KONA™

Kona102 ePassport with BAC Security Target Lite

Version 1.2
May 2013

kona i

Published by
KONA I Co, 150-872,
8F EXCON Venture Tower, 15-24 Yeouido-Dong Yongdungpo-Gu, Seoul, Korea.
Tel: 82-2-2168-7500
Fax: 82-2-769-1670
Homepage: www.konai.com

Version Information

1.0	March	2012	Create
1.1	April	2013	Update TOE from version 1.0.1 to 1.1.1
1.2	May	2013	Update TOE from version 1.1.1 to 1.1.2

Table of Contents

1. ST Introduction

1.1. ST Reference

Document No:	SP-02-18
Document Title:	Kona102 ePassport with BAC Security Target Lite
Version:	1
Revision:	2
Release date:	02/05/2013

1.2. TOE Reference

Name:	Kona102 ePassport [BAC configuration]
Version:	1
Revision:	1
Update (patch):	2

1.3. TOE Overview

The TOE defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the 'ICAO Doc 9303' [ICAO].

The TOE is composed of:

- the circuitry of the MRTD's chip (the integrated circuit, IC NXP Secure Smart Card Controllers P5CD081V1A)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system Kona102 ePassport version 1.1.2),
- the MRTD application and
- the associated guidance documentation.

It provides the security level of EAL4 augmented with ALC_DVS.2.

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 Basic 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 according to 'ICAO Doc 9303' [ICAO].

The TOE comprises:

- the circuitry of the MRTD's chip (the integrated circuit, IC NXP Secure Smart Card Controllers P5CD081V1A)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system Kona102 ePassport version 1.1.2),
- the MRTD application and
- 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:

the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder:
(1) the biographical data on the biographical data page of the passport book,
(2) the printed data in the Machine-Readable Zone (MRZ) and
(3) the printed portrait.
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:
(1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
(2) the digitized portraits (EF.DG2),
(3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both1
(4) the other data according to LDS (EF.DG5 to EF.DG16) and
(5) the Document security object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and

the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and 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 Basic Access Control Mechanism. This security target does not address the Active Authentication and the Extended Access Control as optional security mechanisms.

The Basic Access Control is a security feature which 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], normative appendix 5.

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

Phase 2 "Manufacturing"

(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 non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

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

(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.

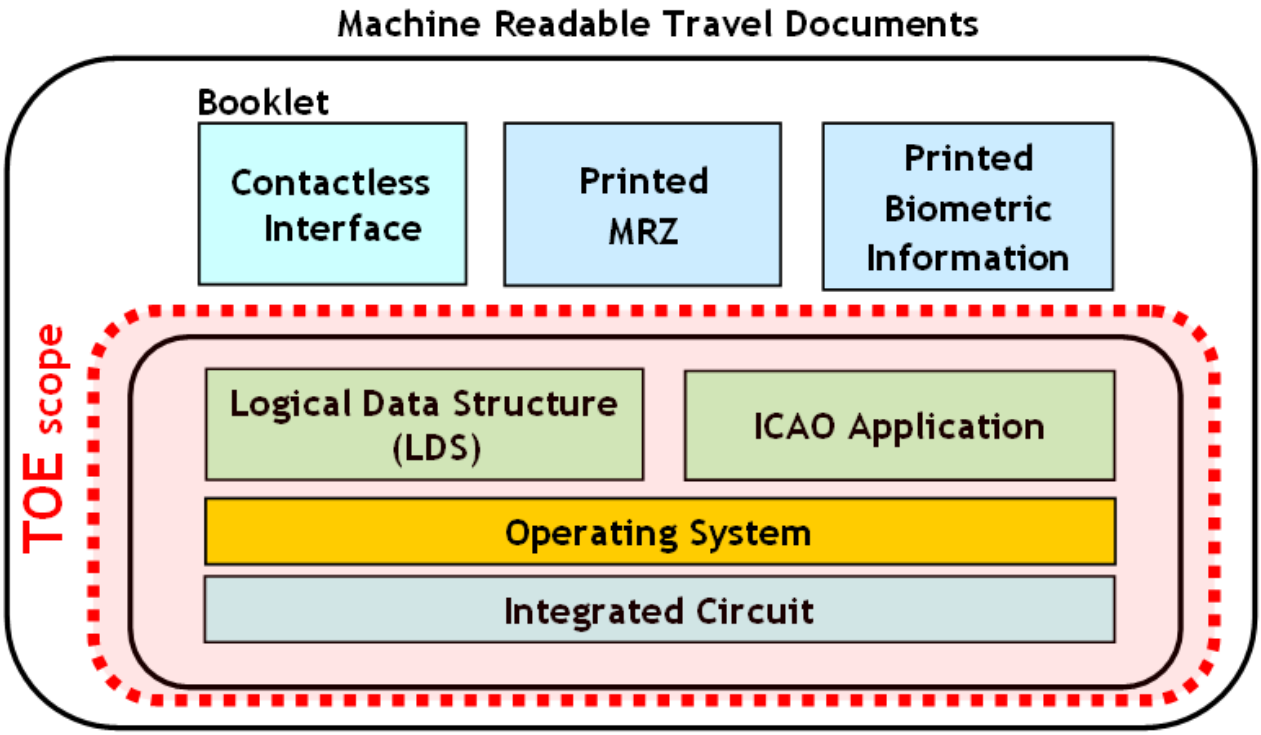
Phase 4 "Operational Use"

