59] [selection: change default, query, modify, delete, clear, [assignment: other operations]]

[60] [assignment: list of TSF data]

[61] [assignment: the authorized identified roles]

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

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_READ

The TSF shall restrict the ability to read[62] the Document Basic Access Keys and Personalization Agent Keys[63] to none[64].

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

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.

Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information flow for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to 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.

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

[62] [selection: change default, query, modify, delete, clear, [assignment: other operations]]

[63] [assignment: list of TSF data]

[64] [assignment: the authorized identified roles]

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1

The TOE shall not emit power variations, timing variations during command execution[65] in excess of non-useful information[66] enabling access to *Personalization Agent Authentication Key*[67] and *none*[68].

FPT_EMSEC.1.2

The TSF shall ensure any unauthorized users[69] are unable to use the following interface smart card circuit contacts[70] to gain access to Personalization Agent Authentication Key[71] and *none*[72]

Dependencies: No other components.

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

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

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

65 [assignment: types of emissions]

66 [assignment: specified limits]

67 [assignment: list of types of TSF data]

68 [assignment: list of types of user data]

69 [assignment: type of users]

70 [assignment: type of connection]

71 [assignment: list of types of TSF data]

72 [assignment: list of types of user data]

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[73].

Dependencies: ADV_SPM.1 Informal TOE security policy model

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1

The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the request of the authorized user*[74] to demonstrate the correct operation of *the TSF*[75].

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

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

Dependencies: FPT_AMT.1 Abstract machine testing.

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

[74] [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]]

[75] [selection: [assignment: parts of TSF]

The TSF will run a self tests for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 will be executed during initial start-up by the "authorized user" Manufacturer in the Phase 2 Manufacturing. Other self tests will run automatically or at the request of an authorized user to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 Operational Use, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks.

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

FPT_PHP.3 **Resistance to physical attack**
Hierarchical to: No other components.

FPT_PHP.3.1

The TSF shall resist physical manipulation and physical probing[76] to the TSF[77] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

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

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

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

[76] [assignment: physical tampering scenarios]

[77] [assignment: list of TSF devices/elements]

FPT_RVM.1 **Non-bypassability of the TSP**
Hierarchical to: No other components.

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

Dependencies: No dependencies.

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

FPT_SEP.1 TSF **domain separation**
Hierarchical to: No other components.

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

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

Dependencies: No dependencies.

5.2. Security Assurance Requirements for the TOE

The evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following components:

ADV_IMP.2 and ALC_DVS.2

The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the MRTD’s chip especially for the absence of unintended functionality. The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD’s development and manufacturing especially for the secure handling of the MRTD’s material.
The minimum strength of function is 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.

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 [PKI] describes the requirements to the public key infrastructure for the 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).

FDP_DAU.1/DS Basic data authentication – Passive Authentication

Hierarchical to: No other components.

FDP_DAU.1.1/ DS The **Document Signer** shall provide a capability to generate evidence that can be used as a guarantee of the validity of logical the MRTD (DG1 to DG16) and the Document Security Object[78].

FDP_DAU.1.2/ DS The **Document Signer** shall provide Inspection Systems of Receiving States or Organization[79] with the ability to verify evidence of the validity of the indicated information.

There are no other SFR for Passive Authentication for the Environment, because this verification does not require processing capabilities of the chip and any reaction of the MRTD. Passive authentication proves only that the contents of the Document Security Object (SOD) and LDS are authentic and not changed.
In contrast to that there are some SFRs for Basic Inspection Systems listed in the following. Without these requirements, e.g. if the Inspection Systems uses a weak key, data that must be protected against disclosure becomes accessible for an attacker. The MRTD must rely on that the following SFRs are met.

[78] [assignment: list of objects or information types]

[79] [assignment: list of subjects]

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

FCS_CKM.1/BAC_BT Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal
Hierarchical to: No other components.

FCS_CKM.1.1/ BAC_BT

The **Basic Terminal** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[80] and specified cryptographic key sizes 112 bit[81] that meet the following: [PKI], Annex E[82].

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

The terminals derive the Document Basic Access Keys from the second line of the printed MRZ data by the algorithm described in [PKI], 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.

[80] [assignment: cryptographic key generation algorithm]

[81] [assignment: cryptographic key sizes]

[82] [assignment: list of standards]

FCS_CKM.4/BT Cryptographic key destruction - BT

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 physical deletion by overwriting the memory data with zeros or random data[83] that meets the following: none[84]. .

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

The basic terminal shall destroy the Document Basic Access Keys of the MRTD and the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging after inspection of the MRTD.

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 Personalization Terminal.

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

Hierarchical to: No other components.

FCS_COP.1.1/ SHA_BT

The **Basic Terminal** shall perform hashing[85] in accordance with a specified cryptographic algorithms SHA-1[86] and cryptographic key sizes none[87] that meet the following: FIPS 180- 2[88].

[83] [assignment: *cryptographic key destruction method*]

[84] [assignment: *list of standards*]

[85] [assignment: list of cryptographic operations]

[86] [assignment: cryptographic algorithm]

[87] [assignment: cryptographic key sizes]

[88] [assignment: list of standards]

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

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/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/ ENC_BT

The **Basic Terminal** shall perform secure messaging – encryption and decryption[89] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[90] and cryptographic key sizes 112 bit[91] that meet the following: FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)[92].

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

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.

[89] [assignment: list of cryptographic operations]

[90] [assignment: cryptographic algorithm]

[91] [assignment: cryptographic key sizes]

[92] [assignment: list of standards]

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

Hierarchical to: No other components.

FCS_COP.1.1/MAC_BT

The **Basic Terminal** shall perform secure messaging – message authentication code[93] in accordance with a specified cryptographic algorithm Retail-MAC[94] and cryptographic key sizes 112 bit[95] that meet the following: FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)[96].

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

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

The Terminal shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below. For the extended components definition refer to [PP] chapter 4.

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

Hierarchical to: No other components.

FCS_RND.1.1/BT

[93] [assignment: list of cryptographic operations]

[94] [assignment: cryptographic algorithm]

[95] [assignment: cryptographic key sizes]

[96] [assignment: list of standards]

The **Basic Terminal** shall provide a mechanism to generate random numbers that meets *functional class P2 with SOF-high of AIS31* [97].

Dependencies: No dependencies.

This SFR requires the terminal to generate random numbers used in the authentication protocols as required by FCS_CKM.1/BAC_BT and FIA_UAU.4 the quality metric shall be chosen to ensure at least the strength of function Basic Access Control Authentication for the challenges

This quality metric ensures the strength of function Basic Access Control Authentication for the challenges. The Terminal shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

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

Hierarchical to: No other components.

FIA_UAU.4.1/BT The **Basic Terminal** shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism [98].

Dependencies: No dependencies.

The Basic Access Control Authentication Mechanism [PKI] 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.

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

[97] [assignment: *list of standards*]

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

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

Hierarchical to: No other components.

FIA_UAU.6.1/BT The **Basic Terminal** shall re-authenticate the user under the conditions each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism[99].

Dependencies: No dependencies.

The Basic Access Control Mechanism specified in [PKI] 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.

The Basic Access Control SFP of the TOE requires protecting the User Data by access control (cf. FDP_ACC.1/BASIC and FDP.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.

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

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

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

Hierarchical to: No other components.

FDP_UCT.1.1/BT The Basic Terminal shall enforce the Basic Access Control SFP[100] to be able to transmit and receive[101] objects in a manner protected from unauthorized 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]

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

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

Hierarchical to: No other components.

