

**SECURITY TARGET LITE  
MICA0 1.3.69 ON IDEALCITIZ 2.1.1  
BAC CONFIGURATION**

**Reference:** 2017\_2000024546

**Issue Date:** 2017-02-01

**SECURITY TARGET LITE**

Ref.: 2017\_2000024546

**MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION**Page: **2/97**

## TABLE OF CONTENTS

<b>DOCUMENT EVOLUTION</b>	<b>7</b>
<b>1 ST Introduction</b>	<b>8</b>
<b>1.1 ST Identification</b>	<b>8</b>
<b>1.2 TOE Reference</b>	<b>8</b>
<b>1.3 TOE Overview</b>	<b>8</b>
<b>1.4 TOE Description</b>	<b>9</b>
1.4.1 TOE Definition	9
1.4.2 TOE usage and security features for operational use	10
1.4.3 TOE life cycle	12
<b>2 Conformance Claims</b>	<b>18</b>
<b>2.1 CC Conformance Claim</b>	<b>18</b>
<b>2.2 PP Claim</b>	<b>18</b>
<b>2.3 Package Claim</b>	<b>18</b>
<b>2.4 PP Conformance Rationale</b>	<b>18</b>
2.4.1 Main aspects	18
2.4.2 Overview of differences between the PP and the ST	19
<b>3 Security Problem Definition</b>	<b>22</b>
<b>3.1 Assets</b>	<b>22</b>
<b>3.2 Users / Subjects</b>	<b>22</b>
<b>3.3 Threats</b>	<b>23</b>
<b>3.4 Organisational Security Policies</b>	<b>26</b>
<b>3.5 Assumptions</b>	<b>27</b>
<b>4 Security Objectives</b>	<b>29</b>
<b>4.1 Security Objectives for the TOE</b>	<b>29</b>
<b>4.2 Security Objectives for the Operational Environment</b>	<b>31</b>
4.2.1 Issuing State or Organisation	31
4.2.2 Receiving State or Organisation	33
<b>4.3 Security Objectives Rationale</b>	<b>34</b>
4.3.1 Threats	34
4.3.2 Organisational Security Policies	35
4.3.3 Assumptions	35
4.3.4 SPD and Security Objectives	36
<b>5 Extended Requirements</b>	<b>39</b>
<b>5.1 Definition of the Family FAU_SAS</b>	<b>39</b>
5.1.1 FAU_SAS Audit data storage	39
<b>5.2 Definition of the Family FCS_RND</b>	<b>39</b>
5.2.1 FCS_RND Generation of random numbers	40
<b>5.3 Definition of the Family FIA_API</b>	<b>40</b>
5.3.1 FIA_API Authentication Proof of Identity	40
<b>5.4 Definition of the Family FMT_LIM</b>	<b>41</b>
5.4.1 FMT_LIM Limited capabilities and availability	41
<b>5.5 Definition of the Family FPT_EMSEC</b>	<b>42</b>
<b>6 Security Requirements</b>	<b>44</b>

<b>6.1</b>	<b>Security Functional Requirements</b>	<b>44</b>
6.1.1	Class FAU Security Audit	44
6.1.2	Class Cryptographic Support (FCS)	44
6.1.3	Random Number Generation (FCS_RND.1)	47
6.1.4	Class FIA Identification and Authentication	47
6.1.5	Class FDP User Data Protection	50
6.1.6	Class FMT Security Management	52
6.1.7	FPT Protection of the Security Functions	54
<b>6.2</b>	<b>Security Assurance Requirements</b>	<b>55</b>
<b>6.3</b>	<b>Security Requirements Rationale</b>	<b>56</b>
6.3.1	Objectives	56
6.3.2	Rationale tables of Security Objectives and SFRs	58
6.3.3	Dependencies	60
6.3.4	Rationale for the Security Assurance Requirements	62
6.3.5	ALC_DVS.2 Sufficiency of security measures	63
<b>7</b>	<b>TOE Summary Specification</b>	<b>64</b>
<b>7.1</b>	<b>TOE Summary Specification</b>	<b>64</b>
7.1.1	SF.IA Identification and Authentication	64
7.1.2	SF.CF Cryptographic functions support	64
7.1.3	SF.ILTB Protection against interference, logical tampering and bypass	65
7.1.4	SF.AC Access control / Storage and protection of logical travel document data	65
7.1.5	SF.SM Secure Messaging	65
7.1.6	SF.LCM Security and life cycle management	66
<b>7.2</b>	<b>SFRs and TSS</b>	<b>68</b>
7.2.1	SFRs and TSS - Rationale	68
<b>8</b>	<b>Statement of Compatibility concerning Composite Security Target</b>	<b>71</b>
<b>8.1</b>	<b>Separation of the platform TSF</b>	<b>71</b>
<b>8.2</b>	<b>Compatibility between the Composite Security Target and the Platform Security Target</b>	<b>80</b>
<b>8.3</b>	<b>Compatibility of Assurance Requirements</b>	<b>83</b>
<b>9</b>	<b>Annex</b>	<b>84</b>