(Step7) The TOE is used as MRTD chip by the 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.

(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 a embedded software that controls the IC.



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.

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)
- [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 3, July 2009 conformant.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 3, July 2009 extended conformance with FAU_SAS.1, FCS_RND.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 3, July 2009 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", Basic Access Control version 1.10, 25th March 2009.

This security target and the TOE claim conformity with EAL4+, augmented with ALC_DVS.2 (Sufficiency of security measures).

3.1. Conformance Claim rationale

The security target and the TOE are conformant with CC version 3.1 release 3 and the protection profile with CC version 3.1 release 1 for Part 1, and release 2 for Part 2 and Part3. The following statements show the non-incompatibility between both:

- The differences between part 1 of CC version 3.1 in Release 1 and Release 3 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 3 applicable in the definition of some SFR. 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 R2 it applies FPT_TST.1.3 the requirements applies to TSF executable code, while in R3 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 3 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 R3 and PP conformant with CC v3.1 R1 and R2. The difference in the SFR is identified in the current ST.

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 Basic 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 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]. 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. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons as the 'ICAO Doc 9303' [ICAO] the TOE described in this security target 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 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].

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 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.

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", Basic Access Control PP(paragraph 54).

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", Basic Access Control PP (paragraph 55).

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", Basic Access Control PP (paragraph 56).

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", Basic Access Control PP (paragraph 57).

4.2.5. A.BAC-Keys Cryptographic quality of Basic Access Control Keys

This assumption is included in the ST and it is described in the MRTD, “ICAO Application", Basic Access Control PP (paragraph 59).

4.3. Threats

4.3.1. T.Chip_ID Identification of MRTD’s chip

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

4.3.2. T.Skimming Skimming the logical MRTD

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Basic Access Control PP, paragraph 64.

4.3.3. T.Eavesdropping Eavesdropping to the communication between TOE and inspection system

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

4.3.4. 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", Basic Access Control PP (paragraph 66).

4.3.5. T.Abuse-Func Abuse of Functionality

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

4.3.6. 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", Basic Access Control PP (paragraph 69).

4.3.7. T.Phys-Tamper Physical Tampering

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

4.3.8. T.Malfunction Malfunction due to Environmental Stress

This threat is included in the ST and it is described in the MRTD, "ICAO Application", Basic Access Control PP (paragraph 71).

4.4. Organizational Security Policies

4.4.1. 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", Basic Access Control PP (paragraph 73).

4.4.2. 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", Basic Access Control PP (paragraph 74).

4.4.3. P.Personal_Data Personal data protection policy

This security policy is included in the ST and it is described in the MRTD, "ICAO Application", Basic Access Control PP (paragraph 75).