FDP_UIT.1.1/BT The **Basic Terminal** shall enforce the Basic Access Control SFP[102] to be able to transmit and receive[103] user data in a manner protected from modification, deletion, insertion and replay[104] 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[105] 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]

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

[101] [selection: transmit, receive]

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

[103] [selection: transmit, receive]

[104] [selection: modification, deletion, insertion, replay]

[105] [selection: modification, deletion, insertion, replay]

Personalization Terminals

The TOE supports different authentication and access control mechanisms which may be use 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.

The Personalization Terminal shall meet the requirement "Authentication Proof of Identity (FIA_API)" as specified below (cf. [PP]).

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

Hierarchical to: No other components.

FIA_API.1.1/SYM_PT

The **Personalization Terminal** shall provide a Authentication Mechanism based on Triple-DES[106] to prove the identity of the Personalization Agent[107].

Dependencies: No dependencies.

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 [ISO 7816-4] 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).

[106] [assignment: authentication mechanism]

[107] [assignment: authorized user or rule]

6. TOE Summary Specification

6.1. TOE Security Functions

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

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

TOE Security Function	***SOF claim***	***Description***
SF.Cryptographic Support	High	The random number generators and hash functions are probabilistic mechanisms.
SF. Identification and Authentication	High	The mechanism for identification/authentication of the roles is probabilistic.
SF.Protection	High	This TOE Security Function is realized by a probabilistic or permutational noncryptographic mechanism.
SF.Security Management	not appropriate	This TOE Security Function is not realized by a probabilistic or permutational noncryptographic mechanism
SF.User Data Protection	not appropriate	This TOE Security Function is not realized by a probabilistic or permutational noncryptographic mechanism

Table 2 - TOE Security Functions and SOF claim

SF.Cryptographic Support

This Security Function provides the cryptographic support for the other Security Functions.
This Security Function is composed of:

1) DES key generation in accordance with the Document Basic Access Control Key Derivation Algorithm with key sizes of 112 bit that meet: [PKI], Annex E.

2) Hashing in accordance with SHA-1 that meet the following: FIPS 180-2.

3) Secure messaging – encryption and decryption with Triple-DES in CBC mode and key sizes of 112 bit that meet: [PKI]; Annex E.

4) Secure messaging – message authentication with Retail MAC and key sizes of 112 bit that meet: ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2).

5) Random number generation according to functional class P2 AIS31 for key generation and authentication process.

6) After each BAC session the relevant Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging are destroyed.

This Security Function has the level of strength SOF-high.

SF.Identification and Authentication

The identification and authentication for the TOE user is managed by this security function.

This Security Function is composed of:

1) Storage of IC Identification Data in audit records through the Manufacturer.

2) possibility to read before user identification and authentication:

- The Initialization Data in Phase 2 “Manufacturing”,

- The ATQB in Phase 3 “Personalization of the MRTD”,

- The ATQB if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,

- The logical MRTD if the TOE is configured for use with Primary Inspection Systems in Phase 4 “Operational Use”

Note: the functional requirement says ATS, ATS is for type A the TOE supports Type B. ATS for type B is ATQB.

3) TSF mediated actions on behalf of an user require his prior successful identification and authentication if Basic Access Control [PKI] is activated and if it is not specified in this chapter otherwise

4) Prevention of reuse of authentication data.

5) User authentication provided through:

- Basic Access Control Authentication Mechanism

- Symmetric Authentication Mechanism based on Triple-DES

6) User authentication for the Personalization Agent through:

- Symmetric Authentication Mechanism with the Personalization Agent Key

7) User authentication for the Basic Inspection System through:

- The Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

8) Enabling the authentication of an user under the conditions that each command is sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism

This Security Function has the level of strength SOF-high..

SF. User Data Protection

The user data protection is managed by this security function.
This Security Function is composed of:

1) In the TOE configuration for use with Primary Inspection Systems:

   • Allowing only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,

   • Allowing the terminals to read only the data of the groups DG1 to DG16 of the logical MRTD.

2) In the TOE configuration for use with Basic Inspection Systems

   • Allowing only the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,

   • Allowing only the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD [PKI].

3) Not allowing anybody to modify any of the data groups DG1 to DG16 of the logical MRTD in the usage phase

4) Ability to read the data of the groups DG1 to DG16 of the logical MRTD.

5) Ability to write the data of the data groups DG1 to DG16 of the logical MRTD.

6) Ensuring that transmitted and received user data is protected from modification, deletion, insertion and replay errors through secure messaging when BAC is enabled.

7) Ensuring that transmitted and received objects are protected from unauthorized disclosure through secure messaging when BAC is enabled.

8) Determination on receipt of user data if modification, deletion, insertion and replay have occurred through secure messaging when BAC is enabled

SF.Security Management

The security management of the TOE is managed by this security function.
This Security Function is composed of:

1) Enabling and disabling the TSF Basic Access Control only through the Personalization Agent.

2) Initialization, personalization and configuration of the TOE are only allowed for the Manufacturer and the Personalization Agent.

3) Ability to write the Initialization Data and Pre-personalization Data restricted to the Manufacturer.

4) Ability to disable read access for users to the Initialization Data restricted to the Personalization Agent.

5) Test Features of the TOE are not available for the user in Phase 4 “Operational Use”. If Test Features are performed by the TOE than no User Data can be disclosed or manipulated, no TSF data can be disclosed or manipulated, no software can be reconstructed and no substantial information about construction of TSF can be gathered which may enable other attacks.

6) Maintenance of the security roles: Manufacturer, Personalization Agent, Primary Inspection System, Basic Inspection System.

7) Only the Personalization Agent is allowed to write the Document Basic Access Keys.

8) Nobody is allowed to read the Document Basic Access Keys and Personalization Agent Keys.

SF.Protection (Protection of TSC)

This Security Function protects the TSF functionality, TSF data and user data. If BAC is enabled, no unencrypted data transmission between TOE and the outside of the TOE is allowed.
This Security Function is composed of:

1) Hiding information about IC power consumption and command execution time.

2) The TOE ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

3) Maintaining a security domain for the TSF execution that protects it from interference and tampering by entrusted subjects.

4) Enforcing separation between the security domains of subjects in the TSC.

5) Detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.

6) Detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

7) Ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Authentication Key and logical MRTD data.

8) Preserve a secure state when a failure is detected by TSF according to FPT_TST.1.

9) Run a suite of self tests during initial start-up, periodically during normal operation, at the condition Reset of the TOE to demonstrate the correct operation of the TSF.

10) Provide authorized users with the capability to verify the integrity of TSF data.

11) Provide authorized users with the capability to verify the integrity of stored TSF executable code.

This Security Function has the level of strength SOF-high.

