LG CNS

# XSmart e-Passport V1.5 BAC with AA on M7892

# Security Target

The certified ST is written in Korean(including some English). This document is a translation of the original from Korean into English.

# [ History ]

| Version | Scope | History | Date |
|---|---|---|---|
| V1.0 | New | New Publication | 2021.11.30 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# [ Table of Contents ]

# Referenced Documents

| | |
|---|---|
| [CC] | Common Criteria for Evaluation of IT Security, Version 3.1r5 |
| [CEM] | Common Criteria Methodology for Evaluation of IT Security , Version 3.1r5, CCBM-2017-04-004 |
| [CCMB] | CCMB-2017-04-004, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation |
| [PACE-PP-0068] | Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22th July 2014 |
| [EAC-PP-0056] | Common Criteria Protection Profile Machine Readable Travel Document with ,,ICAO Application", Extended Access Control with PACE (EAC-PP) version 1.3.2, 5th December 2012 |
| [ICPP] | Security IC Platform Protection Profile; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007, Version 1.0, June 2007 |
| [BAC-PP-0055] | Protection Profile - Machine Readable Travel Document with ICAO Application and Basic Access Control, BSI-CC-PP-0055, Version 1.10, 25th March 2009 |
| [ICST] | Security Target Lite M7892 B11 Recertification including optional Software Libraries November, 2020. BSI-DSZ-CC-0782-V5-2020 |
| [GPCS] | GlobalPlatform Card Specification, Version 2.1.1, GlobalPlatform Inc., March 2003 |
| [MRTD] | ICAO Doc 9303, Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs, seventh Edition, 2015 |
| [EAC] | Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents -Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26. February 2015 |
| [KM] | ISO/IEC 11770-3: Information technology . Security techniques . Key management -- Part 3: Mechanisms using asymmetric techniques, 2008 |
| [ISO14443] | ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11 |
| [ISO7816] | ISO/IEC 7816: Identification cards . Integrated circuit cards, Version Second Edition, 2008 |
| [PKCS] | PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993 |
| [ECC-TR] | Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, 17.04.2009 |
| [AIS31] | Functionality classes and evaluation methodology for physical random number generators AIS31, Version 2.1, 2011-12-02 |

# 1. Introduction

This section provides the information necessary for identifying security target and TOE.

## 1.1. Security Target Reference

| | |
|---|---|
| Subject | XSmart e-Passport V1.5 BAC with AA on M7892 Security Target |
| ST Identification | XSMART e-Passport V1.5_ASE(BAC with AA)_V1.4.docx |
| Version | V1.4 |
| Author | LG CNS |
| Evaluation Criteria | Information Protection System Common Criteria V3.1r5 |
| Evaluation Assurance Level | EAL4+ (ALC_DVS.2,ATE_DPT.2) |
| Protection Profile | BSI-CC-PP-0055 |
| Keywords | ICAO, machine readable travel document, basic access control |

Table 1 Reference of Security Target

## 1.2. TOE Reference

| | |
|---|---|
| TOE Name | XSmart e-Passport V1.5 BAC with AA on M7892<br>- TOE Release Date : 2021.10.12 |
| Component of TOE | - SW: e-Passport_V15(source code image)<br>- User Guide for Management ( XSMART e-Passport V1.5_AGD(BAC with AA)_V1.3.docx )<br>- HW: IC Chip |
| TOE code identification | Hexa code :<br>e-Passport_V15_CLFX2400P.hex (impelemented on SLE78CLFX2400P)<br>e-Passport_V15_CLFX3000P.hex(impelemented on SLE78CLFX3000P)<br>e-Passport_V15_CLFX4000P.hex(impelemented on SLE78CLFX4000P) |
| IC Chip | Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware) |
| IC Chip reference | BSI-DSZ-CC-0782-V5-2020 |

Table 2 Reference of TOE

## 1.3. TOE Boundaries

This document is the security target regarding the XSmart e-Passport V1.5 BAC with AA on M7892 (referred to as **"XSmart e-Passport"** hereafter), which is the composite TOE composed of a COS in charge of the chip operating system and an IC chip as a part of hardware. TOE supports Basic Access Control and Active Authentication according to [MRTD].

XSmart e-Passport is the composed of HAL(Hardware Abstraction Layer), AML(Application Middle Layer), LDS layer and IC Chip H/W.

- HAL(Hardware Abstraction Layer) actually performs I/O handling according to ISO/IEC 7816 and ISO/IEC 14443 and memory management through the chip interface. It supports the DES/RSA/AES/ECC security function using H/W Crypto Library.

- AML(Application Middle Layer) that lies in the middle of HAL and LDS layer provides useful function required for key management, transaction, encryption mechanism.

- LDS layer supports [MRTD] standard functions of the BAC and AA defined by the International Civil Aviation Organization (ICAO).
  After the first e-passport program is loaded in FLASH area, it is activated through the installation and issuance process.

- SLE 78CLFX2400P/3000P/4000P are the contact/contactless IC chips from Infineon Technologies that have been certified by the Common Criteria from BSI.
  - Protection Profile: Security IC Platform Protection Profile, Version 1.0, June 2007, BSI-PP-0035-2007
  - TOE : Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware)
  - Certification Number : BSI-DSZ-CC-0782-V5-2020
  - Assurance level: CC EAL 6+ (ALC_FLR.1)
  - Certified cryptography library: RSA4096 v2.07.003, EC v2.07.003, SHA-2 v1.01

- Library for TOE :
  - RSA API(CI70-LIB-4k-XSMALL-HUGE.lib)
  - Toolbox API(CI70-LIB-toolbox-XSMALL-HUGE.lib)
  - Basic Crypto Functions(CI70-LIB-base-XSMALL-HUGE.lib)

The TOE uses the IC chip's authentication cryptographic library RSA4096, but only uses the RSA2048 cryptographic logic

### 1.3.1 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) and providing Basic Access Control.

The TOE comprises of

- the circuitry of the contactless/contact chip incl. all IC dedicated software
- Hardware abstraction layer for IC chip (HAL)
- The Application middle layer for MRTD application (AML)
- the MRTD application (LDS)
- the associated guidance documentation

### 1.3.2 TOE Usage and Security Features for Operational Use

A State or organization issues MRTD to be used by the holder for international travel. The traveler presents a MRTD to the Inspection System to prove his or her identity. The MRTD in context of this 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 traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) 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 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)
3. the printed portrait

the logical MRTD as data of the MRTD holder stored according to the Logical Data Struc ture 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
4. the other data according to LDS (EF.DG5 to EF.DG16)
5. the Document Security Object

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

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g.control of materials, personalization procedures). 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 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[ MRTD].
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. In addition, this Security Target address the Active Authentication

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (Secure Messaging) with this inspection system [ICAO Doc 9303], normative appendix 5.

### 1.3.3 TOE Life Cycle

The TOE life cycle is described in terms of the four life cycle phases. With respect to [ICPP], the TOE life cycle is additionally subdivided into 7 step.

Phase 1: Development

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

(Step 2) The software developer 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 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

(Step 3) In a first step the TOE integrated circuit is produced containing the MRTD's chip

Dedicated Software and the parts of the MRTD's chip Embedded Software in the 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 manufacturer to the MRTD manufacturer.
If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories.

(Step 4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book

(Step 5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD's chips with pre-personalization Data.

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

(Inlay production) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book. The inlay production including the application of the antenna is NOT part of the TOE and takes part after the delivery.

Phase 3: Personalization of the MRTD

(Step 6) The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrollment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object.

