KONA2 D2320N ePassport EAC Security Target Lite

V01.02 (2016.05.21)

R&D Center

NOTE: This information must be used exclusively for the operation of KONA I programs. It may not be duplicated, published, or disclosed without KONA I’s written permission.

Revision History

KONA2 D2320N ePassport EAC Security Target Lite

No.	Ver.	Date	Description of Change	Chapter	Writer
1	V01.00	2015/10/16	New Publication	All	KONA I
2	V01.01	2016/04/29	Correct issues during CB validation, update ST issues	1, 2, 6, 7, 8, 10	KONA I
3	V01.02	2016/05/21	Update TOE version	1	KONA I

2016. 05, 21. 3th Release

NOTE: This information must be used exclusively for the operation of KONA I programs. It may not be duplicated, published, or disclosed without KONA I's written permission.

Table of Contents

1. ST Introduction

1.1. ST Reference

Document No:	SP-06-22
Document Title:	KONA2 D2320N ePassport EAC Security Target Lite
Version:	1
Revision:	2
Release date:	2016-05-21

Table 1. ST Reference

1.2. TOE Reference

Name:	KONA2 D2320N ePassport [EAC configuration]
Version:	01
Revision:	03
Update (patch)	00

Table 2. TOE Reference

1.3. TOE Overview

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) [5] and providing the Basic Access Control and Extended Access Control according to the 'ICAO Doc 9303' [ICAO] and BSI TR-03110 [TR-03], respectively.

The TOE is composed of:

- the circuitry of the MRTD's chip (16-Bit RISC Microcontroller for Smart Cards, S3FT9MG rev 0)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system KONA2 D2320N ePassport V01.03.00),
- the associated guidance documentation.

It provides the security level of EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

The TOE type of the current security target is "the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Extended Access Control", compatible with the expected TOE type described in the PP.

2. TOE Description

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 the Basic Access Control, the Active Authentication and the Extended Access Control according to 'ICAO Doc 9303' [ICAO] and BSI TR-03110 [TR-03], respectively.

The TOE comprises of:

- the circuitry of the MRTD's chip (16-Bit RISC Microcontroller for Smart Cards, S3FT9MG rev 0)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (KONA2 D2320N ePassport V01.03.00),
- the associated guidance documentation.

TOE usage and security features for operational use:

A State or Organization issues MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of:

1) 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:
    a. the biographical data on the biographical data page of the passport book,
    b. the printed data in the Machine-Readable Zone (MRZ) and
    c. the printed portrait.
2) The **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [ICAO] 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:
    a. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
    b. the digitized portraits (EF.DG2),
    c. the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
    d. the other data according to LDS (EF.DG5 to EF.DG16) and
    e. 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) [ICAO]. These security measures include the binding of the MRTD’s chip to the passport book.

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

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

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This security target addresses the Chip Authentication described in [TR-03] as an alternative to the Active Authentication stated in [ICAO].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this security target as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfill the ‘Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control’ [PPBAC]. Due to the fact that [PPBAC] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately. The evaluation and certification process might have taken place in advance or could – more likely –be carried out simultaneously to the current process according the PP in hand.

For BAC, 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], normative appendix 5.

The security target requires the TOE to implement the Chip Authentication defined in [TR-03]. The Chip Authentication prevents data traces described in [ICAO], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD’s Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD’s chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The security target requires the TOE to implement the Extended Access Control as defined in [TR-03]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol and (ii) the Terminal Authentication Protocol. The Chip Authentication Protocol (i) authenticates the MRTD's chip to the inspection system and (ii) establishes secure messaging, which is used by Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication can only be performed if Chip Authentication has been successfully executed. The Terminal Authentication Protocol consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

TOE life cycle:

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

Phase 1 "Development"

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

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

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile programmable memories (FLASH) 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"

(Step3) In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile programmable memories (FLASH). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance FLASH).

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

(Step5) 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.

Phase 3 "Personalization of the MRTD"

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

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

Phase 4 "Operational Use"

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

(See the Protection profile for applicable application notes: 1, 2, 3, 4 and 5)

2.1. TOE Architecture

The TOE is a composition of IC hardware and embedded software that controls the IC.