6.2. Assurance Measures

The documentation is produced compliant to the CC. The following documents provide the necessary information to fulfill the assurance requirements listed in the following table:

Assurance Measure	Documentation
ACM_AUT.1	Documentation for Configuration Management
ACM_CAP.4	
ACM_SCP.2	
ADO_DEL.2	Documentation for Delivery and Operation
ADO_IGS.1	
ADV_FSP.2	Functional Specification for Apollo OS e-Passport
ADV_HLD.2	High-Level Design for Apollo OS e-Passport
ADV_IMP.2	Source Code for Apollo OS e-Passport
ADV_LLD.1	Low-Level Design for Apollo OS e-Passport
ADV_RCR.1	Correspondence Demonstration for Apollo OS e-Passport
AGD_ADM.1	Security Policy Model for Apollo OS e-Passport
AGD_USR.1	User Guidance for Apollo OS e-Passport
ALC_DVS.2	Documentation for development security for Apollo OS e-Passport
ALC_LCD.1	Life-cycle model documentation for Apollo OS e-Passport
ALC_TAT.1	Documentation of the development tools for Apollo OS e-Passport
ATE_COV.2	Test Documentation for Apollo OS e-Passport
ATE_DPT.1	Test Documentation for High-Level Design for Apollo OS e-Passport
ATE_FUN.1	Test Documentation of the Functional Testing for Apollo OS e-Passport
ATE_IND.2	Independent testing for Apollo OS e-Passport
AVA_MSU.2	Validation of analysis for Apollo OS e-Passport
AVA_SOF.1	Analysis of Strength of TSF for Apollo OS e-Passport
AVA_VLA.2	Independent vulnerability analysis for Apollo OS e-Passport
ADV_SPM.1	Security policy modeling for Apollo OS e-Passport

Table 3 - Assurance Measures

7. PP Claims

7.1. PP Reference

The conformance of this ST to the Protection Profile Common Criteria Protection Profile Machine Readable Travel Document with ”ICAO Application”, Basic Access Control, Version 1.0, 18.08.2005, BSI-PP-0017 [PP] is claimed.

7.2 PP Refinements

None.

7.3 PP Additions

None.

8. Rationale

8.1. Security Objectives Rationale

The chapters 8.1 and 8.2 have been taken from [PP] without modification and show that the security objectives cover the TOE security environment and IT security requirements are appropriate to satisfy the security objectives.
The tables in sub-sections 8.1, 8.2 and 8.3.1 Rationale for TOE Security Functions provide the mapping of the security objectives and security requirements for the TOE.

	OT.AC_PERS	OT.DATA_INT	OT.DATA_CONF	OT.IDENTIFICATION	OT.PROT_ABUSE_FUNC	OT.PROT_INF_LEAK	OT.PROT_PHYS_TAMPER	OT.MALFUNCTION	OD.ASSURANCE	OD.MATERIAL	OE.PERSONALIZATION	OE.PASS_AUTH_SIGN	OE.EXAM_MRTD	OE.PASSIVE_AUTH_VERIF	OE.PROT_LOGICAL_MRTD	OE.SECURE_HANDLING
T.CHIP_ID				X												X
T.SKIMMING			X													X
T.EAVESDROPPING			X													
T.FORGERY	X	X					X					X	X	X		
T.ABUSE_FUNC					X											
T.INFORMATION_LEAKAGE						X										
T.PHYS_TAMPER							X									
T.MALFUNCTION								X								
P.MANUFACT									X	X						
P.PERSONALIZATION	X								X		X					
P.PERSONAL_DATA		X	X													
A.PERS_AGENT											X					
A.INSP_SYS													X		X	

Table 4 -Security Objective Rationale

The threat **T.Chip_ID** “Identification of MRTD’s chip” addresses the trace of the MRTD movement by identifying remotely the MRTD’s chip through the contactless communication interface. In case of TOE configuration for use with Basic Inspection Terminals only this threat is countered as described by the security objective ***OT.Identification*** by Basic Access Control. If the TOE is configured for use with Primary Inspection Systems this threat shall be adverted by the TOE environment as described by ***OE.Secure_Handling***.

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

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

The threat **T.Abuse-Func** “Abuse of Functionality” addresses attacks using the MRTD’s chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. The security objectives for the TOE environment ***OD.Material*** “Control over MRTD Material” ensures the control of the MRTD material. The security objectives for the TOE environment ***OD.Assurance*** “Assurance Security Measures in Development and Manufacturing Environment” and ***OE.Personalization*** “Personalization of logical MRTD” ensure that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

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

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

The OSP **P.Personalization** “Personalization of the MRTD by issuing State or Organization only” addresses the

i. the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment ***OE.Personalization*** “Personalization of logical MRTD”, and

ii. the access control for the user data and TSF data as described by the security objective ***OT.AC_Pers*** “Access Control for Personalization of logical MRTD”. Note, the manufacturer equips the TOE with the Personalization Agent Authentication key(s) according to ***OD.Assurance*** “Assurance Security Measures in Development and Manufacturing Environment”. The security objective OT.AC_Pers limits the management of TSF data and the enabling and disabling of the TSF Basic Access Control to the Personalization Agent.

The OSP **P.Personal_Data** “Personal data protection policy” requires the TOE

i. to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and

ii. enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives ***OT.Data_Int*** “Integrity of personal data“which describes the unconditional protection of the integrity of the stored data and the configurable integrity protection during the transmission. The security objective ***OT.Data_Conf*** “Confidentiality of personal data” describes the protection of the confidentiality as configured by the Personalization Agent acting in charge of the issuing State or Organization.

The assumption **A.Pers_Agent** “Personalization of the MRTD’s chip” is covered by the security objective for the TOE environment ***OE.Personalization*** “Personalization of logical MRTD” including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data and the enabling of security features of the TOE according to the decision of the Issuing State or Organization concerning the Basic Access Control.

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objectives for the TOE environment ***OE.Exam_MRTD*** “Examination of the MRTD passport book”. If the Issuing State of Organization decides to protect confidentiality of the logical MRTD than the security objectives for the TOE environment ***OE.Prot_Logical_MRTD*** “Protection of data of the logical MRTD” will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling. If the Issuing State of Organization decides to configure the TOE for use with Primary Inspection Systems than no protection of the logical MRTD data is required by the inspection system.

8.2. Security Requirements Rationale

Security Functional Requirements Rationale

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

	OT.AC_PERS	OT.DATA_INT	OT.DATA_CONF	OT.IDENTIFICATION	OT.PROT_INF_LEAK	OT.PROT_PHYS_TAMPER	OT.PROT_MALFUNCTION	OT.PROT_ABUSE_FUNC
FAU_SAS.1				X				
FCS_CKM.1/BAC_MRTD	(X)	X	(X)					
FCS_CKM.4	(X)		X					
FCS_COP.1/SHA_MRTD	X	X	(X)					
FCS_COP.1/TDES_MRTD	X	X	X					
FCS_COP.1/MAC_MRTD	X	X	X					
FCS_RND.1/MRTD	(X)	X	X					
FIA_UID.1			X	X				
FIA_UAU.1			X					
FIA_UAU.4/MRTD	X	X	X					
FIA_UAU.5/MRTD	X	X	X					
FIA_UAU.6/MRTD	X	X	X					
FDP_ACC.1/PRIM	X	X						
FDP_ACF.1/PRIM	X	X						
FDP_ACC.1/BASIC	X	X	X					
FDP_ACF.1/BASIC	X	X	X					
FDP_UCT.1/MRTD	X	X	X					
FDP_UIT.1/MRTD	X	X	X					
FMT_MOF.1	X	X	X					
FMT_SMF.1	X	X	X					
FMT_SMR.1	X	X	X					
FMT_LIM.1								X
FMT_LIM.2								X
FMT_MTD.1/INI_ENA				X				
FMT_MTD.1/INI_DIS				X				
FMT_MTD.1/KEY_WRITE	X	X	X					
FMT_MTD.1/KEY_READ	X	X	X					

	OT.AC_PERS	OT.DATA_INT	OT.DATA_CONF	OT.IDENTIFICATION	OT.PROT_INF_LEAK	OT.PROT_PHYS_TAMPER	OT.PROT_MALFUNCTION	OT.PROT_ABUSE_FUNC
FPT_EMSEC.1	X				X			
FPT_TST.1					X		X	
FPT_RVM.1								X
FPT_FLS.1					X		X	
FPT_PHP.3					X	X		
FPT_SEP.1							X	X