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

Phase 4: Operational Use

(Step 7) The TOE is used as MRTD chip by the traveler and the Inspection Systems in the "Operational Use" phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

### 1.3.4 Non-TOE hardware/software/firmware required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application.

Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

### 1.3.5 TOE SCOPE

This security target includes native e-passport program and IC chip hardware with firmware and crypto library.

#### 1.3.5.1. Physical scope of TOE

This picture illustrates the physical scope of TOE.

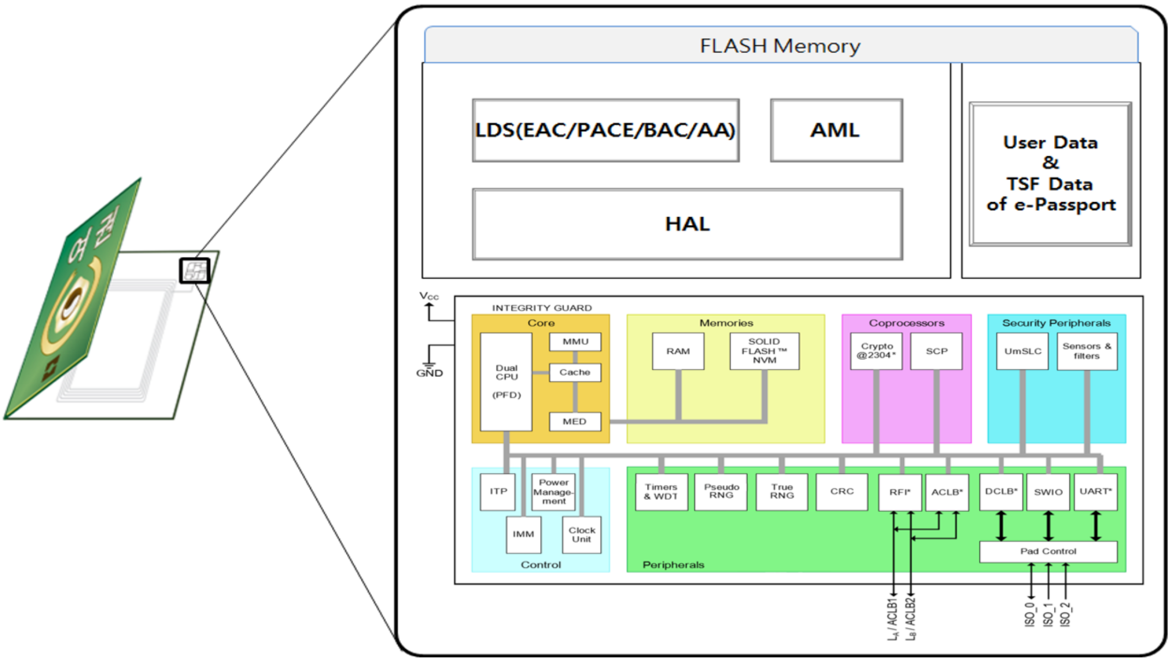


Figure. Physical scope of TOE

The physical scope of TOE includes the IC chip in the passport booklet, e-Passport application with user data and TSF data.
The components of IC chip as are CPU, Crypto Co-Processor, I/O, Memory (RAM, FLASH), and various H/W functions.

The ICAO defines the baseline security methods Passive Authentication, and Basic Access control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control in the [MRTD].
This security target address the protection of the logical MRTD by Basic Access Control and Active Authentication but does not address the Extended Access Control and Password Authenticated Connection Establishment.

In IC Chip's flash area, after e-Passport application is installed, flash area is changed to locked state.
Also, e-passport data like biometric data (face, fingerprint) and TSF data (keys for authentication, seed key for BAC) are saved in the flash area.

Infineon SLE 78CLFX2400P/3000P/4000P which is the composition element of the IC chip, is a product certified with CCRA EAL 6+ assurance level, and the composition elements included in the authentication are IC chip hardware and cryptographic calculation software library as shown in the following. However, unspecified libraries are not included in the scope of the TOE.

IC Chip hardware

- 16 bit microprocessor(CPU)
- 8KB RAM
- ROM : Not user available, H/W only)
- FLASH : 240KB(2400P), 300KB(3000P), 404KB(4000P)
- Memory Protection Unit(MPU), Random Number Generator(RNG), Timer(TIM), Crypto co-processor
- RF interface, address and data bus(ADBUS)
- True Random Number Generator (TRNG)

Software library for cryptographic operation

- 3DES , AES, RSA/ECC library
- Hash function( SHA-224, SHA-256, SHA-384, SHA-512)

Application Note:

For SHA-1, it is implemented as a separate software, only the portion that is used as part of the electronic passport is the TOE scope.

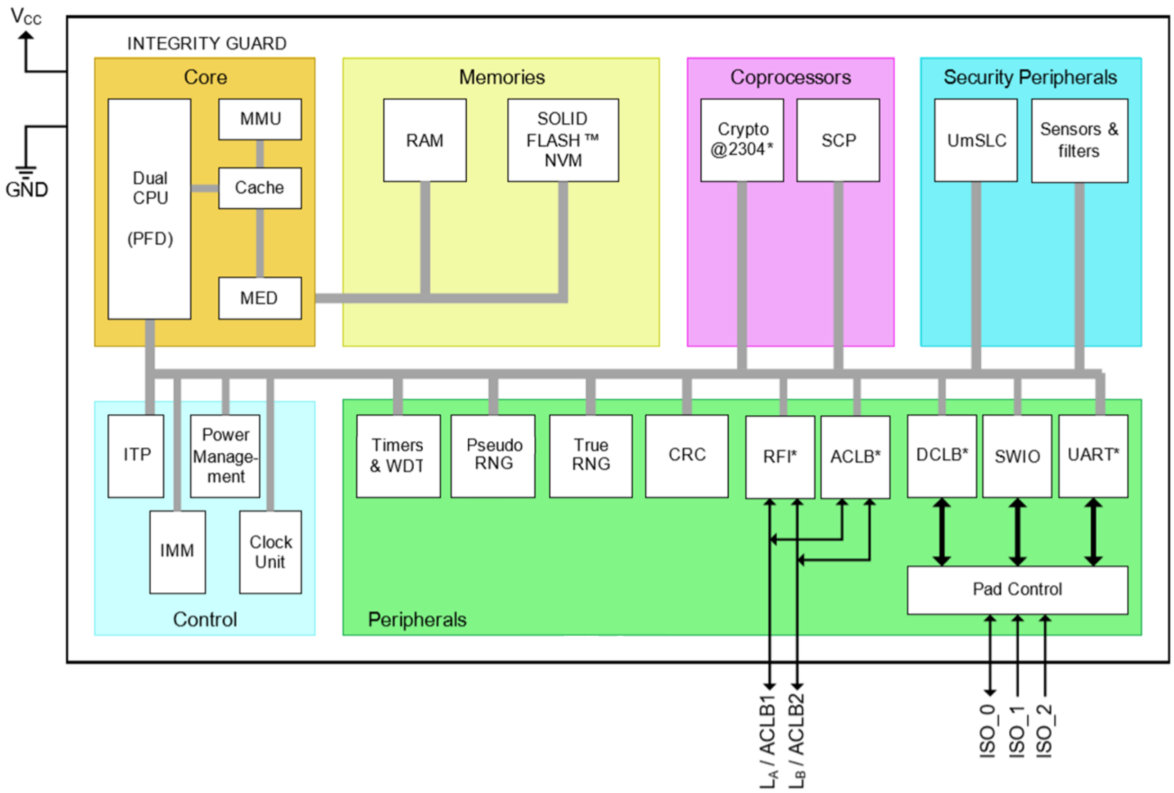


Figure. IC Chip H/W diagram

The IC chip hardware provide SCP module used in the symmetric key encryption according to DES and AES standards, Crypto 2304T Crypto module used in the asymmetric key encryption, physical security measures such as shield, temperature sensor, voltage sensor, and filter, and non-determinant hardware random number generator.
The firmware provides IC chip hardware management function such as flash download or hardware testing. The cryptographic calculation software library provides calculations such as digital signature generation/verification for hash value, ECDH key exchange, ECC/RSA key pair generation, and ECC/RSA public key verification.