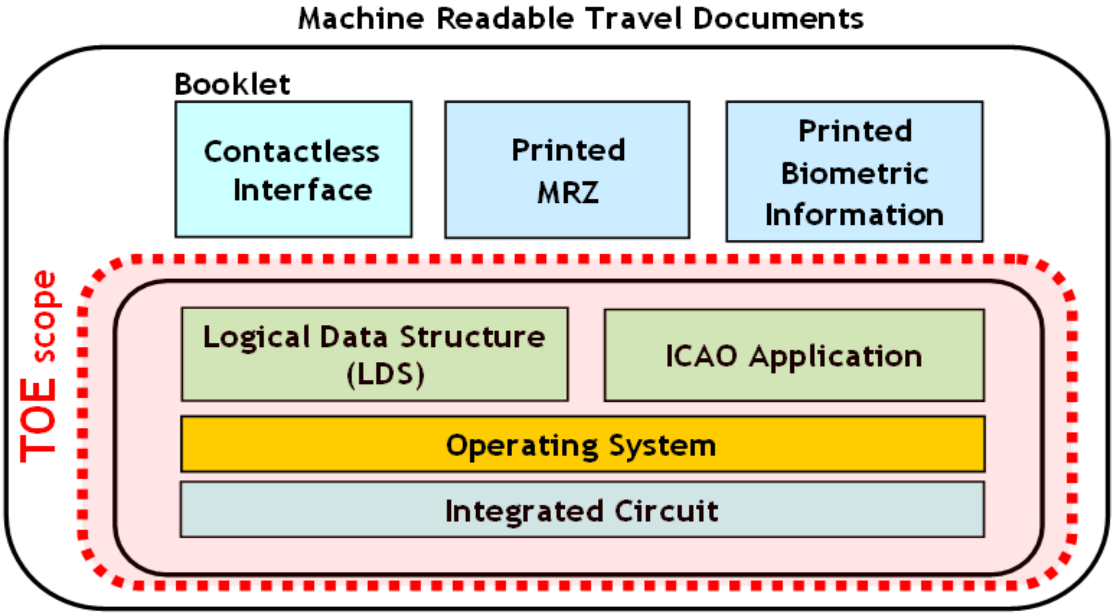

Figure 1. TOE Scope

The TOE is defined to comprise the chip and the hardware abstraction layer 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.

2.1.1. TOE guidance

The guidance documentation consists of the:

- [GU] this guide is delivered to the card holder (card holder or receiving state)
- [GP] this guide is delivered to the personalization agent (issuing state)
- [GA] this guide is only used by KONA I internally.
- [DEL] this guide is used by all the entities to deliver the TOE between them.

3. Conformance Claim

This security target claims the following conformance with Common Criteria:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012 conformant.

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012 extended conformance with FAU_SAS.1, FCS_RND.1, FIA_API.1, FMT_LIM.1, FMT_LIM.2 and FPT_EMSEC.1 (defined in the chapter 6. *Extended component definition*).

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 4, September 2012 conformant.

This security target claims the following conformance with protection profiles:

- A strict conformance with Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control version 1.10, 25th March 2009.

This security target and the TOE claim conformity with EAL5+, augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis)

3.1. Conformance Claim Rationale

The security target and the TOE are conformant with CC version 3.1 Release 4 and the protection profile with CC version 3.1 Release 1 for Part 1 and Release 2 for Part 2 and Part 3. The following statements show the non-incompatibility between both:

- The differences between part 1 of CC version 3.1 in Release 1 and Release 4 are only in definitions and in identification of glossary, therefore it is not relevant.
- The differences between part 2 of CC version 3.1 in Release 2 and Release 4 applicable in the definition of some SFRs. Some of them are refined for aligning the SFR with the whole definition of the TOE. The following list shows the SFR that suffered changes:
    - FAU_SAR.1, description of components
    - FAU_SEL.1.1, requirements modification
    - FDP_ACF.1.4, requirements modification Information flow control functions (FDP_IFF), family behaviour
    - FDP_UCT.1.1, requirements modification
    - FDP_UIT.1.1, requirements modification
    - TSF self-test (FPT_TST), requirements modification, because in the PP conformant with Revision 2, the requirements of FPT_TST.1.3 applies to TSF executable code, while in Revision 3, it applies TSF or parts of TSF. Our selection covers all the TSF

- The differences between part 3 of CC version 3.1 in Release 2 and Release 4 applicable in the definition of some SAR.
    - Definition of EAL4 reducing the ATE_DPT from 2 to 1

  - Definition of EAL6 level
  - APE class definitions
  - Refinement of the definition of TSFI meaning
  - Suppression of ADV_SPM.1.5C
  - Mandatory providing of the delivery documentation, Development site security, flaw remediation and documentation of tools and techniques
  - Renaming terms of architectural design for security architecture description.
  - Module definition regarding implementation of SFR.