Table 5 -Coverage of Security Objective for the TOE by SFR

The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” address the access control of the writing the logical MRTD and the management of the TSF for Basic access Control. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/PRIM and FDP_ACF.1/BASIC in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups DG1 to DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD and FIA_UAU.5/MRTD. In case the Basic Access Control Authentication Mechanism was used the SFR FIA_UAU.6/MRTD describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/BAC_MRTD, FCS_COP.1/SHA_MRD, FCS_RND.1 (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP:1/MAC_MRTD for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) because the Personalization Agent handles the configuration of the TSF Basic Access Control according to the SFR FMT_MOF.1 and the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data if Basic Access Control is enabled. The SFR FMT_MTD.1/KEY_READ preventing read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/PRIM and FDP_ACF.1/BASIC in the same way: only the Personalization Agent is allowed to write data of the groups DG1 to DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization)

If the TOE is configured for the use with Basic Inspection Terminals only by means of FMT_MOF.1 the security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD. The SFR FIA_UAU.6/MRTD, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/BAC_MRTD, FCS_COP.1/SHA_MRD, FCS_RND.1 (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY requires the Personalization Agent to establish the Document Basic Access Control Keys and the Personalization Agent handles the configuration of the TSF Basic Access Control according to the SFR FMT_MOF.1.

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups DG1 to DG16 if the TOE is configured for the use with Basic Inspection Systems by means of FMT_MOF.1. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. The read access to the logical MRTD data is defined by the FDP_ACC.1/BASIC and FDP_ACF.1.2/BASIC: only the successful authenticated Personalization Agent and the successful authenticated Basic Inspection System are allowed to read the data of the logical MRTD. The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Control Keys).

The SFR FIA_UAU.4/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The FIA_UAU.5 enforce the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 request secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the

transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode.

The SFR FCS_CKM.1/BAC_MRTD, FCS_CKM.4, FCS_COP.1/SHA_MRTD and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

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

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

Furthermore, if the TOE is configured for use with Basic Inspection Terminals the TOE shall identify themselves only to a successful authenticated Basic Inspection System in Phase 4 “Operational Use”. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data. The SFR FMT_MTD.1/INI_DIS allow the Personalization Agent to disable Initialization Data if their use in the phase 4 “Operational Use” violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD’s chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application note 28). The FMT_MTD.1/INI_ENA restricts the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

The security objective **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality” is ensured by (i) the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other which may not be used after TOE Delivery, (ii) the SFR FPT_RVM.1 which prevents by monitoring the bypass and deactivation of security features or functions of the TOE, and (iii) the SFR FPT_SEP.1 which prevents change or explore security features or functions of the TOE by means of separation the other TOE functions.

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

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

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

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

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

ii. the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction, and

iii. the SFR FPT_SEP.1 limiting the effects of malfunctions due to TSF domain separation.

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

	OE.PERSONALIZATION	OE.EXAM_MRTD	OE.PROT_LOGICAL_MRTD
Document Signer			
FDP_DAU.1/DS		X	
Terminal			
FCS_CKM.1/BAC_BT	X		X
FCS_CKM.4/BT			X
FCS_COP.1/SHA_BT	X		X
FCS_COP.1/ENC_BT	X		X
FCS_COP.1/MAC_BT	X		X
FCS_RND.1/BT	X		X
FIA_UAU.4/BT	X		X
FIA_UAU.6/BT	X		X
FIA_UCT.1/BT	X		X
FCS_UIT.1/BT	X		X
Personalization Agent			
FIA_AP I.1 /SYM_PT	X		

Table 6 - Coverage of Security Objectives for the IT environment by SFR

The document signer provides the security function Passive Authentication according to FDP_DAU.1 (DS to support the inspection system to verify the logical MRTD. The security objective **OE.Prot_Logical_MRTD** “Protection of data of the logical address the protection of handling. The SFR FIA_UAU.4/BT and FIA_UAU.6/BT address the terminal part of the Basic Access Control Authentication Mechanism and FDP_UCT.1/BT and FDP_UIT.1/BT the secure messaging established by this mechanism. The SFR FCS_CKM.1/BAC_BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT and FCS_RND.1/BT are necessary to implement this mechanism.

The BIS shall destroy the Document Access Control Key and the secure messaging key after inspection of the MRTD because they are not needed any more.

The **OE.Personalization** "Personalization of logical MRTD" requires the MRTD personalization terminal to authenticate themselves to the MRTD's chip to get the write authorization. This implies to implement the Basic Access Control Authentication Mechanism with the Personalization Agent Authentication Keys or support the symmetric authentication protocol according to the SFR FIA_API.1/SYM_PT.

Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.
The table 7 shows the dependencies between the SFR and of the SFR to the SAR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	N/A
FCS_CKM.1/BAC_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD justification 1 for non-satisfied dependencies
FCS_CKM.4/MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 1 for non-satisfied dependencies
FCS_COP.1/SHA_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security	FCS_CKM.1, FCS_CKM.4, justification 2 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	attributes	
FCS_COP.1/TDES_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 3 for non-satisfied dependencies
FCS_COP.1/MAC_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 3 for non-satisfied dependencies
FCS_RND.1/MRTD	No dependencies	N/A
FIA_UID.1	No dependencies	N/A
FIA_UAU.1	FIA_UAU.1 Timing of authentication	fulfilled
FIA_UAU.4/MRTD	No dependencies	N/A
FIA_UAU.5/MRTD	No dependencies	N/A
FIA_UAU.6/MRTD	No dependencies	N/A
FDP_ACC.1/PRIM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/PRIM
FDP_ACC.1/BASIC	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/BASIC
FDP_ACF.1/PRIM	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.1/PRIM, justification 4 for non-satisfied dependencies
FDP_ACF.1/BASIC	FDP_ACC.1 Subset access control, FMT_MSA.3 Static	FDP_ACC.1/BASIC, justification 4 for non-

SFR	Dependencies	Support of the Dependencies
	attribute initialization	satisfied dependencies
FDP_UCT.1/MRTD	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/BASIC, justification 5 for non-satisfied dependencies
FDP_UIT.1/MRTD	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/BASIC, justification 5 for non-satisfied dependencies
FMT_MOF.1	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	fulfilled
FMT_LIM.1	FMT_LIM.2	fulfilled
FMT_LIM.2	FMT_LIM.1	fulfilled
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FPT_EMSEC.1	No dependencies	N/A
FPT_FLS.1	ADV_SPM.1	fulfilled by EAL4

SFR	Dependencies	Support of the Dependencies
FPT_PHP.3	No dependencies	N/A
FPT_RVM.1	No dependencies	N/A
FPT_SEP.1	No dependencies	N/A
FPT_TST.1	FPT_AMT.1 Abstract machine testing	See justification 6 for non-satisfied dependencies

Table 7 - Dependencies between the SFR for the TOE

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

No. 1: The SFR FCS_CKM.1/BAC_MRTD uses only the Document Basic Access Keys to generate the secure messaging keys used for FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD. The SFR FCS_CKM.4/MRTD destroys these keys automatically. These simple processes do not need any special security attributes for the secure messaging keys.

No. 2: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR is needed to be defined for this specific instantiation of FCS_COP.1.