SCP(Symmetric Crypto)

- TDES encryption and decryption
- Retail MAC and Full Triple DES MAC generation/verification
- AES encryption and decryption

Crypto@2404T

- Big Number calculation for RSA/ECC cryptographic calculation
- Key distribution calculation for ECC session key distribution
- ECC Digital signature verification calculation for ECDSA
- Digital signature generation calculation with RSA algorithms

SHA-2 library
This library provides SHA-224, SHA-256, SHA-384, SHA-512. However, HMAC is not included in the scope of the TOE.

### 1.3.5.2. Logical scope of TOE

TOE communicates with the inspection system according to the communication protocol defined in ISO/IEC 14443-4. TOE implements the security mechanism BAC and AA defined in [MRTD].
This picture illustrates the logical scope of TOE.

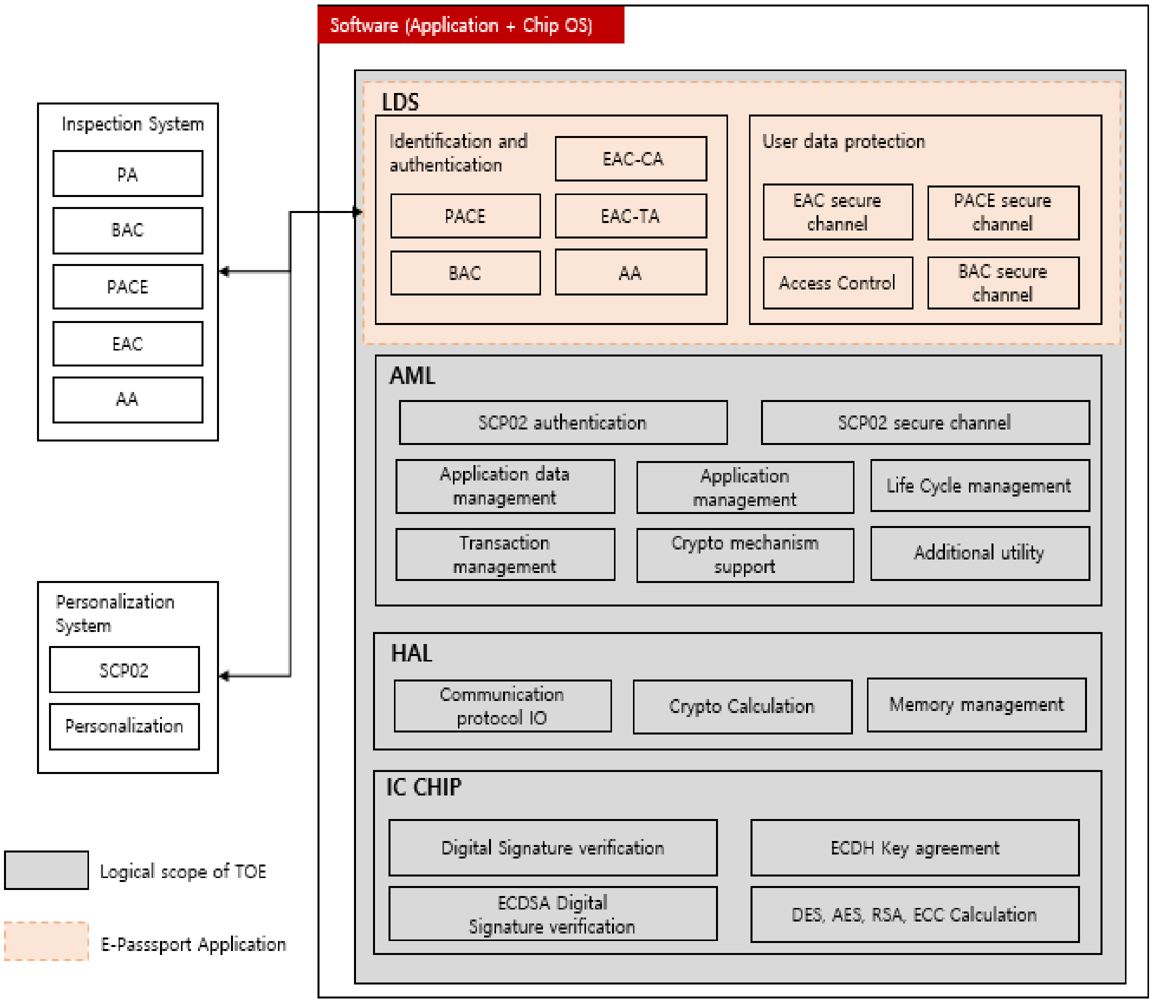


Figure. Logical scope of TOE

### e-Passport application (LDS)

e-Passport application program is an IC chip application program which implements the function for storing/processing e-passport identity information and the security mechanism to securely protect it according to the LDS (Logical Data Structure) format in [MRTD]. e-passport application program provides security management function for e-passport application program to the authenticated Personalization agent through SCP02 security mechanism provided in the card manager, and permits access to e-passport user data through BAC secure messaging only when the access rights were acquired through BAC secure messaging. Also, AA security mechanisms are provided as methods to judge counterfeiting of e-passport user data.

### Application Middle Layer(AML)

AML is a middle layer for electronic passport application, in conjunction with HAL, to support the functions of logic necessary for the key management, transaction and encryption operations.

**Hardware Abstraction Layer(HAL)**

HAL is the hardware-dependent IC chip implementation like IC chip booting, hardware resource management, algorithm operation using crypto library, security configuration setting of the IC chip. For SHA-1, it is implemented as a separate software, only the portion that is used as part of the electronic passport is the TOE scope.

**Physical attack countermeasures**

To prevent a variety of physical attack from the outside, IC Chip protection is enabled. Upon detecting a security violation, OS responds as card response stop, delay of card response, card termination.

In addition, it provides a defense function to prevent various external attacks such as side-channel attacks and active shield, and provides a function to defend against various attacks using sensors that detect abnormal environments (temperature, voltage, light, etc.).

# 2. Conformance Claims

## 2.1. CC Conformance Claim

This security target claims conformance to

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

as follows

- Part 2 extended,
- Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1 Revision 5, April 2017[CEM] has to be taken into account.

## 2.2. PP Reference

The conformance of this ST to the Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10, BSI-CC-PP-0055 [BAC-PP-0055] is claimed.

## 2.3. Package Claim

This security target is conforming to assurance package EAL4 augmented with ALC_DVS.2 and ATE_DPT.2 defined in [CC-3].

## 2.4. Conformance rationale

This ST claims strict conformance to the [BAC-PP-0055].

# 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 EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [ICAO Doc 9303]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the Inspection System for the Chip Authentication and the Active Authentication Public Key (EF.DG15) for Active Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons the [ICAO Doc 9303] specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

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

The TOE prevents read access to sensitive User Data

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

A sensitive 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 holder is used by the traveler to prove his possession of a genuine MRTD.

**Subjects**

ST 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.

**Personalization Agent**

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object.

**Terminal**

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

**Inspection system (IS)**

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System (BIS) (i) contains a terminal for the 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 MRTD or other parts of the passport book providing this information. The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism.