These differences don't affects to the compatibility between TOE conformant with CC v3.1 Revision 4 and PP conformant with CC v3.1 Revision 1 and Revision 2. The difference in the SFR is identified in the current ST.

This security target doesn’t introduce any additional threat, organization security policy or assumption, objectives for the TOE or environment to the PP. Only uses the iteration operation over several SFR to differentiate features over the same requirements, being:

- FCS_COP.1/SIG_VER (DSA verification with EC)
- FCS_COP.1/SHA
- FCS_COP.1/SYM
- FCS_COP.1/MAC
- FMT_MTD.1/INI_ENA
- FMT_MTD.1/INI_DIS
- FMT_MTD.1/CVCA_INI
- FMT_MTD.1/CVCA_UPD
- FMT_MTD.1/DATE
- FMT_MTD.1/KEY_WRITE
- FMT_MTD.1/CAPK
- FMT_MTD.1/KEY_READ

This security target claims conformity with EAL5 extending the EAL4 from the PP. The differences in the assurance components do not reduce the EAL, indeed enforce some requirements based on module testing and semiformal description of the development parts

- ADV_FSP.4 passes to ADV_FSP.5 (semiformal description of interfaces)
- ADV_TDS.3 passes to ADV_TDS.4 (modules description)
- ALC_CMS.4 passes to ALC_CMS.5 (including tools in the CM list)
- ALC_TAT.1 passes to ALC_TAT.2 (implementation based on Standards)
- ATE_DPT.1 passes to ADV_DPT.3 (testing at module level)
- Adding the component ADV_INT.2 (well-structure internals description)
- AVA_VAN.3 passes to AVA_VAN.4, however the PP and this ST claims for AVA_VAN.5.

The developer uses the EAL5+ for providing more assurance to their customers.

The TOE type of the current security target is " the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) and providing the Extended Access Control ", compatible with the expected TOE type described in the PP.

4. Security Problem Definition

4.1. Introduction

Assets

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

Logical MRTD 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 traveller to prove his possession of a genuine MRTD.

Subjects

This security target considers the following subjects:

Manufacturer

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

Personalization Agent

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

Country Verifying Certification Authority

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

Document Verifier

The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.

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 traveller and verifying its authenticity and (ii) verifying the traveller 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.

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

Attacker
A threat agent trying (i) to manipulate the logical MRTD without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or (iii) to forge a genuine MRTD.

4.2. Assumptions

4.2.1. A.MRTD_Manufact MRTD manufacturing on step 4 to 6

This assumption is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 60).

4.2.2. A.MRTD_Delivery MRTD delivery during steps 4 to 6

This assumption is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 61).

4.2.3. A.Pers_Agent Personalization of the MRTD's chip

This assumption is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 62).

4.2.4. A.Insp_Sys Inspection Systems for global interoperability

This assumption is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 63).

4.2.5. A.Signature_PKI PKI for Passive Authentication

This assumption is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 64).

4.2.6. A.Auth_PKI PKI for Inspection Systems

This assumption is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 65).

4.3. Threats

4.3.1. T.Read_Sensitive_Data Read the sensitive biometric reference data

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 68).

4.3.2. T.Forgery Forgery of data on MRTD’s chip

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 69).

4.3.3. T.Counterfeit MRTD’s chip

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 70).

4.3.4. T.Abuse-Func Abuse of Functionality

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 72).

4.3.5. T.Information_Leakage Information Leakage from MRTD’s chip

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 73).

4.3.6. T.Phys-Tamper Physical Tampering

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 74).

4.3.7. T.Malfunction Malfunction due to Environmental Stress

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 75).

4.4. Organizational Security Policies

4.4.1. P.BAC-PP Fulfillment of the Basic Access Control Protection Profile

This security policy is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 77).

4.4.2. P.Sensitive_Data Privacy of sensitive biometric reference data

This security policy is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 78).

4.4.3. P.Manufact Manufacturing of the MRTD’s chip

This security policy is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 79).

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

This security policy is included in the ST and it is described in the MRTD, “ICAO Application'', Extended Access Control PP (paragraph 80).