No. 3: The SFR FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD use the automatically generated secure messaging keys assigned to the session with the successfully authenticated BIS only. There is no need for any special security attributes for the secure messaging keys.

No. 4: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.2) is necessary here.

No. 5: The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the use secure messaging between the MRTD and the BIS. There is no need for additional SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels it is the only one.

No. 6: The TOE consists of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

The following table shows the dependencies between the SFR for the IT environment and of the SFR to the SAR of the TOE.

SFR	Dependencies	Support of the Dependencies
FDP_DAU.1	No dependencies	N/A
FCS_CKM.1/BAC_BT	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1/TENC_BT, FCS_COP.1/MAC_BT justification 7 for non-satisfied dependencies
FCS_CKM.4/BT	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 7 for non-satisfied dependencies
FCS_COP.1/SHA_BT	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 8 for non-satisfied dependencies
FCS_COP.1/ENC_BT	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 9 for non-satisfied dependencies
FCS_COP.1/MAC_BT	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 9 for non-satisfied dependencies
FCS_RND.1/BT	No dependencies	N/A
FIA_UAU.4/BT	No dependencies	N/A
FIA_UAU.6/BT	No dependencies	N/A

SFR	Dependencies	Support of the Dependencies
FDP_UCT.1/BT	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/BASIC, justification 10 for non-satisfied dependencies
FDP_UIT.1/BT	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/BASIC, justification 10 for non-satisfied dependencies
FIA_API.1/SYM_PT	No dependencies	N/A

Table 8 - Dependencies between the SFR for the IT environment

Justification for non-satisfied dependencies between the SFR for the IT environment.

No. 7: The SFR FCS_CKM.1/BT derives the Document Basic Access Keys and uses this key to generate the secure messaging keys used for FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD. The SFR FCS_CKM.4/BT destroys these keys. These processes do not need any special security attributes for the secure messaging keys.
No. 8: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR is needed to be defined for this specific instantiation of FCS_COP.1.
No. 9: The SFR FCS_COP.1/ENC_BT and FCS_COP.1/MAC_BT use the automatically generated secure messaging keys assigned to the session with the successfully authenticated MRTD only. There is no need for any special security attributes for the secure messaging keys.
No. 10: The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the use secure messaging between the MRTD and the BIS. There is no need to provide further description of this communication.

Security Assurance Requirements Rationale

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

The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the MRTD's chip especially for the absence of unintended functionality.

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

The minimal strength of function "high" was selected to ensure resistance against direct attacks on functions based on probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE to fulfill OT.AC_PERS and OT.Data_Conf if the TOE is configured for the use with Basic Inspection Systems. This is consistent with the security objective OD.Assurance.

The components ADV_IMP.2 and ALC_DVS.2 augmented to EAL4 have dependencies to other security requirements fulfilled within EAL4
Dependencies ADV_IMP.2
ADV_LLD.1 Descriptive low-level design
ALC_TAT.1 Well-defined development tools
Dependencies ALC_DVS.2: no.

8.3. Statement of Compatibility between the Composite Security Target and the Platform Security Target

This chapter shows that the security objectives, security requirements and security functionality in the Composite-ST and the Platform-ST are compatible

8.3.1. Separation of the Platform-TSF

SEF1: Operating state checking is relevant Platform-TSF, because the operating state is monitored with sensors for the operating voltage, clock signal frequency, and temperature and electromagnetic radiation. The TOE falls into the defined secure state in case of a specified range violation. The defined secure state causes the chip internal reset process.
The parameters for the filters and sensors are set during production and not accessible by the Embedded Software after TOE finishing.

Thus the FPT_FLS.1 and FPT_SEP.1 defined in Composite-ST are covered.

SEF2: Phase management with test mode lock-out is relevant Platform-TSF, because during start-up of the TOE the decision for the user mode or the test mode is taken dependent on several phase identifiers (phase management). If test mode is the active phase the TOE requests authentication before any action (test mode lock-out)
If the chip identification mode is requested the chip identification data (O.Identification) stored in a non modifiable EEPROM area is reported.

Thus the security functional requirements FMT_LIM.1, FMT_LIM.2 and FAU_SAS.1 defined in Composite-ST are covered.

SEF3: Protection against snooping is relevant Platform-TSF, because several mechanisms protect the TOE against snooping the design or the user data during operation and even it is out of operation (power down). The entire design is kept in a non standard way to prevent attacks using standard analysis methods. A Smartcard dedicated CPU with a non public bus protocol is used which makes analysis complicated.
Thus the security functional requirements FPT_PHP.3 defined in Composite-ST are satisfied.

SEF4: Data encryption and data disguising is irrelevant.

SEF5: Random number generation is relevant Platform-TSF, because the TOE is equipped with a true random generator based on physical probabilistic controlled effects. The random data can be used from the Smartcard Embedded Software as well as from the security enforcing functions. The generated numbers are true random due to the construction principle.
Thus the security functional requirements FCS_RND.1 defined in Composite-ST are covered.

SEF6: TSF self test is relevant Platform-TSF, because the TSF of the TOE has either hardware controlled self test which can be started from the Smartcard Embedded Software by a RMS function call or can be tested directly from the Smartcard Embedded Software for the active shield. As any attempt to modify the sensor devices will be detected from the test.
Thus the security functional requirements FPT_TST.1 defined in Composite-ST are covered.

SEF7: Notification of physical attack is relevant Platform-TSF, because the entire surface of the TOE is protected with the active shield. Attacks over the surface are detected when the shield lines are cut or get contact. The attempt to use an opened device will be detected.
Thus the security functional requirements FPT_PHP.3 defined in Composite-ST are covered.

SEF8: Memory Management Unit (MMU) is relevant Platform-TSF, because the MMU in the TOE gives the Smartcard Embedded Software the possibility to define different access rights for memory areas and components.
Thus the security functional requirements FDP_ACC.1 and FDP_ACF.1defined in Composite-ST are covered.

SEF9: Cryptographic Support is relevant Platform-TSF, because the TOE is equipped with several hardware accelerators to support the standard cryptographic operations. The component is a hardware DES encryption unit. The key for the cryptographic 3DES operations are provided from the Smartcard Embedded Software (environment).
Thus the security functional requirements FCS_COP.1.1/ TDES_MRTD and FCS_COP.1/MAC_MRTD defined in Composite-ST are covered.

8.3.2. Platform-SFR

According to the mapping in table 16 “mapping of SFR and SEF” chapter 6.10 in the platform-ST the following platform-ST SFR are relevant for the composite-ST:

Platform SFR	Composite SFR	Rational
FAU_SAS.1.1	FAU_SAS.1.1	The requirements are match they have the same meaning
FCS_RND.1	FCS_RND.1	The requirements are match they have the same meaning
FMT_LIM.1	FMT_LIM.1	The requirements are match they have the same meaning
FMT_LIM.2	FMT_LIM.2	The requirements are match they have the same meaning
FPT_FLS.1	FPT_FLS.1	The requirements are match they have the same meaning
FPT_PHP.3.1	FPT_PHP.3.1	The requirements are match they have the same meaning
FPT_SEP.1.1	FPT_SEP.1.1	The requirements are match they have the same meaning
FPT_SEP.1.2	FPT_SEP.1.2	The requirements are match they have the same meaning
FRU_FLT.2.1		The requirement is not specified in Composite-ST, however according to the specification of this requirement it is used by the Composite-ST
FPT_TST.2.1	FPT_TST.1.1	The requirements are match they have the same meaning
FDP_ACC.1.1	FDP_ACC.1.1/ PRIM	The requirements are match they have the same

		meaning
FDP_ACF.1	FDP_ACF.1	The requirements are match they have the same meaning
FMT_SMF.1	FMT_SMF.1	The requirements are match they have the same meaning
FMT_MSA.3.1		The requirement is not to find in Composite-ST, however according to the dependencies between the SFR it is used by the Composite-ST
FMT_MSA.3.2		The requirement is not to find in Composite-ST, however according to the dependencies between the SFR it is used by the Composite-ST
FMT_MSA.1		The requirement is not to find in Composite-ST, however according to the dependencies between the SFR it is used by the Composite-ST
FCS_COP.1	FCS_COP.1.1/ TDES_MRTD FCS_COP.1/MAC_MRTD	The requirements are match they have the same meaning
FDP_SDI.1		The requirement is not to find in Composite-ST, however according to the dependencies between the SFR it is used by the Composite-ST
FDP_SDI.2		The requirement is not to find in Composite-ST, however according to the dependencies between the SFR it is used by the Composite-ST

Table 9 – Mapping of Platform SFRs and Composite SFRs

8.3.3. Platform-SFR for the environment

According to the description in Platform-ST paragraphs 5.2.1 / 5.2.2 the following SFRs for the environment are relevant for Composite-ST.

Platform SFR	Composite SFR	Rational
FDP_ITC.1		The requirement is not to find in Composite-ST, however according to the dependencies between the SFR it is used by the Composite-ST.
FCS_CKM.4	FCS_CKM.4/BT	The requirements are match they have the same meaning
FMT_MSA.2		The requirement is not to find in Composite-ST, however according to the dependencies between the SFR it is used by the Composite-ST.
FCS_CKM.1.1	FCS_CKM.1.1	The requirements are match they have the same meaning
RE.Phase-1	FDP_UCT.1.1/ MRTD FDP_UIT.1.1/ MRTD FDP_UIT.1.2/ MRTD FMT_MOF.1.1	The requirements are match they have the same meaning
RE.Cipher	FMT_MTD.1.1/ KEY_READ	The requirements are match they have the same meaning

Table 10 – Mapping of Platform SFRs for the environment and Composite SFRs

8.3.4. Platform-Security Objectives

According to Platform-ST paragraph 8.2 the following security objectives defined in Platform-ST are relevant for Composite-ST

Platform Security objective	Composite security objective	Rational
O.Add-Functions	OT.Data_Conf OT.AC_Pers	the composite-ST security objective OT.Data_Conf OT.AC_Pers matches the platform-ST security objective O.Add-Functions 1 And O.Add-Functions 2 is Used by the embedded software according to composite – ST FCS_CKM.1 and FCS_COP.1
O.Phys-Manipulation	OT.Data_Int OT.Prot_Phys-Tamper	The security objectives are match they have the same meaning
O.Malfunction	OT.Prot_Malfunction	The security objectives are match they have the same meaning
O.Leak-Inherent	OT.Prot_Inf_Leak Protection	The security objectives are match they have the same meaning
O.Phys-Probing	OT.Prot_Inf_Leak	The security objectives are match they have the same meaning
O.Leak-Forced	OT.Prot_Inf_Leak	The security objectives are match they have the same meaning
O.Abuse-Func	OT.Prot_Abuse_Func	The security objectives are match they have the same meaning
O.Identification	OT.Identification	The security objectives are match they have the same meaning
O.RND		This security objective is Used by the embedded software according to FCS_RND.1.

Table 11 – Mapping of Platform security objectives and Composite security objectives

8.3.5. Platform-Security Objectives for the environment

According to the Platform-ST paragraph 8.2 the following security objectives for the environment defined in Platform-ST are relevant for Composite-ST.

Platform Security objective	Composite security objective	Rational
OE.Plat-Appl	OT.Data_Int, OT.Prot_Inf_Leak	The security objectives are match they have the same meaning
OE.Resp-Appl	OT.AC_Pers	The security objectives are match they have the same meaning
OE.Process-TOE	OD.Assurance	The security objectives are match they have the same meaning
OE.Process-Card	OE.Personalization	The security objectives are match they have the same meaning

Table 12 – Mapping of Platform security objectives for the environment and Composite security objectives

8.3.6. Platform-Assumptions

According to the Platform -ST paragraph 8.1 the following assumptions defined in Platform-ST are relevant for Composite-ST.

Platform assumption	Composite assumption	Rational
A.Process-Card		Covered by OD.Assurance
A.Key-Function		considered for the development of the embedded software
A.Plat-Appl		considered for the development of the embedded software
A.Resp-Appl		considered for the development of the embedded software

Table 13 – Mapping of Platform assumptions and Composite assumptions

8.3.7. Platform-OSPs

According to the Platform-ST paragraph 8.1 the following OSPs defined in Platform-ST are relevant for Composite-ST.

Platform OSP	Composite OSP	Rational
P.Add-Functions	P.Personal_Data	The OSPs are match the have the same meaning
P.Process-TOE	P.Manufact P.Personalization	The OSPs are match the have the same meaning

Table 14 – Mapping of Platform OSPs and Composite OSPs

8.3.8. Platform-Threats

According to Platform-ST paragraph 8.1 the following threats defined in Platform-ST are relevant for Composite-ST.

Platform Threats	Composite Threats	Rational
T.Leak-Inherent	T.Information_Leakage	The threats are match the have the same meaning
T.Phys-Probing	T.Phys_Tamper	The threats are match the have the same meaning
T.Malfunction	T.Malfunction	The threats are match the have the same meaning
T.Phys-Manipulation	T.Forgery T.Phys_Tamper	The threats are match the have the same meaning
T.Leak-Forced	T.Information_Leakage	The threats are match the have the same meaning
T.Abuse-Func	T.Abuse_Func	The threats are match

Table 15 – Mapping of Platform threats and Composite threats

8.4. TOE Summary Specification Rationale

In this section it is shown that the security functions are suited to fulfil the security requirements. It is demonstrated that at least one security function meets each security requirement. Furthermore it is shown that all security functions are needed and that they form an integrated unity to meet the security requirements.

Fulfilling the Security Functional Requirements

	SF.Cryptographic Support	SF.Identification and Authentication	SF. User Data Protection	SF.Security Management	SF.Protection (Protection of TSC)
FAU_SAS.1.1		1			
FCS_CKM1.1/BAC_MRTD	1				
FCS_CKM.4.1/MRTD	6				
FCS_COP.1.1/SHA_MRTD	2				
FCS_COP.1.1/TDES_MRTD	3				
FCS_COP.1.1/MAC_MRTD	4				
FCS_RND.1.1/MRTD	5				
FIA_UID.1.1		2			
FIA_UID.1.2		3			
FIA_UAU.1.1		2			
FIA_UAU.1.2		3			
FIA_UAU.4.1/MRTD		4			
FIA_UAU.5.1		5			
FIA_UAU.5.2		6,7			
FIA_UAU.6.1/MRTD		8			
FDP_ACC.1.1/PRIM			1		