The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

**MRTD Holder**

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

**Traveler**

Person presenting the MRTD to the Inspection System and claiming the identity of the MRTD holder.

**Attacker**

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

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

## 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.MRTD_Manufact MRTD manufacturing on steps 4 to 6**

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

**A.MRTD _Delivery MRTD delivery during steps 4 to 6**

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

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

**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 Chip Authentication Public Key (EF.DG14)if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip).

The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

**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 traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

**A.BAC-Keys (Cryptographic quality of Basic Access Control Keys)**

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the [ICAO Doc 9303], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

## 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)**
**Adverse action** An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.
**Threat agent** Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.
**Asset** Anonymity of user.

**T.Skimming (Skimming the logical MRTD)**
**Adverse action** An attacker imitates an Inspection System trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.
**Threat agent** Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.
**Asset** Confidentiality of logical MRTD data.

**T.Eavesdropping (Eavesdropping to the communication between TOE and Inspection System)**
**Adverse action** An attacker is listening to an existing 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 these data in advance.
**Threat agent** Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.
**Asset** Confidentiality of logical MRTD data.

**T.Forgery (Forgery of data on MRTD's chip)**
**Adverse action** An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.
This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book,

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

**Threat agent** Having enhanced basic attack potential, being in possession of one or more legitimate MRTDs.

**Asset** Authenticity of logical MRTD data.

The TOE shall avert the threats as specified below.

**T.Abuse-Func (Abuse of Functionality)**

**Adverse action** An attacker may use functions of the TOE which shall not be used in "Operational Use" 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.

**Threat agent** Having enhanced basic attack potential, being in possession of a legitimate MRTD.

**Asset** Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

**T.Information_Leakage (Information Leakage from MRTD's chip)**

**Adverse action** 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).

**Threat agent** Having enhanced basic attack potential, being in possession of a legitimate MRTD.
**Asset** Confidentiality of logical MRTD and TSF data.

**T.Phys-Tamper (Physical Tampering)**
**Adverse action** 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) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the Inspection System) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.
**Threat agent** Having enhanced basic attack potential, being in possession of a legitimate MRTD.
**Asset** Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

**T.Malfunction (Malfunction due to Environmental Stress)**
**Adverse action** An attacker may cause a malfunction of TSF or of the MRTD's chip Em bedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software. This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

**Threat agent** Having enhanced basic attack potential, being in possession of a legitimate MRTD.

**Asset** Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

**T. Counterfeit**

**Adverse action** An attacker may be disguised as a genuine holder with copying data stored on the e-Passport and counterfeiting the data page.

**Threat agent** Having enhanced basic attack potential

**Asset** Logical data of e-Passport

## 3.4. Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

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

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

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

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

**P.Personal Data Personal data protection policy**

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13,EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by Inspection Systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the 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 [ICAO Doc 9303].

# 4. Security Objectives

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

## 4.1. Security Objectives for the TOE

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

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

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Note: The OT.AC_Pers implies that

1. the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) cannot be changed by write access after personalization
2. the Personalization Agents may (i) add (fill) DATA_INTo the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

**OT.Data_Int (Integrity of personal data)**

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

**OT.Data_Conf (Confidentiality of personal data)**

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself 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.

Note: The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.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. This Security Objective requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' that the Inspection System derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this Security Target. Thus the read access must be prevented even in case of a successful BAC Authentication.

**OT.Identification (Identification and Authentication of the TOE)**

The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 Manufacturing and Phase 3 Personalization of the MRTD. The storage of the Pre-Personalization Data includes writing of the Personalization Agent Key(s).
In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated
Basic Inspection System or Personalization Agent.

Note: 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 and for traceability and/or to secure shipment of the TOE from Phase 2 into the Phase 3. This Security Objective addresses security features of the TOE to be used by the TOE manufacturing.

In the Phase 4 the TOE is identified by the Document Number as part of the printed and digital MRZ. This Security Objective forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

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

**OT.AA_Proof Proof of MRTD'S chip authenticity**

The TOE must support the Basic and General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO-9303]. The authenticity prove provided by MRTD's chip shall be protected against attacks with enhanced basic attack potential.

**OT.Prot_Abuse_Func (Protection against Abuse of Functionality)**

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

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

**OT.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

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

**OT.Prot_Phys-Tamper (Protection against Physical Tampering)**

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with basic-enhanced 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.

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

## 4.2. Security Objectives for the Operational Environment

**Issuing State or Organization**

The Issuing State or Organization will implement the following Security Objectives of the TOE environment.

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

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

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

**OE.MRTD_Delivery Protection of the MRTD delivery**

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

- Non-disclosure of any security relevant information
- Identification of the element under delivery
- Meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment)
- Physical protection to prevent external damage
- Secure storage and handling procedures (including rejected TOE's)
- Traceability of TOE during delivery including the following parameters:
    - Origin and shipment details
    - Reception, reception acknowledgment
    - Location material/information

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

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

**OE.Personalization Personalization of logical MRTD**

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

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

**OE.BAC-Keys Cryptographic quality of Basic Access Control Keys**
The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

**OE.AA_Key_MRTD MRTD Active Authentication Key**
The issuing State or Organization has to establish the necessary public key infra-structure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) sign the Active Authentication Private Key, and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 (if generated), and (iii) support inspection systems of receiving States or organization to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip and Active Authentication Public Key by means of the Document Security Object.

**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 traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control .

**OE.Passive_Auth_Verif Verification by Passive Authentication**

The border control officer of the receiving State uses the Inspection System to verify the traveler as MRTD holder. The Inspection Systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing CA Public Key and the Document Signer 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 or Organization 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).

## 4.3. Security Objective Rationale

Table 4.1 provides an overview for security objectives coverage.

| | OT.AC_Pers | OT.Data_Int | OT.Data_Conf | OT.Identification | OT.Prot_Abuse-Func | OT.Prot_Inf_Leak | OT.Prot_Phys-Tamper | OT.AA_Proof | OT.Prot_Malfunction | OE.MRTD_Manufact | OE.MRTD_Delivery | OE.Personalization | OE.Pass_Auth_Sign | OE.BAC-Keys | OE.Exam_MRTD | OE.Passive_Auth_Verif | OE.Prot_Logical_MRTD | OE.AA_Key_MRTD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.Chip_ID | | | | x | | | | | | | | | | x | | | | |
| T.Skimming | | | x | | | | | | | | | | | x | | | | |
| T.Eavesdropping | | | x | | | | | | | | | | | | | | | |
| T.Forgery | x | x | | | | | x | | | | | | x | | x | x | | |
| T.Abuse-Func | | | | | x | | | | | | | x | | | | | | |

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.Information_Leakage | | | | | | x | | | | | | | | | | | | |
| T.Phys-Tamper | | | | | | | x | | | | | | | | | | | |
| T.Malfunction | | | | | | | | | x | | | | | | | | | |
| T.Counterfeit | | | | | | | | x | | | | | | | | | | x |
| P.Manufact | | | | x | | | | | | | | | | | | | | |
| P.Personalization | x | | | x | | | | | | | | | | | | | | |
| P.Personal_Data | | x | x | | | | | | | | | | | | | | | |
| A.MRTD_Manufact | | | | | | | | | | x | | | | | | | | |
| A.MRTD_Delivery | | | | | | | | | | | x | | | | | | | |
| A.Pers_Agent | | | | | | | | | | | | x | | | | | | |
| A.Insp_Sys | | | | | | | | | | | | | | | x | | x | |
| A.BAC-Keys | | | | | | | | | | | | | | x | | | | |

Table 4.1: Security Objective Rationale

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

The OSP **P.Personalization** "Personalization of the MRTD by issuing State or Organization only" addresses the (i) the enrollment 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 Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the 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" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT.Data_Conf** "Confidentiality of personal data" describes the protection of the confidentiality.