5. 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.

5.1. Security Objectives for the TOE

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

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 83).

5.1.2. OT.Data_Int Integrity of personal data

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 85).

5.1.3. OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 86).

5.1.4. OT.Identification Identification and Authentication of the TOE

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 87).

5.1.5. OT.Chip_Auth_Proof Proof of MRTD’s chip authenticity

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 88).

5.1.6. OT.Prot_Abuse-Func Protection against Abuse of Functionality

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 91).

5.1.7. OT.Prot_Inf_Leak Protection against Information Leakage

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 92).

5.1.8. OT.Prot_Phys-Tamper Protection against Physical Tampering

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 94).

5.1.9. OT.Prot_Malfunction Protection against Malfunctions

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 95).

5.2. Security Objectives for the Operational Environment

5.2.1. OE.MRTD_Manufact Protection of the MRTD Manufacturing

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 98).

5.2.2. OE.MRTD_ Delivery Protection of the MRTD delivery

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 99).

5.2.3. OE.Personalization Personalization of logical MRTD

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 100).

5.2.4. OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 101).

5.2.5. OE.Auth_Key_MRTD MRTD Authentication Key

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 102).

5.2.6. OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 103).

5.2.7. OE.BAC_PP Fulfillment of the Basic Access Control Protection Profile

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 104)

5.2.8. OE.Exam_MRTD Examination of the MRTD passport book

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 106)

5.2.9. OE.Passive_Auth_Verif Verification by Passive Authentication

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 107).

5.2.10. OE.Prot_Logical_MRTD Protection of data from the logical MRTD

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 108).

5.2.11. OE.Ext_Insp_Systems Authorization of Extended Inspection Systems

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 110).

5.3. Security Objectives Rationale

The following table provides an overview for security objectives coverage:

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.BAC-PP	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_Systems
T.Read_Sensitive_Data			X												X					X
T.Forgery	X	X						X					X				X	X		
T.Counterfeit					X									X			X			
T.Abuse-Func						X														
T.Information_Leakage							X													
T.Phys-Tamper								X												
T.Malfunction									X											
P.BAC-PP																X				
P.Sensitive_Data			X												X					X
P.Manufact				X																
P.Personalization	X			X								X								
A.MRTD_Manufact										X										
A.MRTD_Delivery											X									
A.Pers_Agent												X								
A.Insp_Sys																	X		X	
A.Signature_PKI													X				X			
A.Auth_PKI															X					X

Table 3. Coverage table between SPD and Objectives

The OSP **P. BAC-PP** is directly addressed by the **OE.BAC-PP**.

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 enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD”, and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD”. Note the manufacturer equips the TOE with the Personalization Agent 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.Sensitive_Data** “Privacy of sensitive biometric reference data” is fulfilled and the threat **T.Read_Sensitive_Data** “Read the sensitive biometric reference data” is countered by the TOE-objective **OT.Sens_Data_Conf** “Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems".

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

The threat **T.Counterfeit** "MRTD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of MRTD's chip authentication" using an authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_MRTD** "MRTD Authentication Key". According to **OE.Exam_MRTD** "Examination of the MRTD passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip.

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.

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 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 enrolment, 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” which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD’s chip. 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.Signature_PKI** “PKI for Passive Authentication” is directly covered by the security objective for the TOE environment **OE.Pass_Auth_Sign** “Authentication of logical MRTD by Signature” covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_MRTD** “Examination of the MRTD passport book”.

The assumption **A.Auth_PKI** “PKI for Inspection Systems” is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** “Authorization for use of sensitive biometric reference data” requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organizations only. The Document Verifier of the receiving State is required by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems” to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organization has to establish the necessary public key infrastructure.

6. Extended Components Definition

This security target uses components defined as extensions to CC part 2. Some of these components are extracted from defined in (PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001.

6.1. Definition of Family FAU_SAS

This family and components (FAU_SAS.1) of security functional requirements are included and described in the MRTD, "ICAO Application", Extended Access Control PP (section 5.1).

6.2. Definition of Family FCS_RND

This family and components (FCS_RND.1) of security functional requirements are included and described in the MRTD, "ICAO Application", Extended Access Control PP (section 5.2).

6.3. Definition of Family FIA_API

This family and components (FIA_API.1) of security functional requirements are included and described in the MRTD, "ICAO Application", Extended Access Control PP (section 5.3).