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", Basic Access Control PP (paragraph 79).

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", Basic Access Control PP (paragraph 81).

5.1.3. OT.Data_Conf Confidentiality of personal data

This security objective for the TOE is included in the ST and it is described in the MRTD, “ICAO Application", Basic Access Control PP (paragraph 82).

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", Basic Access Control PP (paragraph 84).

5.1.5. 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", Basic Access Control PP (paragraph 87).

5.1.6. 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", Basic Access Control PP (paragraph 88).

5.1.7. 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", Basic Access Control PP (paragraph 90).

5.1.8. 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", Basic Access Control PP (paragraph 91).

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", Basic Access Control PP (paragraph 94).

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", Basic Access Control PP (paragraph 95).

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", Basic Access Control PP (paragraph 96).

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", Basic Access Control PP (paragraph 97).

5.2.5. OE.BAC-Keys Cryptographic quality of Basic Access Control Keys

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

5.2.6. 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", Basic Access Control PP (paragraph 100).

5.2.7. 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", Basic Access Control PP (paragraph 101).

5.2.8. 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", Basic Access Control PP (paragraph 102).

5.3. Security Objectives Rationale

The following table provides an overview for security objectives coverage:

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.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
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								
P.Manufact				X												
P.Personalization	X			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			

Coverage table between SPD and Objectives

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 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 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.Abuse-Func** “Abuse of Functionality” addresses attacks using the MRTD’s chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality”. 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 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”. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** “Protection of data from the logical MRTD” will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

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** “Cryptographic quality of Basic Access Control Keys” ensuring the sufficient key quality to be provided by the issuing State or Organization.

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", Basic 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", Basic Access Control PP (section 5.2).

6.3. 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", Basic Access Control PP (section 5.3).

6.4. 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", Basic Access Control PP (section 5.4).

7. Security Requirements

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

- Assignment: is denoted as underlined text; e.g.: assignment
- Selection: value defined between square-bracket and italic; e.g.: *[italic]*
- 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”, “Basic Inspection System” and “Terminal” used in the following chapter is given in section 3.1 from the [PP]. Note that all these subjects are acting for homonymous external entities. All used objects are defined in section 7 from the [PP].
The operations “write”, “read”, “modify”, and “disable read access” are used in accordance with the general linguistic usage. The operations “transmit”, “receive” and “authenticate” are originally taken from Common Criteria 3.1 R3 Part 2.

Definition of security attributes:

security attribute	meaning	values
Terminal authentication status	None (any Terminal)	Default role (i.e. without authorisation 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.
	Personalisation Agent	Terminal is authenticated as Personalisation Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

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 – 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 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] normative appendix 5.

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

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 sizes 112 bit that meet the following: FIPS 46-3 [DES] and [ICAO]; normative appendix 5, A5.3.

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: [*FIPS46-3 [DES]*]

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).

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: independent bits with Shannon entropy of 7.976 bits per octet.

7.1.3. Class FIA Identification and Authentication

Nane	SFR for the TOE	Algorithms and key sizes according to [6],

		normative appendix 5, and [20]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	**either** Triple-DES with 112 bit keys or AES with 128 up to 256 bit keys (cf. FCS_COP.1/AUTH) **(Not used in this Security Target)**

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 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.

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*].

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 mechanism(s) [*the Symmetric Authentication Mechanism with the Personalization Agent Key, none*]
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.1)” as specified below (Common Criteria Part 2).

Authentication failure handling (FIA_AFL.1)
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*30* ***consecutive***] unsuccessful authentication attempts occur related to failure of a Triple-DES based authentication event.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall terminate itself.

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 – Basic 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.

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 – Basic 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.

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. 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

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 user data in a manner protected from unauthorised 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.

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

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

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

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

Hierarchical to: No other components.
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.

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/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/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 and Personalization Agent Keys to none.

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 electromagnetic field in excess of values that allows deduce sensitive information enabling access to Personalization Agent Key(s) and none.