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. This threat is countered as described by the security objective **OT.Identification** by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys.**

The threat **T.Skimming** "Skimming digital MRZ data or the digital portrait" and **T.Eavesdropping** "Eavesdropping to the communication between TOE and inspection system" address the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective **OT.Data_Conf** "Confidentiality of personal data" through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys.**

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 objec tive **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRTD passport book according to **OE.Exam_MRTD** "Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive 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 **OE.Passive_Auth_Verif** "Verification by Passive Authentication".

The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks of misusing MRTD's functionality to disable or bypass the TSFs. The security objective for the TOE **OT.Prot_Abuse-Func** "Protection against abuse of functionality" ensures that the usage of functions which may not be used in the "Operational Use" phase is effectively prevented. Therefore attacks intending to abuse functionality in order to disclose or manipulate critical (User) Data or to affect the TOE in such a way that security features or TOE's functions may be bypassed, deactivated, changed or explored shall be effectively countered. Additionally this objective is supported by the security objective for the TOE environment

**OE.Personalization** "Personalization of logical MRTD" ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

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 threats **T. Counterfeit** are the threats through the unauthorized reproduction of data copy or passport itself. This threat is countered directly by OT.AA_Proof. The Active Authentication Public Key has to be written into EF.DG15 as demanded by **OE.AA_Key_MRTD** "MRTD Authentication Key".

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

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

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 enrollment, the protection with digital signature and the storage of the MRTD holder personal data.

The examination of the MRTD passport book addressed by the assumption **A.Insp_ Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the MRTD passport book". The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data from the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

The assumption **A.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" is directly covered by the security objective for the TOE environment **OE.BAC-Keys** "Crypto graphic quality of Basic Access Control Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization.

# 5. Extended Components Definition

This Security target uses components defined as extensions to CC part 2. Some of these components are defined in protection profile [ICPP], other components are defined in the protection profile [BAC-PP-0055].

## 5.1. DEFINITION OF THE FAMILY FAU_SAS

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

**FAU_SAS Audit data storage**

Family behaviour

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

Component levelling

FAU_SAS Audit storage
1

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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

**FAU_SAS.1 Audit storage**

Hierarchical to: No other components

Dependencies: No dependencies

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

## 5.2. DEFINITION OF THE FAMILY FCS_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class

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

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

**FCS_RND Generation of random numbers**

Family behaviour

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

Component leveling:

FCS_RND Generation of random numbers
1

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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

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

Hierarchical to: No other components

Dependencies: No dependencies

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

## 5.3. DEFINITION OF THE FAMILY FIA_API

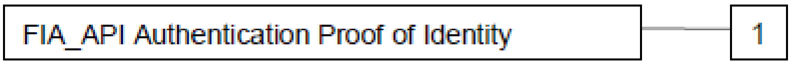
To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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

**FIA_API Authentication Proof of Identity**

Family behaviour

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

Component levelling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

**FIA_API.1 Authentication Proof of Identity**

Hierarchical to: No other components

Dependencies: No dependencies

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

## 5.4. DEFINITION OF THE FAMILY FMT_LIM

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

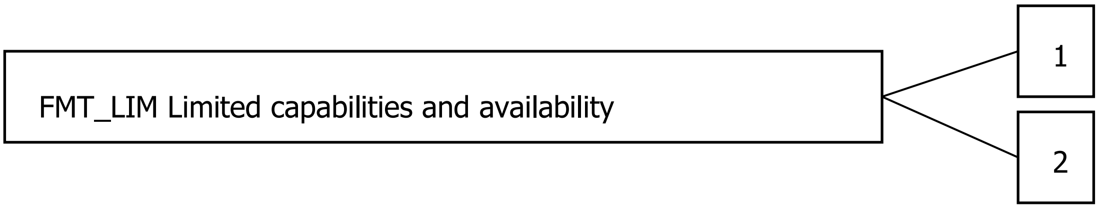
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

**FMT_LIM Limited capabilities and availability**

Family behavior

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

Component leveling:



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

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

Management: FMT_LIM.1, FMT_LIM.2
There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2
There are no actions defined to be auditable.

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

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

**FMT_LIM.1 Limited capabilities**

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

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

The TOE Functional Requirement "Limited availability (FMT_LIM.2)" is specified as follows.
FMT_LIM.2 Limited availability
Hierarchical to: No other components
Dependencies: FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: Limited capability and availability policy].
**Application note**: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that
(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced or conversely
(ii) the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

## 5.5. DEFINITION OF THE FAMILY FPT_EMS

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

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

Family behavior
This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMSEC.1 TOE emanation has two constituents:

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

FPT_EMSEC.1.2 Interface Emanation requires to not emit interface emanation enabling

access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

**FPT_EMSEC.1 TOE Emanation**

Hierarchical to: No other components

Dependencies: No dependencies.

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

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

# 6. Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 [CC] of the CC. Each of these operations is used in this ST.

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

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

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

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

**The definition of the subjects** "Manufacturer", "Personalization Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in chapter 8 or in the following table. The operations "write", "modify", "read" and

" disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and " re-authenticate" are originally . The operation "load" is synonymous to "import" used .

Definition of security attributes:

| Security attribute | value | meaning |
|---|---|---|
| Terminal authentication status | none (any Terminal) | default role (i.e. without authorization after start-up) |
| | Basic Inspection System | terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2. |
| | Personalization Agent | Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2. |

## 6.1. Security Functional Requirements for the TOE

### 6.1.1 Class FAU Security Audit

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

**FAU_SAS.1 Audit storage**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application Note: The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the

MRTD's chip (see FMT_MTD.1/INI_DIS).

### 6.1.2 Class Cryptographic Support (FCS)

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 keys to be generated by the TOE.

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

Hierarchical to: No other components.

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

FCS_CKM.1.1/Session

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Document Basic Access Key Derivation Algorithm* and specified cryptographic key sizes *112 bit* that meet the following: [*ICAO DOC 9303], normative appendix 5*

Note: 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 [ICAO Doc 9303], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO Doc 9303], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)".

**FCS_CKM.4 Cryptographic key destruction**

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion of key value by overwriting with zero* that meets the following: *none.*

Note: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

**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 Cryptographic operation – Hash for Key Derivation**

Hierarchical to: No other components.

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

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

**FCS_COP.1/ENC Cryptographic operation – Encryption / Decryption Triple DES**

Hierarchical to: No other components.

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

FCS_COP.1.1/ENC The TSF shall perform Secure Messaging (BAC) - *encryption and decryption* in accordance with a specified cryptographic algorithm *Triple-DES in CBC mode* and cryptographic key size *112 bit* that meet the following: *FIPS 46-3 and [ICAO Doc 9303] volume 2, normative appendix 5, A5.3.*

Note: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control

Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

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

Hierarchical to: No other components.

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

FCS_COP.1.1/AUTH The TSF shall perform symmetric authentication - *encryption and decryption* in accordance with a specified cryptographic algorithm <*Triple-DES*> and cryptographic key sizes <*112*> *bit* that meet the following: *<FIPS 46-3 >*

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

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

Hierarchical to: No other components.

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

FCS_COP.1.1/MAC

The TSF shall perform Secure Messaging - *message authentication code* in accordance with a specified cryptographic algorithm *Retail MAC* and cryptographic key sizes *112 bit* that meet the following:*ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2), in section 7.2.*

Note: 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 and FIA_UAU.4.