6.4. Definition of Family FMT_LIM

This family and components (FMT_LIM.1 and FMT_LIM.2) of security functional requirements are included and described in the MRTD, "ICAO Application", Extended Access Control PP (section 5.4).

6.5. Definition of Family FPT_EMSEC

This family and components (FPT_EMSEC.1) of security functional requirements are included and described in the MRTD, "ICAO Application", Extended Access Control PP (section 5.5).

7. Security Requirements

This chapter describes the security requirements for the TOE, considering this notation for the operation for SFR:

- Assignment: value defined between square-bracket and italic; e.g.: [assignment: *values*]
- Selection: value defined between square-bracket and italic; e.g.: [selection: *values*]
- Iteration: denoted with / separator and component identifier; e.g.: FCS_COP.1/SHA
- Refinement: denoted as bold text; e.g.: **Content**

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 4.1. Note that all these subjects are acting for homonymous external entities. All used objects are defined either in this section 7 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 taken from Common Criteria 3.1 R4 Part 2. The operation "load" is synonymous to "import" used in Common Criteria 3.1 R4 Part 2.

Definition of security attributes:

security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR-03], A.5.1); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA
	DV (domestic)	roles defined in the certificate used for authentication (cf. [TR-03], A.5.1); Terminal is authenticated as domestic Document Verifier after successful CA and TA
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR-03], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA and TA
	IS	roles defined in the certificate used for authentication (cf. [TR-03], A.5.1); Terminal is authenticated as Extended Inspection System after successful CA and TA
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [TR-03], A.5.1)
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR-03], A.5.1)
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [TR-03], A.5.1)

Table 4. Security Attributes

The following table provides an overview of the keys and certificates used:

Name	Data

Country Verifying Certification Authority Private Key (SKCVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SKCVCA) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PKCVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PKCVCA) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (CCVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [TR-03] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PKCVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (CDV)	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PKDV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (CIS)	The Inspection System Certificate (CIS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PKIS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Active Authentication Key Public Key Pair	The Active Authentication Public Key Pair (SKAA, PKAA) are used for Active Authentication.
Active Authentication Public Key (PKAA)	The Active Authentication Public Key (PKICC) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Active Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Active Authentication Private Key (SKAA)	The Active Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SKICC, PKICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PKICC)	The Chip Authentication Public Key (PKICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SKICC)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document

	Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

Table 5. Keys and Certificates

7.1. Security Functional Requirements for the TOE

This section describes the security functional requirements for the TOE.

7.1.1. 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.

7.1.2. 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 key to be generated by the TOE.

FCS_CKM.1 Cryptographic key generation – Elliptic Curve Diffie-Hellman Keys by the TOE

Hierarchical to:	No other components.
Dependencies	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: *ECDH compliant to ISO 15946*] and specified cryptographic key sizes [assignment: *192, 224 and 256 bit*] that meet the following: [TR-03 Annex A.1]

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

FCS_CKM.4 Cryptographic key destruction – MRTD

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *physically irreversible destruction of stored keys]* that meets the following: [assignment: *none*].

7.1.2.1. 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 [selection: *SHA-1, SHA-224, SHA-256*] and cryptographic key sizes none that meet the following: [selection: *FIPS 180-2*]

FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption

Hierarchical to: No other components.

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

FCS_COP.1.1/ SYM The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm [assignment: *Triple-DES with CBC mode*] and cryptographic key sizes [assignment: *112 bit*] that meet the following: 'TR-03110', [TR-03].

FCS_COP.1/MAC Cryptographic operation –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 [assignment: *Triple-DES with Retail-mode*] and cryptographic key sizes [assignment: *112 bit*] that meet the following: 'TR-03110', [TR-03].

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD

Hierarchical to: No other components.

Dependencies [[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ SIG_VER The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm [assignment: *ECDSA*] and cryptographic key sizes [assignment: *192, 224 and 256 bit*] that meet the following: [assignment: *ISO15946-2*].

7.1.2.2. 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 [assignment:

1. *Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.*
2. *The average Shannon entropy per internal random bit exceeds 0.997(7.976 bits per octet)*

}

7.1.3. Class FIA Identification and Authentication

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

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 establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
3. to identify themselves by selection of the authentication key
4. to carry out the Chip Authentication Protocol
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.

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.Terminal Authentication Protocol,
2. Authentication Mechanism based on [selection: *Triple-DES*].