	SF.Cryptographic Support	SF.Identification and Authentication	SF. User Data Protection	SF.Security Management	SF.Protection (Protection of TSC)
FDP_ACC.1.1/BASIC			2		
FDP_ACF.1.1/PRIM			1		
FDP_ACF.1.2/PRIM			1,4,5		
FDP_ACF.1.3/PRIM			1		
FDP_ACF.1.4/PRIM			3		
FDP_ACF.1.1/ BASIC			2		
FDP_ACF.1.2/ BASIC			2,4,5		
FDP_ACF.1.3/ BASIC			2		
FDP_ACF.1.4/ BASIC			3		
FDP_UCT.1.1/MRTD			7		
FDP_UIT.1.1/MRTD			6		
FDP_UIT.1.2/MRTD			8		
FMT_MOF.1.1				1	
FMT_SMF.1.1				2	
FMT_SMR.1.1				6	
FMT_SMR.1.2				6	
FMT_LIM.1.1				5	
FMT_LIM.2.1				5	
FMT_MTD.1.1/INI_ENA				3	
FMT_MTD.1.1/INI_DIS				4	
FMT_MTD.1.1/KEY_WRITE				7	
FMT_MTD.1.1/KEY_READ				8	

	SF.Cryptographic Support	SF.Identification and Authentication	SF. User Data Protection	SF.Security Management	SF.Protection (Protection of TSC)
FPT_EMSEC.1.1					1
FPT_EMSEC.1.2					7
FPT_FLS.1.1					8,6
FPT_TST.1.1					9
FPT_TST.1.2					10
FPT_TST.1.3					11
FPT_PHP.3.1					5
FPT_RVM.1.1					2
FPT_SEP.1.1					3
FPT_SEP.1.2					4

Table 16 - Assignment: security requirements – security functions

Justifications for the correspondence between functional requirements and security functions

FAU_SAS.1.1 requires that the Manufacturer has the capability to store the IC Identification Data in the audit records. SF.Identification and Authentication.1 states that the Storage of IC Identification Data in audit records through the Manufacturer is supported by the TOE and therefore meets the above stated TOE SFR.

FCS_CKM.1.1/ BAC_MRTD requires that the Document Basic Access Control Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [PKI], Annex E. are applied. SF.Cryptographic Support.1 states that DES key generation in accordance with the Document Basic Access Control Key Derivation Algorithm with key sizes of 112 bit that meet: [PKI], Annex E are supported by the TOE and therefore meets the above stated TOE SFR.

FCS_CKM.4.1/ MRTD requires that cryptographic keys are destroyed in accordance with a specified cryptographic key destruction method physical deletion by overwriting the memory data with zeros or random data that meets the following: none. SF.Cryptographic Support.6 states that after each BAC session the relevant Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging are destroyed and therefore meets the above stated TOE SFR.

FCS_COP.1.1/ SHA_MRTD requires that hashing is performed in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: FIPS 180-2. SF.Cryptographic Support.2 states that hashing by the TOE is performed in accordance with SHA-1 that meet the following: FIPS 180-2 and therefore meets the above stated TOE SFR.

FCS_COP.1.1/ TDES_MRTD requires that secure messaging – encryption and decryption is performed in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: [PKI]; Annex E. SF.Cryptographic Support.3 states that secure messaging – encryption and decryption is performed with Triple-DES in CBC mode and key sizes of 112 bit that meet: [PKI]; Annex E and therefore meets the above stated TOE SFR.

FCS_COP.1.1/MAC_MRTD requires that secure messaging – message authentication code is performed 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). SF.Cryptographic Support.4 states that secure messaging – message authentication is performed with Retail MAC and key sizes of 112 bit that meet: ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2) and therefore meets the above stated TOE SFR.

FCS_RND.1.1/ MRTD requires that the TSF shall provide a mechanism to generate random numbers that meet AIS31. SF.Cryptographic Support.5 states that random number generation according AIS31 for key generation and authentication process is supported by the TOE and therefore meets the above stated TOE SFR.

FIA_UID.1.1 requires that the TSF shall allow
(1) To read the Initialization Data in Phase 2 “Manufacturing”,
(2) To read the ATS in Phase 3 “Personalization of the MRTD”,
(3) To read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,
(4) To read the logical MRTD if the TOE is configured for use with Primary Inspection System s in Phase 4 “Operational Use” on behalf of the user to be performed before the user is identified.
SF.Identification and authentication.2 states that the TOE realizes the possibility to read before user identification and authentication:

- The Initialization Data in Phase 2 “Manufacturing”,

- The ATQB in Phase 3 “Personalization of the MRTD”,

- The ATQB if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,

- The logical MRTD if the TOE is configured for use with Primary Inspection Systems in Phase 4 “Operational Use”

and therefore meets the above stated TOE SFR.

FIA_UID.1.2 requires that TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
SF.Identification and authentication.3 states that the TSF mediated actions on behalf of a user require his prior successful identification and authentication if it is not specified in this chapter otherwise and therefore meets the above stated TOE SFR.

FIA_UAU.1.1 requires that the TSF shall allow
(1) To read the Initialization Data in Phase 2 “Manufacturing”,
(2) To read the ATS in Phase 3 “Personalization of the MRTD”,
(3) To read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,
(4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System s in Phase 4 “Operational Use” on behalf of the user to be performed before the user is authenticated.
SF.Identification and authentication.2 states that the TOE realizes the possibility to read before user identification and authentication:

- The Initialization Data in Phase 2 “Manufacturing”,

- The ATQB in Phase 3 “Personalization of the MRTD”,

- The ATQB if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”,

- The logical MRTD if the TOE is configured for use with Primary Inspection Systems in Phase 4 “Operational Use”

and therefore meets the above stated TOE SFR.

FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
SF.Identification and authentication.3 states that the TSF mediated actions on behalf of a user require his prior successful identification and authentication if it is not specified in this chapter otherwise and therefore meets the above stated TOE SFR.

FIA_UAU.4.1/ MRTD requires that the TSF shall prevent reuse of authentication data related to
1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on Triple-DES.
SF.Identification and authentication.4 realizes the prevention of reuse of authentication data and therefore meets the above stated TOE SFR.

FIA_UAU.5.1 requires that the TSF shall provide
1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on Triple-DES
to support user authentication.
SF.Identification and authentication.5 realizes user authentication provided through:

- Basic Access Control Authentication Mechanism

- Symmetric Authentication Mechanism based on Triple-DES

and therefore meets the above stated TOE SFR.

FIA_UAU.5.2 requires that 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.

SF.Identification and authentication.6 realizes User authentication for the Personalization Agent through:

- Symmetric Authentication Mechanism with the Personalization Agent Key

SF.Identification and authentication.7 realizes user authentication for the Basic Inspection System through:

- The Basic Access Control Authentication Mechanism with the Document Basic Access Keys

and therefore meets the above stated TOE SFR.

FIA_UAU.6.1/MRTD requires that 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.
SF.identification and authentication.8 enables the authentication of a user under the conditions that each command is sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and therefore meets the above stated TOE SFR.

FDP_ACC.1.1/ PRIM requires that 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.
SF.user data protection.1 in the TOE configuration for use with Primary Inspection Systems:

- allows only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,
- allows only the terminals to read the data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACC.1.1/ BASIC requires that 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.
SF.user data protection.2 in the TOE configuration for use with Basic Inspection Systems only

- allows the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
- allows the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.1/PRIM requires that 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 into 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.
SF.user data protection.1 in the TOE configuration for use with Primary Inspection Systems:

- allows only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,

- allows only the terminals to read the data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.2/ PRIM requires that 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.
SF.user data protection.1 in the TOE configuration for use with Primary Inspection Systems:

- allows only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,

- allows only the terminals to read the data of the groups DG1 to DG16 of the logical MRTD

SF.user data protection.5 realizes the ability to write the data of the data groups DG1 to DG16 of the logical MRTD.
SF.user data protection.4 realizes the ability to read the data of the groups DG1 to DG16 of the logical MRTD and therefore meets the above stated TOE SFR.