## TABLES

<b>Table 1 Threats and Security Objectives – Coverage .....</b>	<b>36</b>
<b>Table 2 Security Objectives and Threats - Coverage .....</b>	<b>37</b>
<b>Table 3 OSPs and Security Objectives – Coverage .....</b>	<b>37</b>
<b>Table 4 Security Objectives and OSPs - Coverage.....</b>	<b>38</b>
<b>Table 5 Assumptions and Security Objectives for the Operational Environment – Coverage .....</b>	<b>38</b>
<b>Table 6 Security Objectives for the Operational Environment and Assumptions - Coverage .....</b>	<b>38</b>
<b>Table 7 Security Objectives and SFRs – Coverage.....</b>	<b>58</b>
<b>Table 8 SFRs and Security Objectives .....</b>	<b>59</b>
<b>Table 9 SFRs Dependencies .....</b>	<b>61</b>
<b>Table 10 SARs Dependencies .....</b>	<b>62</b>
<b>Table 11: Compatibility between platform Functionalities and the composite ST</b>	<b>72</b>
<b>Table 12: Compatibility between platform SFRs and the composite ST – Firewall Policy</b>	<b>73</b>
<b>Table 13: Compatibility between platform SFRs and the composite ST – Application Programming Interface .....</b>	<b>75</b>
<b>Table 14: Compatibility between platform SFRs and the composite ST – Card Security Management .....</b>	<b>75</b>
<b>Table 15: Compatibility between platform SFRs and the composite ST – AID Management .....</b>	<b>76</b>
<b>Table 16: Compatibility between platform SFRs and the composite ST – INSTG Security Functional Requirements .....</b>	<b>76</b>
<b>Table 17: Compatibility between platform SFRs and the composite ST – ADELG Security Functional Requirements .....</b>	<b>77</b>
<b>Table 18: Compatibility between platform SFRs and the composite ST – ODELG Security Functional Requirements .....</b>	<b>77</b>
<b>Table 19: Compatibility between platform SFRs and the composite ST – CARG Security Functional Requirements .....</b>	<b>78</b>
<b>Table 20: Compatibility between platform SFRs and the composite ST – PACE Functional Requirements .....</b>	<b>78</b>
<b>Table 21: Compatibility between platform SFRs and the composite ST - OSG Security Functional Requirements .....</b>	<b>79</b>
<b>Table 22: Compatibility between platform SFRs and the composite ST - LifeCycle Security Functional Requirements .....</b>	<b>79</b>
<b>Table 23: Compatibility between platform and composite ST .....</b>	<b>83</b>

## FIGURES

<b>Figure 1: TOE Perimeter .....</b>	<b>10</b>
<b>Figure 2: TOE life-cycle.....</b>	<b>13</b>

**SECURITY TARGET LITE**

Ref.: 2017\_2000024546

**MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION**Page: **7/97****DOCUMENT EVOLUTION**

<b>Date</b>	<b>Version</b>	<b>Author</b>	<b>Revision</b>
01/02/2017	1.0	Safran I&S	Final Public Version

## 1 ST INTRODUCTION

The aim of this document is to describe the Security Target Lite for the Machine Readable Travel Document (MRTD) with the ICAO application, Basic Access Control and Active Authentication on the Safran I&S IdealCitiz 2.1.1 Java Card Platform.

### 1.1 ST IDENTIFICATION

<b>Title</b>	Security Target Lite MICA0 on IdealCitiz 2.1.1, BAC configuration
<b>Reference</b>	2017_2000024546
<b>Version</b>	1.0
<b>Date</b>	01/02/2017
<b>ITSEF</b>	LETI-CEA
<b>Certification Body</b>	ANSSI
<b>Author</b>	SAFRAN I&S
<b>CC Version</b>	3.1 Revision 4
<b>Assurance Level</b>	EAL4 augmented with ALC_DVS.2
<b>Protection Profiles</b>	Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application“, Basic Access Control, BSI-PP-0055, Version 1.10, 25th March 2009 [BAC-PP]

### 1.2 TOE REFERENCE

<b>TOE name</b>	MICA0 on IdealCitiz 2.1.1, BAC configuration
<b>TOE version number</b>	1.3.69
<b>Name of Platform</b>	IdealCitiz 2.1.1 open platform
<b>Version of Platform</b>	2.1.1
<b>IC Identifiers</b>	Infineon M7892/93 B11 [ST-IC]
<b>Chip Ref. Certificate</b>	M7892: BSI-DSZ-CC-0782-V2-2015 [CR-IC] M7893: BSI-DSZ-CC-0879-V2-2015 [CR-IC]

### 1.3 TOE OVERVIEW

The Security Target (ST) defines the security objectives and requirements for the contactless and contact 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 method Basic Access Control and Active Authentication in the 'ICAO Doc 9303' [ICAO-9303].

Therefore, the main features and their origin are the following:

- Authentication by the Basic Access Control (BAC), using the Document Basic Access Key Derivation Algorithm according to 'ICAO Doc 9303' [ICAO-9303], Normative Appendix 5.
- Active Authentication (AA), to protect the MRTD's chip against chip substitution according to 'ICAO Doc 9303' [ICAO-9303], Volume II, Section IV, 5.6.2. It prevents copying the LDS Security Object (SO<sub>D</sub>) and proves that the SO<sub>D</sub> has been read from the authentic chip.

## 1.4 TOE DESCRIPTION

### 1.4.1 TOE Definition

The Target of Evaluation (TOE) is a contact or contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing Basic Access Control according to the ICAO document [ICAO-9303] and the protection profile [BAC-PP]. Additionally to the [BAC-PP] the TOE provides Active Authentication according to [ICAO-9303].