**FCS_COP.1/AA Active Authentication**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AA
The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm Table 4 algorithm and cryptographic key sizes Table 4 Key size that meet the following: Table 4 List of standards.

| Algorithm | Key size | Algorithms and key sizes |
|---|---|---|
| RSA | 2048 | ISO9796-2 |

Application note:
The dependency of FCS_COP.1/AA on FCS_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.

**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 Quality metric for random numbers**
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet *class P2 defined in [AIS31].*
Note: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

### 6.1.3 Class FIA Identification and Authentication

Note: Table 6.1 provides an overview on the authentication mechanisms used.

| Name | SFR for the TOE | Algorithms and key sizes |
|---|---|---|
| Basic Access Control Authentication Mechanism | FIA_AFL.1,<br>FIA_UAU.4,<br>FIA_UAU.6 | Triple-DES, 112 bit keys;<br>Retail-MAC, 112 bit keys |

| | | |
|---|---|---|
| Symmetric Authentication Mechanism for Personalization | FIA_UAU.4, | Triple-DES, 112 bit keys |

Table 6.1: 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.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow
1. to read the Initialization Data in Phase 2 "Manufacturing"
2. to read the random identifier in Phase 3 "Personalization of the MRTD"
3. to read the random identifier in Phase 4 "*Operational Use"*
on behalf of the user to be performed before the user is identified.

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

Note: 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 creates the user role Personalization 2 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. 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.

Note: In the "Operational Use" phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD's chip use a randomly chosen identifier for the communication channel to allow the terminal to communicate with more then one RFID. This identifier 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.
Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow
1. to read the Initialization Data in Phase 2 "Manufacturing"
2. to read the random identifier in Phase 3 "Personalization of the MRTD"
3. to read the random identifier in Phase 4 "*Operational Use*"
on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Note: The Basic Inspection System and the Personalization Agent authenticate themselves.

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

**FIA_UAU.4 Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to
1. Basic Access Control Authentication Mechanism
2. Authentication Mechanism based on *<Triple-DES>*

Note: The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.

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

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.
Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide
1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on *<Triple-DES>*
to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:
1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms *<the Symmetric Authentication Mechanism with 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*

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

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

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism*.*

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.6)" as specified below (Common Criteria Part 2 ).

**FIA_AFL.1 Authentication failure handling**

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

FIA_AFL.1.1 The TSF shall detect when *<1>* unsuccessful authentication attempt occurs related to BAC authentication

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall <*accumulates the delay time*>*.*

**FIA_API.1/AA Authentication Proof of Identity – Active Authentication**

Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_API.1.1/AA The TSF shall provide an *Active Authentication Protocol according to [MRTD]* to prove the identity of the *TOE.*

**6.1.4 Class FDP User Data Protection**

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

**FDP_ACC.1 Subset access control**

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the *Basic Access Control SFP* on terminals gaining write, read and modification access to data in the *EF.COM,EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD*.

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

**FDP_ACF.1 Security attribute based access control**
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

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

1. Subjects:
   (a) Personalization Agent
   (b) Basic Inspection System
   (c) Terminal
2. Objects:
   (a) data EF.DG1 to EF.DG16 of the logical MRTD
   (b) data in EF.COM
   (c) data in EF.SOD
3. Security attributes:
   (a) *authentication status of terminals*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation
among controlled subjects and controlled objects is allowed:

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD,EF.DG1 to EF.DG16 of the logical MRTD
2. the successfully authenticated Basic Inspection System is allowed to read the data in *EF.COM, EF.SOD, EF.DG1,EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD and perform Active Authentication.*

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

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

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

**Inter-TSF-Transfer**

Note: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of 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 ).

**FDP_UCT.1 Basic data exchange confidentiality – MRTD**

Hierarchical to: No other components.

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

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

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

**FDP_UIT.1 Data exchange integrity – MRTD**

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel or
FTP_TRP.1 Trusted path]

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

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

### 6.1.5 Class FMT Security Management

Note: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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.
Dependencies: No Dependencies

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

1. Initialization
2. Pre-personalization
3. *Personalization*

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.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles:

1. Manufacturer
2. Personalization Agent
3. *Basic Inspection System*

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

Note: 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.
Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow

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

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.
Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availabilities 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
4. Substantial information about construction of TSF to be gathered which may enable other attacks

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 Prepersonalization Data**

Hierarchical to: No other components.

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

FMT_MTD.1.1/INI_ENA

The TSF shall restrict the ability to *<write>* the *Initialization Data* and *Pre-personalization Data* to the *Manufacturer*

Note: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric ryptographic Personalization Agent 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.

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

FMT_MTD.1.1/INI_DIS

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

Note: According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer.

The TOE restricts the ability to write the Initialization Data and the Prepersonalization 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 writes the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access will be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

**FMT_MTD.1/AAPK Management of TSF data – Active Authentication Private Key**

Hierarchical to: No other components.

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

FMT_MTD.1.1/AAPK

The TSF shall restrict the ability to <*load>* the *Active Authentication Private Key* to the *Personalization Agent*

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_WRITE

The TSF shall restrict the ability to <*write>* the *Document Basic Access Keys and the Active Authentication Keys* to the *Personalization Agent*

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_READ

The TSF shall restrict the ability to *<read>* the *Document Basic Access Keys, the Active Authentication Private key* and *Personalization Agent Keys* to *none*

Note: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

### 6.1.6 Class FPT Protection of Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSF testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFR "Non-bypassability of the TSP (FPT RVM.1)" and "TSF domain separation (FPT SEP.1)" together with "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)" prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.
The TOE shall meet the requirement "TOE Emanation (FPT_EMSEC.1)" as specified below (Common Criteria Part 2 extended).

**FPT_EMSEC.1 TOE Emanation**
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_EMSEC.1.1
The TOE shall not emit *information about IC power consumption* in excess of *non-useful information* enabling access to *Personalization Agent Key*, *transport key*, *AA Private Key.*

FPT_EMSEC.1.2
The TSF shall ensure *any unauthorized users* are unable to use the following interface *smart card circuit contacts* to gain access to *Personalization Agent Key , transport key, AA Private Key.*

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.

Dependencies: No dependencies.

FPT_FLS.1.1

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

1. Exposure to out-of-range operating conditions where therefore a malfunction could occur
2. failure detected by TSF according to *FPT_TST.1*

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.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests <during initial start-up> to demonstrate the correct operation of the TSF.

FPT_TST.1.2 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.

Note: If the MRTD's chip uses state of the art smart card technology it will run the some self tests at the request of the authorized user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 is executed

during initial start-up by the "authorized user" Manufacturer in the Phase 2 "Manufacturing".

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.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *physical manipulation* *and physical probing* to *the TSF* by responding automatically such that the SFRs are always enforced.