FDP_ACF.1.3/ PRIM requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
SF.user data protection.1 in the TOE configuration for use with Primary Inspection Systems:

- allows only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,
- allows only the terminals to read the data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.4/ PRIM requires that 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.
SF.user data protection.3 is not allowing the terminals to modify any of the data groups DG1 to DG16 of the logical MRTD in the usage phase and therefore meets the above stated TOE SFR.

FDP_ACF.1.1/ BASIC requires that the TSF shall enforce the Basic Access Control SFP to objects based on the following:
1. Subjects:
a. Personalization Agent
b. Primary Inspection System
2. Objects: data into 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.
SF.user data protection.2 in the TOE configuration for use with Basic Inspection Systems only

- allows the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
- allows the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.2/ BASIC requires that 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.
SF.user data protection.2 in the TOE configuration for use with Basic Inspection Systems only

- allows the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
- allows the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD

SF.user data protection 5 realizes the ability to write the data of the data groups DG1 to DG16 of the logical MRTD.
SF.user data protection.4 realizes the ability to read the data of the groups DG1 to DG16 of the logical MRTD and therefore meets the above stated TOE SFR.

FDP_ACF.1.3/ BASIC requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
SF.user data protection.2 in the TOE configuration for use with Basic Inspection Systems only

- allows the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
- allows the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.4/ BASIC requires that 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.
SF.user data protection.3 is not allowing anybody to modify any of the data groups DG1 to DG16 of the logical MRTD in the usage phase and therefore meets the above stated TOE SFR.

FDP_UCT.1.1/ MRTD requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure.
SF.user data protection.7 ensures that transmitted and received objects are protected from unauthorized disclosure through secure messaging when BAC and therefore meets the above stated TOE SFR.

FDP_UIT.1.1/ MRTD requires that 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.
SF.user data protection.6 ensures that transmitted and received user data is protected from modification, deletion, insertion and replay errors through secure messaging when BAC is enabled and therefore meets the above stated TOE SFR.

FDP_UIT.1.2/ MRTD requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.
SF.user data protection.8 determines on receipt of user data if modification, deletion, insertion and replay has occurred through secure messaging when BAC is enabled and therefore meets the above stated TOE SFR.

FMT_MOF.1.1 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.
SF.security managment.1 enables and disables the TSF Basic Access Control only through the Personalization Agent. With enabled Basic Access Control secure messaging is enabled which enables to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred and therefore meets the above stated TOE SFR.

FMT_SMF.1.1 requires that the TSF shall be capable of performing the following security management functions:
1. Initialization,
2. Personalization
3. Configuration.

SF.security managment.2 assigns initialization, personalization and configuration to the Manufacturer and Personalization Agent and therefore meets the above stated TOE SFR.

FMT_SMR.1.1 requires that the TSF shall maintain the roles
1. Manufacturer,
2. Personalization Agent,
3. Primary Inspection System,
4. Basic Inspection System.
SF.security managment.6 maintains the security roles: Manufacturer, Personalization Agent, Primary Inspection System, Basic Inspection System and therefore meets the above stated TOE SFR.

FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles.
SF.security managment.6 maintains the security roles: Manufacturer, Personalization Agent, Primary Inspection System, Basic Inspection System and therefore meets the above stated TOE SFR.

FMT_LIM.1.1 requires that the TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.
SF.security managment.5 deploys Test Features after TOE Delivery that does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks and therefore meets the above stated TOE SFR.

FMT_LIM.2.1 requires that the TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.
SF.security managment.5 deploys Test Features after TOE Delivery that does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/ INI_ENA requires that the TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.
SF.security managment.3 has the ability to write the Initialization Data and Pre-personalization Data restricted to the Manufacturer and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/ INI_DIS requires that the TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.
SF.security managment.4 has the ability to disable read access for users to the Initialization Data restricted to the Personalization Agent and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/ KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent.
SF.security managment.7 restricts the ability to write the Document Basic Access Keys to the Personalization Agent and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/ KEY_READ requires that the TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none.
SF.security managment.8 restricts the ability to read the Document Basic Access Keys and Personalization Agent Keys to none and therefore meets the above stated TOE SFR.

FPT_EMSEC.1.1 requires that the TOE shall not emit information about IC power consumption and command execution time in excess of non useful information enabling access to Personalization Agent Authentication Key and logical MRTD data.
SF.protection.1 hides information about IC power consumption and command execution time, to ensure that the IC contacts VCC, GND and IO can not be used to gain access to Personalization Agent Authentication Key and logical MRTD data and therefore meets the above stated TOE SFR.

FPT_EMSEC.1.2 requires that 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 logical MRTD data.
SF. protection.7 Ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Authentication Key and logical MRTD data and therefore meets the above stated TOE SFR.

FPT_FLS.1.1 requires that 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.
SF.protection.8 preserves a secure state when a failure is detected by TSF according to FPT_TST.1.
SF.Protection.6 provides Detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

and therefore meets the above stated TOE SFR.

FPT_TST.1.1 requires that the TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the condition Reset of the TOE to demonstrate the correct operation of the TSF.
SF.protection.9 provide suite of self tests during initial start-up, periodically during normal operation, at the condition Reset of the TOE to demonstrate the correct operation of the TSF and therefore meets the above stated TOE SFR.

FPT_TST.1.2 requires that the TSF shall provide authorized users with the capability to verify the integrity of TSF data.
SF.protection.10 provides authorized users with the capability to verify the integrity of TSF data and therefore meets the above stated TOE SFR.

FPT_TST.1.3 requires that the TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.
SF.protection.11 provides authorized users with the capability to verify the integrity of stored TSF executable code and therefore meets the above stated TOE SFR.

FPT_PHP.3.1 requires that the TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the TSP is not violated.
SF.protection.5 provides detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation and therefore meets the above stated TOE SFR.

FPT_RVM.1.1 requires that the TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. SF.protection.2 provides the invocation of TSP enforcement functions. After succeeding each function within the TSC is allowed to proceed and therefore meets the above stated TOE SFR.

FPT_SEP.1.1 requires that the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
SF.protection.3 maintains a security domain for the TSF execution that protects it from interference and tampering by untrusted subjects and therefore meets the above stated TOE SFR.

FPT_SEP.1.2 requires that the TSF shall enforce separation between the security domains of subjects in the TSC.
SF.protection.4 enforces separation between the security domains of subjects in the TSC and therefore meets the above stated TOE SFR.

Consistency of the Strength of Function Claims

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

8.5. PP Claims Rationale

Since the ST security objectives and requirements are identical to those of the claimed PP [PP], this part of the ST is omitted.

8.6. Abbreviations

CC	Common Criteria, see [CC]
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
SEF	Security Enforcing Functions
SOF	Strength of Function
TSF	TOE Security Functions
TSC	TOE Scope of Control
TSP	TOE Security Policy
BIS	Basic Inspection System
OSP	Organizational Security Policy
PIS	Primary Inspection System
SAR	Security assurance requirements
SFP	Security Function Policy
SFR	Security Function Requirement

8.7. References

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

[CC-1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001

[CC-2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002

[CC-3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

[CC-4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

[PKI] MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, International Civil Aviation Organization, Version 1.1, October 01 2004

[SSMR] Annex to Section III Security Standards for Machine Readable Travel Documents, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[PP_IC] 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

[FIPS] 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

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

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

[CCDB] Composite product evaluation for Smart Card and similar devices