The TOE (MICAO on IDEalCitiz 2.1.1; BAC configuration) is composed of

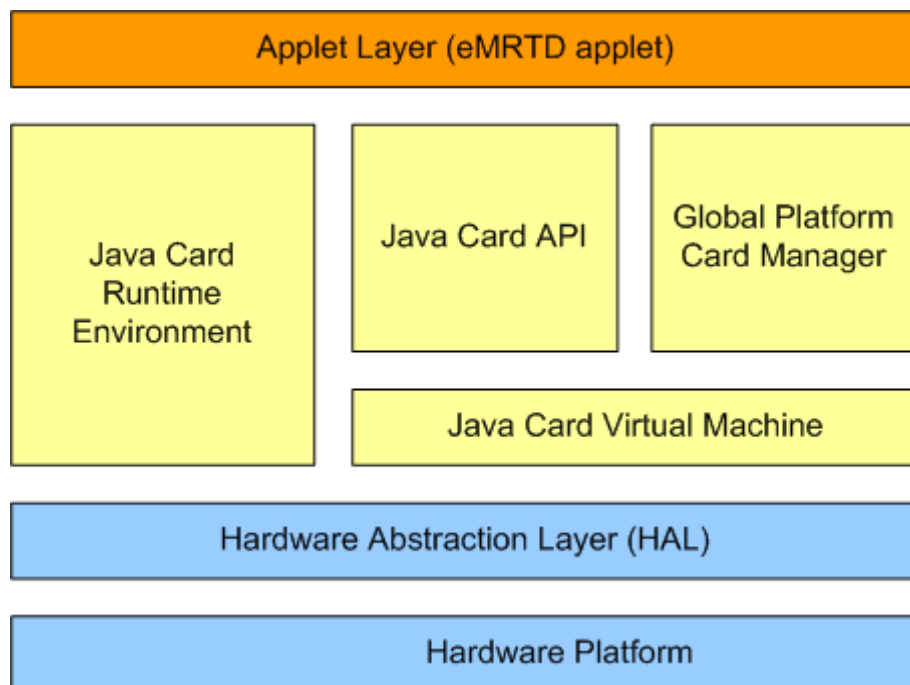
- the IDEalCitiz 2.1.1 open platform, comprising of
  - the circuitry of the MRTD's chip (the Infineon Security Controller M7892/93 B11 integrated circuit, IC) with hardware for the contact and contactless interface;
  - the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software;
  - the IC Embedded Software (operating system): IDEalCitiz 2.1.1 java card platform;
- the MRTD application MICAO on IDEalCitiz 2.1.1, BAC configuration Applet loaded in FLASH;
- the associated guidance documentation.

MICAO 1.3.69 Application is a set of Java card services intended to be used on the IDEalCitiz 2.1.1 java card Platform, which is certified according to CC EAL 5+ [PLTF-ST]. This Platform is based on the Infineon M7892/93 B11 IC security controller, which is itself certified according to CC EAL 6+ [ST-IC], [CER-IC].

A schematic overview of the TOE is shown in Figure 1:

- The MRTD's chip circuitry and the IC dedicated software forming the Smart Card Platform (Hardware Platform and Hardware Abstraction Layer);
- The IC embedded software running on the Smart Card Platform consisting of
  - Java Card virtual machine, ensuring language-level security;
  - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
  - Java card API, providing access to the card's resources for the Applet;
  - Global Platform Card Manager, responsible for management of Applets on the card.

- Native Mifare application; for this TOE the Mifare application is disabled.
- The Applet Layer is the **MICA0 1.3.69 on IDEALCITIZ 2.1.1, BAC configuration** Applet.



**Figure 1: TOE Perimeter**

#### 1.4.2 TOE usage and security features for operational use

A State or Organisation issues a MRTD to be used by the holder for international travel. The traveler presents its MRTD to the inspection system to prove his or her identity. The MRTD in the 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 the LDS for contactless and contact based machine reading.

The authentication of the traveler is based on:

- i. the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and
- ii. optional biometrics using the reference data stored in the MRTD.

The issuing State or Organization ensures the authenticity of the data of genuine MRTDs. The receiving State trusts genuine MRTDs of the issuing State or Organization.

The security functionality of the TOE will be externally available to the user by APDU commands according to the access conditions specified by the according policies considering the life cycle state, user role and security state.

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

- a) the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visually readable data including (but not limited to) personal data of the MRTD holder:

(1) the biographical data on the biographical data page of the passport book,

- (2) the printed data in the Machine Readable Zone (MRZ) and
  - (3) the printed portrait.
- b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure as specified by ICAO in [ICAO-9303] on the contactless or contact based integrated circuit. It presents contactless and/or contact based readable data including (but not limited to) personal data of the MRTD holder:
- (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  - (2) the digitized portraits (EF.DG2),
  - (3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both<sup>1</sup>
  - (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-9303]. 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 method 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 the logical MRTD and the Data Encryption of sensitive biometrics as optional security measure in the ICAO document [ICAO-9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD

- i. in integrity by write-only-once access control and by physical means, and
- ii. in confidentiality by the Basic Access Control Mechanism, and
- iii. in authenticity by the Active Authentication of the MRTD's chip.

This security target does not address the Extended Access Control as optional security mechanism.

The Basic Access Control is a security feature which is mandatorily supported by the TOE. The inspection system

- (i) optically reads the MRTD,
- (ii) authenticates itself as inspection system by means of the 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-9303], normative appendix 5.