Note: 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.

| | 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 | OT.AA_Proof |
|---|---|---|---|---|---|---|---|---|---|
| FAU_SAS.1 | | | | x | | | | | |
| FCS_CKM.1 | x | x | x | | | | | | |
| FCS_CKM.4 | x | | x | | | | | | |
| FCS_COP.1/SHA | x | x | x | | | | | | |
| FCS_COP.1/ENC | x | x | x | | | | | | |
| FCS_COP.1/AUTH | x | x | | | | | | | |
| FCS_COP.1/MAC | x | x | x | | | | | | |
| FCS_COP.1/AA | | | | | | | | | x |
| FCS_RND.1 | x | x | x | | | | | | |
| FIA_UID.1 | | | x | x | | | | | |
| FIA_AFL.1 | | | x | x | | | | | |
| FIA_UAU.1 | | | x | x | | | | | |
| FIA_UAU.4 | x | x | x | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| FIA_UAU.5 | x | x | x | | | | | | |
| FIA_UAU.6 | x | x | x | | | | | | |
| FIA_API.1/AA | | | | | | | | | x |
| FDP_ACC.1 | x | x | x | | | | | | |
| FDP_ACF.1 | x | x | x | | | | | | |
| FDP_UCT.1 | x | x | x | | | | | | |
| FDP_UIT.1 | x | x | x | | | | | | |
| FMT_SMF.1 | x | x | x | | | | | | |
| FMT_SMR.1 | x | x | x | | | | | | |
| FMT_LIM.1 | | | | | | | | x | |
| FMT_LIM.2 | | | | | | | | x | |
| FMT_MTD.1/INI_ENA | | | | x | | | | | |
| FMT_MTD.1/INI_DIS | | | | x | | | | | |
| FMT_MTD.1/AAPK | | x | | | | | | | x |
| FMT_MTD.1/KEY_WRITE | x | x | x | | | | | | |
| FMT_MTD.1/KEY_READ | x | x | x | | | | | | x |
| FPT_EMSEC.1 | x | | | | x | | | | |
| FPT_TST.1 | | | | | x | | x | | |
| FPT_FLS.1 | x | | | | x | | x | | |
| FPT_PHP.3 | x | | | | x | x | | | |

Coverage of Security Objectives for the TOE by SFR

## 6.2 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ALC_DVS.2

ATE_DPT.2

### 6.3 Security Requirements Rationale

### 6.3.1 Security Functional Requirements Rationale

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

The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

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

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

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

The security objective **OT.DATA_INT** "Integrity of personal data" requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: Only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD

(cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.
The security objective **OT.DATA_INT** "Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 require the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC MAC Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ. The SRF FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ requires that the Active Authentication Private Key cannot be written unauthorized or read afterwards.

The security objective **OT.Data_Conf** "Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

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

The security objective **OT.Identification** "Identification and Authentication of the TOE" address the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.
Furthermore, the TOE shall identify itself only to a successful authenticated 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 (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification.
The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

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

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

The security objective **OT.AA_Proof** "Proof of MRTD's chip authenticity through AA" addresses the verification of the chip's authenticity. This done by the SFR FIA_API.1/AA which authenticates the chip using cryptographic operations covered by the SFR FCS_COP/AA. The Active Authentication Protocol is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ.

### 6.3.2 Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied.

All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

Table shows the dependencies between the SFR of the TOE.

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|

| | | |
|---|---|---|
| FAU_SAS.1 | No dependencies | n.a. |
| FCS_CKM.1 | [FCS_CKM.2 Cryptographic key distribution or<br>FCS_COP.1 Cryptographic operation],<br>FCS_CKM.4 Cryptographic key destruction | Fulfilled by FCS_COP.1/ENC, and FCS_COP.1/MAC<br>Fulfilled by FCS_CMK.4 |
| FCS_CKM.4 | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] | Fulfilled by FCS_CKM.1 |
| FCS_COP.1/SHA | [FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | Justification 1 for non-satisfied dependencies,<br>Fulfilled by FCS_CKM.4 |
| FCS_COP.1/ENC | [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]<br>FCS_CKM.4 Cryptographic key destruction. | fulfilled by FCS_CKM.1<br>fulfilled by FCS_CKM.4 |
| FCS_COP.1/AUTH | [FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | Justification 2 for non-satisfied dependencies,<br>Justification 2 for non-satisfied dependencies |
| FCS_COP.1/AA | FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1],<br>FCS_CKM.4 | Justification 5 for non-satisfied dependencies |
| FCS_RND.1 | No dependencies | n.a |
| FIA_AFL.1 | FIA_UAU.1 Timing of authentication | fulfilled by FIA_UAU.1 |
| FIA_UID.1 | No dependencies | n.a. |

| | | |
|---|---|---|
| FIA_UAU.1 | FIA_UID.1 Timing of identification | Fulfilled by FIA_UID.1 |
| FIA_UAU.4/ | No dependencies | n.a. |
| FIA_UAU.5 | No dependencies | n.a. |
| FIA_UAU.6 | No dependencies | n.a. |
| FIA_API.1/AA | No dependencies | |
| FDP_ACC.1 | FDP_ACF.1 Security attribute based access control | Fulfilled by FDP_ACF.1 |
| FDP_ACF.1 | FDP_ACC.1 Subset access control,<br>FMT_MSA.3 Static attribute initialization | Fulfilled by FDP_ACC.1, justification 3 for non-satisfied dependencies |
| FDP_UCT.1 | [FTP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path]<br>[FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control] | Justification 4 for non-satisfied dependencies<br>Fulfilled by FDP_ACC.1 |
| FDP_UIT.1 | [FTP ITC.1 Inter-TSF trusted channel,or<br>FTP TRP.1 Trusted path]<br>[FDP_ACC.1 Subset access control, or<br>FDP IFC.1 Subset information flow control] | Justification 4 for non-satisfied dependencies<br>Fulfilled by FDP_ACC.1 |
| FMT_SMF.1 | No dependencies | n.a. |
| FMT_SMR.1 | FIA_UID.1 Timing of identification | Fulfilled by FIA_UID.1 |
| FMT_LIM.1 | FMT_LIM.2 | Fulfilled by FMT_LIM.2 |
| FMT_LIM.2 | FMT_LIM.1 | Fulfilled by FMT_LIM.1 |
| FMT_MTD.1/INI_ENA | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/INI_DIS | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/KEY_READ | FMT_SMF.1 Specification of management functions<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1/ |
| FMT_MTD.1/KEY_WRITE | FMT_SMF.1 Specification of management functions<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1/ |
| FMT_MTD.1/AAPK | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1/ |
| FPT_EMESEC.1 | No dependencies | n.a. |
| FPT_FLS.1 | No dependencies | n.a. |
| FPT_PHP.3 | No dependencies | n.a. |

| | | |
|---|---|---|
| FPT_TST.1 | No dependencies | n.a. |

**Table 1 Dependencies between the SFR for the TOE**

Justification for non-satisfied dependencies between the SFR for TOE

No. 1 The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1 nor an import (FDP_ITC.1/2) is necessary.

No. 2 The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE life cycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

No. 3 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.3) is necessary here.

No. 4 The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS respectively GIS. There is no need for the SFR FTP ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP TRP.1 is not applicable here.

No. 5 The SFR FCS_COP.1/AA uses the asymmetric Key permanently stored during the Personalization process. Since the key is permanently stored within the TOE there is no need for FCS_CKM.1 and FCS_CKM.4.

### 6.3.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

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. And the component ATE_DPT.2 is augmented to meet the assurance level of [BAC-PP-0055] based on CC v3.1 Revision 2.
The component ALC_DVS.2 has no dependencies.
All of these are met or exceeded in the EAL4 assurance package.

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

The analysis of the TOE's security requirements with regard to their mutual support and internal consistency demonstrates: The dependency analysis in section 6.3.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.
The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the additional assurance in section 6.3.3 Security Assurance Requirements Rationale components shows that the assurance requirements are mutually supportive and internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.
Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.3.2 Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

# 7. TOE Summary Specification

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

## 7.1. TOE security functions by the software

| SF | Description |
|---|---|
| SF_READ_ACC | Data access control |
| SF_BAC | BASIC ACCESS CONTROL |
| SF_AUTH | Authentication |
| SF_SM | Data Secure Messaging |
| SF_WIRTE_MGT | Write Management |
| SF_CRYPTO | Cryptographic operation |
| SF_PROTECTION | Counter Measure by IC Chip |
| SF_AA | Active Authentication |

TOE Security Fuction

## 7.2. TOE security functions by IC Chip

### 7.2.1. IC chip SFR

| SF | Description |
|---|---|
| SF_DPM | Device phase management |
| SF_PS | Protection against snooping |
| SF_PMA | Protection against modifying attacks |
| SF_PLA | Protection against logical attacks |
| SF_CS | Cryptographic support (3DES, AES, RSA, EC, SHA-2,TRNG) |

Security Function provided by IC Chip

These SF are described in [ICST].