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. Terminal Authentication Protocol,
2. Secure messaging in MAC-ENC mode,
3. Symmetric Authentication Mechanism based on [selection: *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 [selection: *the Symmetric Authentication Mechanism with Personalization Agent Key*].
2. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
3. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism.

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 after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.

The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1)” as specified below (Common Criteria Part 2 extended).

FIA_API.1 Authentication Proof of Identity

Hierarchical to:	No other components.
Dependencies	No dependencies.
FIA_API.1.1	The TSF shall provide a Chip Authentication Protocol according to [TR-03] to prove the identity of the TOE.

7.1.4. Class FDP User Data Protection

Subset access control (FDP_ACC.1)

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

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 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

Security attribute based access control (FDP_ACF.1)

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

FDP_ACF.1 Basic 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 Access Control SFP to objects based on the following:

1. Subjects:
   a. Personalization Agent,
   b. Extended Inspection System,
   c. Terminal,
2. Objects:
   a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
   b. data EF.DG3 and EF.DG4 of the logical MRTD
   c. data in EF.COM,
   d. data in EF.SOD,
3. Security attributes
   a. authentication status of terminals.
   b. Terminal Authorization.

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 Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD.

	3. the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD.
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rule: 1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG3, 2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4, 3. A terminal authenticated as DV is not allowed to read data in the EF.DG3, 4. A terminal authenticated as DV is not allowed to read data in the EF.DG4, 5. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD, 6. Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD

Inter-TSF-Transfer

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

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 Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure after Chip Authentication.

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

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 Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred after Chip Authentication.

7.1.5. Class FMT Security Management

The TOE shall meet the requirement “Specification of Management Functions

(FMT_SMF.1)” as specified below (Common Criteria Part 2).

FMT_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 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. Country Verifying Certification Authority,
4. Document Verifier,
5. domestic Extended Inspection System
6. foreign Extended Inspection System
FMT_SMR.1.2 The TSF shall be able to associate users with roles

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 manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. 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 availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow
1. User Data to be manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,

3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. 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 Prepersonalization Data to the Manufacturer.

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.

FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date

Hierarchical to: No other components.

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

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write the
1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date to [assignment: *Personalization Agent*].

FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifying Certification Authority

Hierarchical to: No other components.

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

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to update the
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate to Country Verifying Certification Authority.

FMT_MTD.1/DATE Management of TSF data – Current date

Hierarchical to: No other components.

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

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify the Current date to
1. Country Verifying Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System

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 to the Personalization Agent

FMT_MTD.1/CAPK Management of TSF data – Chip 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/CAPK	The TSF shall restrict the ability to [selection: *load*] the Chip Authentication Private Key to [assignment: *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 1. Document Basic Access Keys, 2. Chip Authentication Private Key, 3. Personalization Agent Keys to none

The TOE shall meet the requirement “Secure TSF data (FMT_MTD.3)” as specified below (Common Criteria Part 2)

FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components.
Dependencies	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1	The TSF shall ensure that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control

Refinement: The certificate chain is valid if and only if

(1) the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,

(2) the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

(3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

7.1.6. Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

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 [assignment: *electromagnetic field*] in excess of [assignment: *values that allows deduce sensitive information*] enabling access to Personalization Agent Key(s) and Chip Authentication Private Key and [assignment: *none*].

FPT_EMSEC.1.2 The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and Chip Authentication Private Key and [assignment: *none*].

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 [selection: *during initial start-up, periodically during normal operation*] to demonstrate the correct operation of the TSF.

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

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

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.

7.2. 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 5 (EAL5) and augmented by taking the following component:
- ALC_DVS.2 and AVA_VAN.5

7.3. Security Functional Requirement Rationale

The traceability table and the coverage rationale between SFR and security objectives is provided in the [PP], section 6.3.1.

7.4. Dependency Rationale

The dependency analysis for the SFRs is provided in the [PP], section 6.3.2

7.5. Security Assurance Requirement Rationale

This composite ST has a set of assurance requirements at EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 were chosen in order to meet the assurance expectations to this type of TOE which is intended to operate in open environments, where attackers can easily exploit vulnerabilities.
This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices without the need for highly specialized processes and practices. It corresponds to a white box analysis and it can be considered as a reasonable level that can be applied to an existing product line without undue expense and complexity.

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

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives **OT.Sens_Data_Conf** and **OT.Chip_Auth_Proof**.