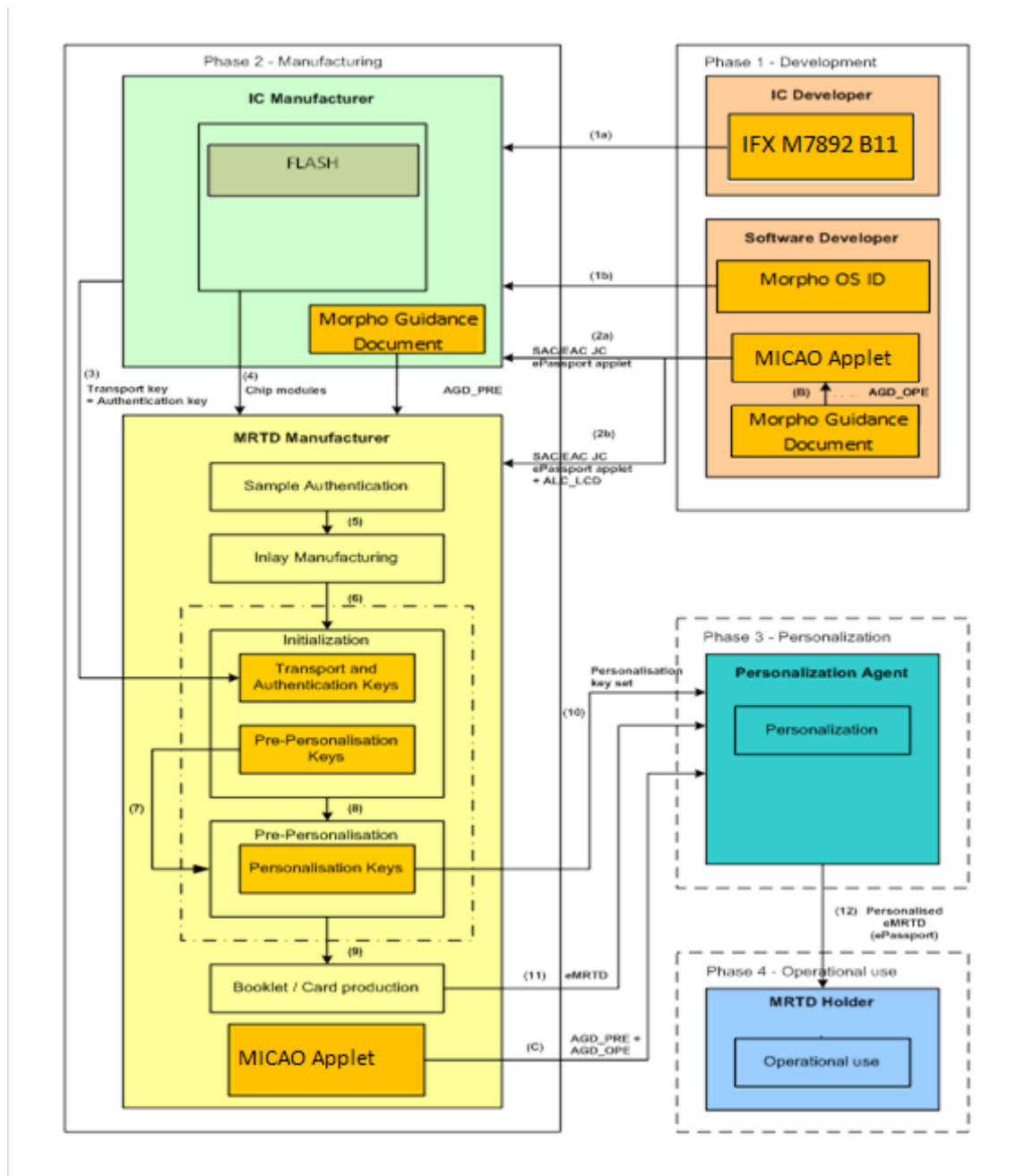
The Active Authentication is provided by the following steps:

<sup>1</sup> These additional biometric reference data are optional. Existing data are protected by means of extended access control.

- i. the inspection system communicates by means of secure messaging established by Basic Access Control,
- ii. the inspection system reads the LDS Document Security Object (SOD) from the MRTD
- iii. the inspection system reads the public key required for Active Authentication from LDS DG15 and verifies by means of the Passive Authentication the authenticity of the MRTD's Active Authentication Public Key using the Document Security Object,
- iv. the inspection system submits the TOE's Active Authentication command and includes a generated 8 bytes random number as challenge data.
- v. The TOE signs this challenge with the MRTD's Active Authentication Private Key and returns the signed challenge response (authentication data),
- vi. the inspection system reads the signed challenge response and verifies its signature.

#### 1.4.3 TOE life cycle

The TOE life cycle is described in terms of its four life cycle phases. (With respect to the [SIC-PP], the TOE life-cycle is additionally subdivided into 7 steps in the PP. These steps are denoted too in the following, although the sequence of the steps differs for the TOE life cycle).



**Figure 2: TOE life-cycle**

**Actors :**

IC Developer, IC Manufacturer	Infineon
Software Developer	Safran I&S (Osny)
Travel document manufacturer	Infineon

1.4.3.1 PHASE 1 "DEVELOPMENT"

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

(Step 2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the Safran I&S Embedded Software

(IDealCitiz 2.1.1 platform) and develops the ePassport application and the guidance documentation associated with these TOE components.

The MICA0 application is integrated either in ROM or in EEPROM of the chip. Depending on the intention

- (a) the ePassport application is securely delivered directly from the software developer (Safran I&S) to the IC manufacturer (Infineon). The applet code will be integrated into the FLASH code by the IC manufacturer, or
- (b) the ePassport application and the guidance documentation is securely delivered directly from the software developer (Safran I&S) to the travel document manufacturer (Safran I&S).

#### 1.4.3.2 PHASE 2 "MANUFACTURING"

(Step 3) In a first step, the TOE integrated circuit is produced containing the travel document's chip Dedicated Software, the parts of the travel document's chip Embedded Software, and in case of alternative a) the ePassport application in the non-volatile non-programmable memories (FLASH). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacturer to the travel document manufacturer.

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

(Step 4) The travel document manufacturer combines the IC with hardware for the contact based / contactless interface in the travel document unless the travel document consists of the chip only.

(Step 5) The travel document manufacturer

1. in case of alternative b), adds the ePassport application in the non-volatile programmable memories (for instance FLASH) if necessary,
2. creates the ePassport application and
3. equips travel document's chips with pre-personalization Data.

**BAC PP Application note 1:** Creation of the application for this TOE implies Applet instantiation.

For this Security Target the following name mappings to the protection profile [BAC-PP] apply:

- MRTD's chip Dedicated SW = Low level IC libraries
- travel document's chip Embedded Software = IDealCitiz 2.1.1 java card platform.
- ePassport application = the **MICA0 1.3.69 on IDealCitiz 2.1.1, BAC configuration** Applet run time code or an instantiation of it.
- Pre-personalization Data = Personalization Agent Key Set and Card Production Life Cycle (CPLC) data.