**SF_DPM**

:Device Phase Management

The life cycle of the IC chip TOE is split-up in several phases. Chip development and production (phase 2, 3, 4) and final use (phase 4-7) is a rough split-up from IC chip TOE point of view. These phases are implemented in the IC chip TOE as test mode (phase 3) and user mode (phase 4-7). In addition a chip identification mode exists which is active in all phases. The chip identification data (O.Identification) is stored in a in the not changeable configuration page area and non-volatile memory. In the same area further IC chip TOE configuration data is stored. In addition, user initialization data can be stored in the non-volatile memory during the production phase as well. During this first data programming, the TOE is still in the secure environment and in Test Mode.

**SF_PS**

:Protection against Snooping

All contents of all memories of the IC chip TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. There is no plain data on the chip. In addition the data transferred over the busses, the SFRs and the peripheral devices (CRC, RNG and Timer) are encrypted as well.

The memory content and bus encryption is done by the MED using a complex key management and by the memories, RAM, CACHE and the bus are entirely encrypted.

Therefore, no data in plain are handled anywhere on the IC chip and thus also the two CPUs compute entirely masked. The symmetric cryptographic co-processor is entirely masked as well.

**SF_PMA**

: Protection against Modifying Attacks

The IC chip TOE is equipped with an error detection code (EDC) which covers the memory system of RAM, ROM and EEPROM and includes also the MED, MMU and the bus system. Thus introduced failures are detected and in certain errors are also automatically corrected. In order to prevent accidental bit faults during production in the ROM, over the data stored in ROM an EDC value is calculated.

**SF_PLA**

: Protection against Logical Attacks

The memory access control of the IC chip TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of the privileged levels and gives the software the possibility to define different access rights. The address permissions of the privilege levels are controlled by the MMU. In case of an access violation the MMU will trigger a reset and then a trap service routine can react on the access violation. The policy of setting up the MMU and specifying the memory ranges, to a certain extend, for the privilege levels . with the exception of the IFX level - is defined from the user software (OS).

**SF_CS**

: Cryptographic Support

The IC chip TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic operations. This security function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function respectively mathematic algorithm itself is not used from the IC chip TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The components are a co-processor supporting the DES and AES algorithms and a combination of a co-processor and software modules to support RSA cryptography, RSA key generation, ECDSA signature generation and verification, ECDH key agreement and EC public key calculation and public key testing.

# 8. Glossary and Acronyms

| Term | Definition |
|---|---|
| *Active Authentication* | Security mechanism defined in [ICAO DOC 9303] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization |
| *Application note* | Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE. |
| *Audit records* | Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data. |
| *Authenticity* | Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization |
| *Basic Access Control (BAC)* | Security mechanism by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there) |
| *Basic Inspection System (BIS)* | An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD. |
| *Biographical data (biodata).* | The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa |
| *biometric reference data* | Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data. |

| | |
|---|---|
| *Counterfeit* | An unauthorized copy or reproduction of a genuine security document made by whatever means. |
| *Country Signing CA*<br>*Certificate ($C_{CSCA}$)* | Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system. |
| *Document Basic*<br>*Access Keys* | Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book. |
| *Document Security*<br>*Object ($SO_D$)* | A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS) |
| *Eavesdropper* | A threat agent with Enhanced-Basic attack potential reading the<br>communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip. |
| *Enrolment* | The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity |
| *Extended Access*<br>*Control* | Security mechanism identified by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use. the same mechanism to authenticate themselves with Personalization Agent<br>Private Key and to get write and read access to the logical MRTD and TSF data. |
| *Extended Inspection* | A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference |

| | |
|---|---|
| *System (EIS)* | data and supports the terminals part of the Extended Access Control Authentication Mechanism. |
| *Forgery* | Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. |
| *Global*<br>*Interoperability* | The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the<br>standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. |
| *IC Dedicated*<br>*Support Software* | That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases. |
| *IC Dedicated Test*<br>*Software* | That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter. |
| *IC Identification*<br>*Data* | The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. |
| *Impostor* | A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. |
| *Improperly* | A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's |

| | |
|---|---|
| *documented person* | travel document or visa; or (d) no travel document or visa, if required. |
| *Initialisation* | Process of writing Initialisation Data (see below) to the TOE (cf. sec. 1.2, TOE life cycle, Phase 2, Step 3). |
| *Initialisation Data* | Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data). |
| *Inspection* | The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity |
| *Inspection system*<br>*(IS)* | A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. |
| *Integrated circuit*<br>*(IC)* | Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit. |
| *Integrity* | Ability to confirm the MRTD and its data elements on the MRTD's chip have<br>not been altered from that created by the issuing State or Organization |
| *Issuing Organization* | Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). |
| *Logical Data* | The collection of groupings of Data Elements stored in the optional capacity expansion technology. The capacity expansion technology used is the MRTD's chip. |

| | |
|---|---|
| *Structure (LDS)* | |
| *Logical MRTD* | Data of the MRTD holder stored according to the Logical Data Structure as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder<br>(2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),<br>(3) the digitized portraits (EF.DG2),<br>(4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and<br>(5) the other data according to LDS (EF.DG5 to EF.DG16).<br>(6) EF.COM and EF.SOD |
| *Logical travel*<br>*document* | Data stored according to the Logical Data Structure as specified by ICAO in<br>the contactless integrated circuit including (but not limited to)<br>(1) data contained in the machine-readable zone (mandatory),<br>(2) digitized photographic image (mandatory) and<br>(3) fingerprint image(s) and/or iris image(s) (optional). |
| *Machine readable*<br>*travel document*<br>*(MRTD)* | Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. |
| *MRTD application* | Non-executable data defining the functionality of the operating system on the<br>IC as the MRTD's chip. It includes<br>- the file structure implementing the LDS<br>- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14, EF.DG 16, EF.COM and EF.SOD) and<br>- the TSF Data including the definition the authentication data but except the authentication data itself. |

| | |
|---|---|
| *MRTD Basic Access Control* | Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS. |
| *MRTD's Chip* | A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO |

**Acronyms**

| **Acronyms** | **Term** |
|---|---|
| BIS | Basic Inspection System |
| BIS-PACE | Basic Inspection System with PACE |
| CA | Chip Authentication |
| CAN | Card Access Number |
| CC | Common Criteria |
| EAC | Extended Access Control |
| EF | Elementary File |
| ICCSN | Integrated Circuit Card Serial Number. |
| MF | Master File |
| MRZ | Machine readable zone |
| n.a. | Not applicable |
| OSP | Organizational security policy |
| PACE | Password Authenticated Connection Establishment |
| PCD | Proximity Coupling Device |
| PICC | Proximity Integrated Circuit Chip |
| PP | Protection Profile |
| PT | Personalization Terminal |
| RF | Radio Frequency |
| SAR | Security assurance requirements |
| SFR | Security functional requirement |
| SIP | Standard Inspection Procedure |
| TA | Terminal Authentication |

| | |
|---|---|
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy (defined by the current document) |