FPT_EMSEC.1.2 The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and 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 [*during initial start-up and 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 *TSF.*

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 4 (EAL4)

and augmented by taking the following component:

- ALC_DVS.2

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. And the SFR dependency is provided in the [PP], section 6.3.2.

7.4. Security Assurance Requirement Rationale

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

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements.

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 ROM-Masking process. MTRD Manufacturer does not deal with any Pre-personalization data.

- FCS_CKM.1 Cryptographic key generation
  Document Access Keys are used for secure messaging to protect commands and responses exchanged between a terminal and a card according to [ICAO].

- 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/ENC 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/AUTH 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_RND.1 Quality metric for random numbers
  The TSF uses random numbers generated by underlying platform and executes all required tests which ensure level of entropy specified in [STIC].

- FIA_UID.1 Timing of identification
  The TOE implements four life-cycles and decides which TSF-mediated actions are allowed before user identification based on its life-cycle state.

- FIA_UAU.1 Timing of authentication
  The TOE implements four life-cycles and decides which TSF-mediated actions are allowed before user authentication based on its life-cycle state.

- FIA_UAU.4 Single-use authentication mechanisms
  The TSF requires using random number to establish secure channel for Basic Access Control according to [ICAO]. It also requires using challenge to authenticate Personalization Agent keys.

- FIA_UAU.5 Multiple authentication mechanisms
  The TSF implements Basic Access Control Authentication Mechanism using Document Basic Access Keys based on Triple-DES algorithm. It also supports Personalization Agent Authentication using Symmetric Authentication Mechanism based on Triple-DES algorithm.

- FIA_UAU.6 Re-authenticating
  The TSF implements Basic Access Control Authentication Mechanism according to [ICAO]. The TOE always enforces checking by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal.

- FIA_AFL.1 Authentication failure handling
  The TSF terminates itself if 30 times unsuccessful authentication attempts occur related to failure of a Triple-DES based authentication event.

- FDP_ACC.1 Subset access control
  The TSF implements the basic 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 all objects, subjects, rules and operations defined in this SFR as specified in [PP] subsection 6.1.4.2

- FDP_UCT.1 Basic data exchange confidentiality
  The TSF implements Basic Access Control mechanism according to [ICAO], 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], 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 several types of authentication to perform management functions specified in this SFR.

- FMT_SMR.1 Security roles
  The TSF defines roles of Personalization Agent, Basic Inspection System as specified in [PP] 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 to restrict the ability to write the

Initialization Data and Pre-personalization Data to the Manufacturer.

- FMT_MTD.1/INI_DIS Management of TSF data
  The TSF requires Personalization Agent Key authentication to restrict the ability to disable read access for users to Initialization Data to Personalization Agent.

- FMT_MTD.1/KEY_WRITE Management of TSF data
  The TSF requires Personalization Agent Key authentication to restrict the ability to write to Document Basic Access Keys to the Personalization Agent.

- FMT_MTD.1/KEY_READ Management of TSF data
  The TSF does not provide functionality to read Personalization Agent keys and the Document Basic Access Keys to anyone in any life-cycle states.

- FPT_EMSEC.1 TOE Emanation
  The IC and the OS are designed to avoid disclosing of private date 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

10. Bibliography

[PP] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, Version 1.10, 25th March 2009, BSI-CC-PP-0055

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

[ICPP] Security IC Platform Protection Profile, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007

[STIC] NXP Secure Smart Card Controllers P5CD016/021/041V1A/051V1A and P5Cx081V1A Security Target Lite Rev. 1.4 – 25th October 2010, BSI-DSZ-CC-0555

[GDOM] NXP Secure Smartcard Controllers P5CD016/021/041 and P5Cx081 Guidance, Delivery and Operation Manual rev.1.5

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

[FIPS 180-2] 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

[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

[GU] Kona102 ePassport Technical Manual, version 1.3

[GP] Kona102 ePassport Proprietary Command Manual, version 1.5

[DEL] Kona102 ePassport Delivery Procedure Version 1.2