Both the underlying platform and the **MICA0 1.3.69 on IDealCitiz 2.1.1, BAC configuration** Applet provide configuration and life-cycle management functions required for TOE preparation. TOE preparation steps are performed in the manufacturing phase and consist of the following 2 activities:

1. Platform initialisation
2. Pre-personalisation

### **Platform initialization**

Platform initialization consists of the configuration of the IDEalCitiz 2.1.1 platform in accordance with requirements specified in the IDEalCitiz 2.1.1 platform administrator guidance [PLTF-PRE] by using the dedicated platform commands. Furthermore, the Pre-Personalisation Agent key set is installed and (a part of) the CPLC data is updated.

### **Pre-personalisation**

The pre-personalisation consists of the following steps:

- a. IC (chip) Authentication and getting chip access with the pre-personalisation key set.
- b. [optional] In case the **MICA0 1.3.69 on IDEalCitiz 2.1.1, BAC configuration** Applet runtime code does not reside in FLASH, it is loaded into FLASH.
- c. Create applet instance for **MICA0 1.3.69 on IDEalCitiz 2.1.1, BAC configuration** Applet (i.e. installation of the **MICA0 1.3.69 on IDEalCitiz 2.1.1, BAC configuration** Applet);
- d. Set the MRTD irreversibly in its PERSONALISATION life-cycle state by installation of the Personalisation Agent specific personalisation key set.

During step c the CPLC data with the IC Identifier is configured in the ePassport application instance. The last step (d) finalizes the TOE. This is the moment the TOE starts to exist and is ready for delivery to the Personalisation Agent. The guidance documentation for the Personalisation Agent is [AGD\_PRE].

The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation to the Personalisation Agent.

#### 1.4.3.3 PHASE 3 "PERSONALISATION OF THE TRAVEL DOCUMENT"

(Step 6) The personalization of the MRTD includes

- i. the survey of the MRTD holder's biographical data,
- ii. the enrolment of the MRTD holder's biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- iii. the printing of the visually readable data onto the physical MRTD,
- iv. the writing of the TOE User Data and TSF Data into the logical MRTD and
- v. the writing of the TSF Data into the logical MRTD and configuration of the TSF if necessary.

The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of

- i. the digital MRZ data (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-9303] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized



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

### **BAC PP Application note 2**

The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [CC-1] §92) comprise (but are not limited to) the Personalization Agent Authentication Key(s), the Basic Authentication Control Key and (for this Security Target) the Active Authentication Key.

### **BAC PP Application note 3:**

This Security Target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [ICAO-9303]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

The Personalization Agent authenticates by using two symmetric keys (MAC and ENC). In Personalisation life-cycle state, the TOE enforces mutual authentication between Personalisation Agent and TOE based on either of the following symmetric key authentication mechanism:

- ICAO BAC authentication mechanism and secure messaging protocol defined in [ICAO-9303] for 112 bits 3DES with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.
- ISO18013 BAP authentication mechanism defined in [ISO18013-3] for AES-128, 192 or 256 bits using AES secure messaging (CMAC, IV value, tags etc.) as specified in EAC TR-03110 [TR-03110-1] with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.

#### 1.4.3.4 PHASE 4 "OPERATIONAL USE"

(Step 7) The TOE is used as MRTD's 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.

**BAC PP Application note 4:** The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 "Operational Use". This will imply an update of the Document Security Object including the re-signing by the Document Signer.

**BAC PP Application note 5:** The intention of this Security Target is to consider at least the phases 1 and parts of phase 2 (i.e. Step 1 to Step 3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase 2 or later. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC.



Nevertheless, the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

Note, that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

#### 1.4.3.5 NON-TOE HARDWARE/SOFTWARE/FIRMWARE REQUIRED BY THE TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

## 2 CONFORMANCE CLAIMS

### 2.1 CC CONFORMANCE CLAIM

This security target claims to be conformant to the Common Criteria version 3.1, which comprises

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [CC-1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [CC-2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [CC-3]

as follows:

- Part 2 extended with
  - FAU\_SAS Audit data storage
  - FCS\_RND Generation of random numbers
  - FIA\_API Authentication proof of identity
  - FMT\_LIM Limited capabilities and availability
  - FPT\_EMSEC TOE emanation
- Part 3 conformant

The Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012 [CEM] has been taken into account.

### 2.2 PP CLAIM

This security target claims strict conformance to:

- Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application“, Basic Access Control, BSI-PP-0055, Version 1.10, 25<sup>th</sup> March. 2009 [BAC-PP]

### 2.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL4 augmented with ALC\_DVS.2 defined in CC part 3 [CC-3].

### 2.4 PP CONFORMANCE RATIONALE

This ST is claimed to be strictly conformant to the above mentioned PP [BAC-PP]. A detailed justification is given in the following.

#### 2.4.1 Main aspects

- The TOE description (ch. 1.4) is based on the TOE description of [BAC-PP, 2]. It was only enhanced by product specific details.

- All definitions of the security problem definition in [BAC-PP, 3] have been taken exactly from the PP in the same wording.
- All security objectives have been taken exactly from [BAC-PP, 4] in the same wording with one exception (see ch. 2.3.2 below)
- The part of extended components definition has been taken originally from [BAC-PP, 5].
- All SFRs for the TOE have been taken originally from the [BAC-PP, 5.1] added by according iterations, selections and assignments.
- The security assurance requirements (SARs) have been taken originally from the PP.

## 2.4.2 Overview of differences between the PP and the ST

### 2.4.2.1 ASSETS

As a feature that can be optionally configured, the TOE supports **Active Authentication** which according to [ICAO-9303] prevents copying the SO<sub>D</sub> and proves that it has been read from the authentic chip. It proves that the chip has not been substituted.

### 2.4.2.2 THREATS

The threat **T.Counterfeit** has been added to describe an unauthorized copy or reproduction of a genuine MRTD's chip.