The component ALC_DVS.2 augmented to EAL5 has no dependencies to other security requirements.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

All of these are met or exceeded in the EAL5 assurance package.

8. TOE summary specification

This section provides a description of how the TOE satisfies all the security functional requirements.

- **FAU_SAS.1 Audit storage**
  IC Manufacturer writes IC Serial Number during IC manufacturing process. MTRD Manufacturer does not deal with any Pre-personalization data.

- **FCS_CKM.1 Cryptographic key generation**
  As chip authentication is done, a secret seed will be shared between TOE and Terminal using the Elliptic curve Diffie-Hellman Private Key. The TSF generates session keys using the shared secret seed which protect commands and responses exchanged between a terminal and a card.

- **FCS_CKM.4 Cryptographic key destruction**
  Session keys used for secure messaging are destroyed irreversibly.

- **FCS_COP.1/SHA Cryptographic operation**
  The TOE is capable of performing all cryptographic operations defined in all iterations of this SFR. It also meets each standard as specified.

- **FCS_COP.1/SYM Cryptographic operation**
  The TOE is capable of performing all cryptographic operations defined in all iterations of this SFR. It also meets each standard as specified.

- **FCS_COP.1/MAC Cryptographic operation**
  The TOE is capable of performing all cryptographic operations defined in all iterations of this SFR. It also meets each standard as specified.

- **FCS_COP.1/ SIG_VER Cryptographic operation**
  The TOE receives CVCA, DV or IS certificates and verifies their signatures prior to importing them during certificate chaining.

- **FCS_RND.1 Quality metric for random numbers**
  The TSF uses random numbers generated by underlying platform which ensures level of entropy specified in [STIC].

- **FIA_UID.1 Timing of identification**
  The TOE allows secure messaging defined in [ICAO] and Chip Authentication defined in [TR-03] before a user is identified. Other TSF-mandated action such as reading biometric information is not allowed prior to user identification.

- **FIA_UAU.1 Timing of authentication**
  The TOE allows secure messaging defined in [ICAO] and Chip Authentication defined in [TR-03] before a user is authenticated. Other TSF-mandated action such as reading biometric information is not allowed prior to user authentication

- **FIA_UAU.4 Single-use authentication mechanisms**
  The TSF requires using random number to verify an Inspection System for Terminal Authentication according to [TR-03]. It also requires using challenge to authenticate

Personalization Agent keys.

- **FIA_UAU.5 Multiple authentication mechanisms**
  The TSF provides Personalization Agent Authentication and Chip Authentication mechanisms. The TSF only accepts commands which MAC is correctly verified using the key agreed with a terminal. It also requires that Chip Authentication shall precede Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric information.

- **FIA_UAU.6 Re-authenticating**
  After Chip Authentication, the TOE always enforces checking by secure messaging in MAC_ENC mode each command based on Retail-MAC.

- **FIA_API.1 Authentication Proof of Identity**
  The TSF implements Chip authentication protocol according to [TR-03] which use private key stored in the TOE. As this private key cannot be read by an external access in any condition, proving possession of this key can be a valid proof of genuine identification.

- **FDP_ACC.1 Subset access control**
  The TSF implements the access control Policy over the EF.COM, EF.SOD, EF.DG.1 to EF.DG.16 of the logical MRTD, applying the rules and operations over objects defined in FDP_ACF.1

- **FDP_ACF.1 Basic Security attribute based access control**
  The TSF implements Personalization Agent Authentication and Terminal Authentication and enforces all the rules specified in this SFR.

- **FDP_UCT.1 Basic data exchange confidentiality**
  The TSF implements Basic Access Control mechanism according to [ICAO] and Extended Access Control mechanism according to [TR-03], which enforces MAC_ENC mode to protect user data from unauthorised disclosure.

- **FDP_UIT.1 Data exchange integrity**
  The TSF implements Basic Access Control mechanism according to [ICAO] and Extended Access Control mechanism according to [TR-03], which enforces MAC_ENC mode to protect user data from modification, deletion, insertion and replay errors.

- **FMT_SMF.1 Specification of Management Functions**
  The TOE requires Transport Key Authentication to activate itself and Personalization Agent Key Authentication for personalization phase.

- **FMT_SMR.1 Security roles**
  The TSF defines all roles specified in this SFR and associates users with each of those roles by performing key authentications managed by the TSF.