#### **T.Counterfeit**

#### **MRTD's Chip**

*Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveler by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.*

*Threat agent: having high attack potential, being in possession of one or more legitimate MRTDs*

*Asset: authenticity of logical MRTD data*

### 2.4.2.3 ASSUMPTIONS

One assumption was added to cover Active Authentication during Personalization:

*A.Pers\_Agent\_AA Personalization of the MRTD's chip (Active Authentication)  
Additionally to A.Pers\_Agent the Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.*

### 2.4.2.4 SECURITY OBJECTIVES FOR THE TOE

The **OT.Chip\_Auth\_Proof** was added to also cover Active Authentication as follows:

#### **OT.Chip\_Auth\_Proof Proof of MRTD'S chip authenticity**

*The TOE must support the Basic and General Inspection Systems, to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by*

*means of the Active Authentication as defined in [ICAO-9303]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.*

#### 2.4.2.5 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The **OE.Auth\_Key\_MRTD** was added to consider the AA Key pair.

The **OE.AA\_MRTD** has been added by the Basic and General inspection systems.

These additions to the original objectives of the PP do not contradict with any other objective nor mitigate a threat (or part of a threat) meant to be addressed by security objectives for the TOE in the PP.

Their definitions are:

#### **OE.Auth\_Key\_MRTD MRTD Authentication Key**

*The issuing State or Organization has to establish the necessary public key infra-structure in order to*

- i. generate the MRTD's Active Authentication Key Pair,*
- ii. store the Active Authentication Private Key, and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 (if generated), and*
- iii. support inspection systems of receiving States or Organizations to verify the authenticity of the MRTD's chip used for genuine MRTDs by certification of the Active Authentication Public Key by means of the Document Security Object.*

#### **OE.Exam\_MRTD Examination of the MRTD passport book**

*The inspection system of the Receiving State must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability*

- i. includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and*
- ii. implements the terminal part of the Basic Access Control [ICAO-9303]. .*

#### **OE.AA\_MRTD Active Authentication – Inspection Systems**

*An Active Authentication (Basic, General or Extended) Inspection system performs all the functions of the Basic, General or Extended Inspection System respectively, and verifies the IC authenticity with an RSA or ECDSA signature generated by the MRTD (if available).*

#### 2.4.2.6 SECURITY FUNCTIONAL REQUIREMENTS

The Security Target enhances the following security functional requirements to support Active Authentication:

- FDP\_ACF.1 Security attribute based access control- Basic Access Control
- FMT\_MTD.1/KEY\_WRITE Management of TSF data – Key Write
- FMT\_MTD.1/KEY\_READ Management of TSF data – Key Read
- FPT\_EMSEC.1/ TOE Emanation
- FMT\_SMR.1 Security roles

**SECURITY TARGET LITE**

Ref.: 2017\_2000024546

**MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION**Page: **21/97**

This Security Target adds the following security functional requirements to support Active Authentication:

- FCS\_COP.1/SIG\_GEN Cryptographic operation – RSA or ECDSA Signature
- FIA\_API.1/AA Authentication proof of identity

## 3 SECURITY PROBLEM DEFINITION

### 3.1 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 9303]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Active Authentication Public Key (EF.DG15) is used by the inspection system for Active Authentication of the chip. The Chip Authentication Public Key (EF.DG14) 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-9303] the TOE described in this security target specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

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

The TOE prevents access to sensitive User Data

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

#### Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD.

### 3.2 USERS / 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 manufacturing life cycle phase (Phase 2). The TOE itself does not distinguish between the 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 (v) signing the Document Security Object defined in [ICAO 9303].

## Terminal

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

## Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System (BIS) (i) contains a terminal for the contactless/contact based 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. (iv) is recommend to perform Active Authentication (AA). AA verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.

The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

The security attributes of the EIS are defined of the Inspection System Certificates.

## MRTD Holder

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

## Traveler

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

## Attacker

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

## 3.3 THREATS

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

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

### T.Chip\_ID

#### Identification of MRTD's chip

Adverse action: An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless/contact based communication interface.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset: Anonymity of user.

## T.Skimming

### Skimming the logical MRTD

Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless/contact based communication channel of the TOE.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset: confidentiality of logical MRTD data.

## T.Eavesdropping

### Eavesdropping to the communication between TOE and inspection system

Adverse action: An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset: confidentiality of logical MRTD data

## T.Forgery

### Forgery of data on MRTD's chip

Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless/contact based chip.

Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate MRTDs

Asset: authenticity of logical MRTD data

#### *Application Note:*

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



## **T.Abuse-Func**

### **Abuse of Functionality**

Adverse action: An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the MRTD holder.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

## **T.Information\_Leakage**

### **Information Leakage from MRTD's chip**

Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless/contact based interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality of logical MRTD and TSF data

#### *Application Note:*

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

## **T.Phys-Tamper**

### **Physical Tampering**

Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-

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

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

*Application Note:*

Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the MRTD) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the MRTD's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

## T.Malfunction

### Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction of TSF or of the MRTD's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the MRTD outside the normal operating conditions, exploiting errors in the MRTD's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

*Application Note:*

A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

## T.Counterfeit

### MRTD's chip

Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveler by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

Threat agent: having high attack potential, being in possession of one or more legitimate MRTDs

Asset: authenticity of logical MRTD data

## 3.4 ORGANISATIONAL SECURITY POLICIES

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1 [CC 1], sec. 3.2).

## P.Manufact

### Manufacturing of the MRTD's chip

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

## P.Personalization

### Personalization of the MRTD by issuing State or Organization only

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

## P.Personal\_Data

### Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO 9303].

#### *Application Note:*

The organizational security policy P.Personal\_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO 9303]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

## 3.5 ASSUMPTIONS

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

### A.MRTD\_Manufact

#### MRTD manufacturing on steps 4 to 6

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

### A.MRTD\_Delivery

#### MRTD delivery during steps 4 to 6

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

- o Procedures shall ensure protection of TOE material/information under delivery and storage.
- o Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.