- **FMT_LIM.1 Limited capabilities**
  The TSF does not have test features after TOE Delivery.

- **FMT_LIM.2 Limited availability**
  The TSF does not have test features after TOE Delivery.

- **FMT_MTD.1/INI_ENA Management of TSF data**

The TSF requires Transport Key Authentication and Personalization Agent Authentication to write Initialization Data and Pre-personalization Data.

- **FMT_MTD.1/INI_DIS Management of TSF data**
  The TSF requires Personalization Agent Authentication to disable read access for users to the Initialization Data.

- **FMT_MTD.1/CVCA_INI Management of TSF data**
  The TSF requires Personalization Agent Authentication to write initial CVCA Public Key, initial CVCA Certificate and initial Current Date.

- **FMT_MTD.1/CVCA_UPD Management of TSF data**
  The TSF verifies external CVCA certificates with initial CVCA Certificates and imports the certificate only in case that it is verified to be in a valid CVCA certificate chain.

- **FMT_MTD.1/DATE Management of TSF data**
  The TSF updates its Current Date if and only if CVCA, DV or IS certificate are verified to be signed with a valid private key during certificate chaining.

- **FMT_MTD.1/KEY_WRITE Management of TSF data**
  The TSF requires Personalization Agent Authentication to write The Document Basic Access Keys.

- **FMT_MTD.1/CAPK Management of TSF data**
  The TSF requires Personalization Agent Authentication to load the Chip Authentication Private Key.

- **FMT_MTD.1/KEY_READ Management of TSF data**
  The TSF does not provide functionality to read Personalization Agent keys, Chip Authentication Private Keys and Document Basic Access Keys to anyone in any life-cycle phase.

- **FMT_MTD.3 Secure TSF data**
  The TOE implements all requirements related to import a certificate specified in [TR-03].

- **FPT_EMSEC.1 TOE Emanation**
  The IC and the OS are designed to avoid disclosing of Personalization Agent Key(s) and the Chip Authentication Private Key by means of electromagnetic emanations.

- **FPT_FLS.1 Failure with preservation of secure state**
  If the TSF detects abnormal operating conditions or fails one of self-tests, it resets itself and performs self-destruction mechanism when certain condition is met.

- **FPT_TST.1 TSF testing**
  The TSF performs a suite of self-tests and take an action to preserve a secure state if a failure is detected during self-testing.

- **FPT_PHP.3 Resistance to physical attack**
  The TSF is designed to resist against physical manipulation and physical probing by responding automatically.

9. Acronyms

BIS	Basic Inspection System
CC	Common Criteria
EAL	Evaluation Assurance Level
EF	Elementary File
EIS	Extended Inspection System
GIS	General Inspection System
ICAO	International Civil Aviation Organization
IT	Information Technology
MRTD	Machine Readable Travel Document
OSP	Organizational security policy
PP	Protection Profile
RNG	Random Number Generator
SAR	Security assurance requirements
SFP	Security Function Policy
SFR	Security functional requirement
ST	Security Target
TOE	Target of evaluation
TSF	TOE Security Functions
PA	Passive Authentication
AA	Active Authentication
BAC	Basic Access Control
EAC	Extended Access Control

10. Bibliography

[PPBAC] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, Version 1.10, 25th March 2009

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

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

[TR-03] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für icherheit in der Informationstechnik (BSI)

[ICPP] Eurosmart Security IC Platform Protection Profile with augmentation packages, version 1.0, BSI-CC-PP-0084-2014

[STIC] S3FT9MH/ S3FT9MV/ S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional specific IC Dedicated Software Version 1.5 06th January 2016

[GDOM] Security Application Note for S3FT9MD/MC,MF/MT/MS,MH/MK/MG Version 1.9 09th June 2015

[AIS31] A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators version 3.1 25.09.2001

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

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

[SHA-2] Federal Information Processing Standards Publication 180-3 SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2008 October.

[PKCS3] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

[PKCS1] PKCS #1: RSA Cryptographic Standard, An RSA Laboratories Technical Note, Version 1.5, Revised November 1, 1993

[ISO15946-2] ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.

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

[GU] KONA2 D2320N ePassport Operational Guidance

[GP] KONA2 D2320N ePassport Preparative Procedure Guidance

[DEL] KONA2 D2320N ePassport Delivery Procedure

[GA] KONA2 D2320N ePassport Administrator Guidance

End of Document