- o Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

## A.Pers\_Agent

### Personalization of the MRTD's chip

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key(EF.DG14) if stored on the MRTD's chip, (iv) the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip, and (v) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

## A.Pers\_Agent\_AA

### Personalization of the MRTD's chip (Active Authentication)

Additionally to A.Pers\_Agent the Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.

## A.Insp\_Sys

### Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State (i) examining a MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO 9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

#### *Application Note:*

According to [ICAO-9303] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

## A.BAC-Keys

### Cryptographic quality of Basic Access Control Keys

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

#### *Application Note:*

When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

## 4 SECURITY OBJECTIVES

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

### 4.1 SECURITY OBJECTIVES FOR THE TOE

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

#### OT.AC\_Pers

##### Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO 9303] and the TSF data can be written by authorized Personalisation Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalisation. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

*Application Note:*

The OT.AC\_Pers implies that

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

#### OT.Data\_Int

##### Integrity of personal data

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

#### OT.Data\_Conf

##### Confidentiality of personal data

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

*Application Note:*

The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys.

The security objective OT.Data\_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data

defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [ICAO-9303] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this protection profile. Thus the read access must be prevented even in case of a successful BAC Authentication.

## OT.Identification

### Identification and Authentication of the TOE

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

#### *Application Note:*

The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 'Manufacturing' and for traceability and/or to secure shipment of the TOE from Phase 2 'Manufacturing' into the Phase 3 'Personalization of the MRTD'. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 'Operational Use' the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

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

## OT.Chip\_Auth\_Proof

### Proof of MRTD'S chip authenticity

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

## OT.Prot\_Abuse-Func

### Protection against Abuse of Functionality

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

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

## OT.Prot\_Inf\_Leak

### Protection against Information Leakage



<p><b>SECURITY TARGET LITE</b></p> <p><b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b></p>	<p>Ref.: 2017_2000024546</p> <p>Page: <b>31/97</b></p>
---	--

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

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

*Application Note:*

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

**OT.Prot\_Phys-Tamper**

**Protection against Physical Tampering**

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

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

**OT.Prot\_Malfunction**

**Protection against Malfunctions**

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

*Application Note:*

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

**4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT**

**4.2.1 Issuing State or Organisation**

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

**OE.MRTD\_Manufact**

**Protection of the MRTD Manufacturing**

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

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

## OE.MRTD\_ Delivery

### Protection of the MRTD delivery

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

- o non-disclosure of any security relevant information,
- o identification of the element under delivery,
- o meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- o physical protection to prevent external damage,
- o secure storage and handling procedures (including rejected TOE's),
- o traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

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

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

## OE.Personalization

### Personalization of logical MRTD

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

## OE.Pass\_Auth\_Sign

### Authentication of logical MRTD by Signature

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO 9303].

## OE.BAC-Keys

### Cryptographic quality of Basic Access Control Keys



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

### **OE.Auth\_Key\_MRTD**

The issuing State or Organization has to establish the necessary public key infra-structure in order to

- i. generate the MRTD's Active Authentication Key Pair,
- ii. store the Active Authentication Private Key, and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 (if generated), and
- iii. support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip and Active Authentication Public Key by means of the Document Security Object.

#### **4.2.2 Receiving State or Organisation**

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

### **OE.Exam\_MRTD**

#### **Examination of the MRTD passport book**

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO 9303].

### **OE.AA\_MRTD**

#### **Active Authentication - Inspection Systems**

An Active Authentication (Basic, General or Extended) Inspection system performs all the functions of the Basic, General, respectively Extended Inspection System, and verifies the IC authenticity with an RSA or ECDSA signature generated by the MRTD (if available).

### **OE.Passive\_Auth\_Verif**

#### **Verification by Passive Authentication**

The border control officer of the receiving State uses the inspection system to verify the traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

### **OE.Prot\_Logical\_MRTD**

#### **Protection of data of the logical MRTD**

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic

Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

### 4.3 SECURITY OBJECTIVES RATIONALE

#### 4.3.1 Threats

**T.Chip\_ID** 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.

**T.Skimming** address the reading of the logical MRTD through 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.

**T.Eavesdropping** address the reading of the logical MRTD through 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'.

**T.Forgery** 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/contact based 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'.

**T.Abuse-Func** 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.

**T.Information\_Leakage** is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threats is addressed by the directly related security objective OT.Prot\_Inf\_Leak 'Protection against Information Leakage'.

**T.Phys-Tamper** is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threats is addressed by the directly related security objectives OT.Prot\_Inf\_Leak "Protection against Information Leakage", objective OT.Prot\_Phys-

Tamper "Protection against Physical Tampering" and OT.Prot\_Malfunction "Protection against Malfunctions".

**T.Malfunction** is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threats is addressed by the directly related security objective OT.Prot\_Malfunction 'Protection against Malfunctions'.

**T.Counterfeit** 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 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 Active Authentication Public Key has to be written into EF.DG15 as demanded by OE.Auth\_Key\_MRTD "MRTD Authentication Key". According to OE.AA\_MRTD "Active Authentication - Inspection Systems" and OE.Exam\_MRTD "Examination of the MRTD passport book" the Inspection system has to perform the Active Authentication Protocol to verify the authenticity of the MRTD's chip.

#### 4.3.2 Organisational Security Policies

**P.Manufact** 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.

**P.Personalization** 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.

**P.Personal\_Data** 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.

#### 4.3.3 Assumptions

**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.

**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.

**A.Pers\_Agent** The assumptions A.Pers\_Agent "Personalization of the MRTD's chip" and A.Pers\_Agent\_AA "Personalization of the MRTD's chip (Active Authentication)" are 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.

**A.Insp\_Sys** 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 Active 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' 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.

**A.BAC-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.

#### 4.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
<a href="#">T.Chip_ID</a>	<a href="#">OT.Identification</a> , <a href="#">OE.BAC-Keys</a>	<a href="#">Section 4.3.1</a>
<a href="#">T.Skimming</a>	<a href="#">OT.Data_Conf</a> , <a href="#">OE.BAC-Keys</a>	<a href="#">Section 4.3.1</a>
<a href="#">T.Eavesdropping</a>	<a href="#">OT.Data_Conf</a>	<a href="#">Section 4.3.1</a>
<a href="#">T.Forgery</a>	<a href="#">OT.AC_Pers</a> , <a href="#">OT.Data_Int</a> , <a href="#">OT.Prot_Phys-Tamper</a> , <a href="#">OE.Pass_Auth_Sign</a> , <a href="#">OE.Exam_MRTD</a> , <a href="#">OE.Passive_Auth_Verif</a> , <a href="#">OE.Personalization</a>	<a href="#">Section 4.3.1</a>
<a href="#">T.Abuse-Func</a>	<a href="#">OT.Prot_Abuse-Func</a> , <a href="#">OE.Personalization</a>	<a href="#">Section 4.3.1</a>
<a href="#">T.Information Leakage</a>	<a href="#">OT.Prot_Inf_Leak</a>	<a href="#">Section 4.3.1</a>
<a href="#">T.Phys-Tamper</a>	<a href="#">OT.Prot_Phys-Tamper</a> , <a href="#">OT.Prot_Inf_Leak</a> , <a href="#">OT.Prot_Malfunction</a>	<a href="#">Section 4.3.1</a>
<a href="#">T.Malfunction</a>	<a href="#">OT.Prot_Malfunction</a>	<a href="#">Section 4.3.1</a>
<a href="#">T.Counterfeit</a>	<a href="#">OT.Chip_Auth_Proof</a> , <a href="#">OE.Auth_Key_MRTD</a> , <a href="#">OE.Exam_MRTD</a> , <a href="#">OE.AA_MRTD</a>	<a href="#">Section 4.3.1</a>

**Table 1 Threats and Security Objectives – Coverage**

Security Objectives	Threats	Rationale
<a href="#">OT.AC_Pers</a>	<a href="#">T.Forgery</a>	
<a href="#">OT.Data_Int</a>	<a href="#">T.Forgery</a>	
<a href="#">OT.Data_Conf</a>	<a href="#">T.Skimming</a> , <a href="#">T.Eavesdropping</a>	
<a href="#">OT.Identification</a>	<a href="#">T.Chip_ID</a>	
<a href="#">OT.Chip_Auth_Proof</a>	<a href="#">T.Counterfeit</a>	
<a href="#">OT.Prot_Abuse-Func</a>	<a href="#">T.Abuse-Func</a>	
<a href="#">OT.Prot_Inf_Leak</a>	<a href="#">T.Information Leakage</a> , <a href="#">T.Phys-Tamper</a>	
<a href="#">OT.Prot_Phys-Tamper</a>	<a href="#">T.Forgery</a> , <a href="#">T.Phys-Tamper</a>	
<a href="#">OT.Prot_Malfunction</a>	<a href="#">T.Phys-Tamper</a> , <a href="#">T.Malfunction</a>	
<a href="#">OE.MRTD_Manufact</a>		

<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>37/97</b>
--	---

<a href="#">OE.MRTD_Delivery</a>		
<a href="#">OE.Personalization</a>	<a href="#">T.Forgery</a> , <a href="#">T.Abuse-Func</a>	
<a href="#">OE.Pass Auth Sign</a>	<a href="#">T.Forgery</a>	
<a href="#">OE.BAC-Keys</a>	<a href="#">T.Chip_ID</a> , <a href="#">T.Skimming</a>	
<a href="#">OE.Auth Key MRTD</a>	<a href="#">T.Counterfeit</a>	
<a href="#">OE.Exam MRTD</a>	<a href="#">T.Forgery</a> , <a href="#">T.Counterfeit</a>	
<a href="#">OE.AA MRTD</a>	<a href="#">T.Counterfeit</a>	
<a href="#">OE.Passive Auth Verif</a>	<a href="#">T.Forgery</a>	
<a href="#">OE.Prot Logical MRTD</a>		

**Table 2 Security Objectives and Threats - Coverage**

Organisational Security Policies	Security Objectives	Rationale
<a href="#">P.Manufact</a>	<a href="#">OT.Identification</a>	<a href="#">Section 4.3.2</a>
<a href="#">P.Personalization</a>	<a href="#">OT.AC_Pers</a> , <a href="#">OT.Identification</a> , <a href="#">OE.Personalization</a>	<a href="#">Section 4.3.2</a>
<a href="#">P.Personal_Data</a>	<a href="#">OT.Data_Conf</a> , <a href="#">OT.Data_Int</a>	<a href="#">Section 4.3.2</a>

**Table 3 OSPs and Security Objectives – Coverage**

Security Objectives	Organisational Security Policies	Rationale
<a href="#">OT.AC_Pers</a>	<a href="#">P.Personalization</a>	
<a href="#">OT.Data_Int</a>	<a href="#">P.Personal_Data</a>	
<a href="#">OT.Data_Conf</a>	<a href="#">P.Personal_Data</a>	
<a href="#">OT.Identification</a>	<a href="#">P.Manufact</a> , <a href="#">P.Personalization</a>	
<a href="#">OT.Chip Auth Proof</a>		
<a href="#">OT.Prot Abuse-Func</a>		
<a href="#">OT.Prot Inf Leak</a>		
<a href="#">OT.Prot Phys-Tamper</a>		
<a href="#">OT.Prot Malfunction</a>		
<a href="#">OE.MRTD Manufact</a>		
<a href="#">OE.MRTD Delivery</a>		
<a href="#">OE.Personalization</a>	<a href="#">P.Personalization</a>	
<a href="#">OE.Pass Auth Sign</a>		
<a href="#">OE.BAC-Keys</a>		
<a href="#">OE.Auth Key MRTD</a>		
<a href="#">OE.Exam MRTD</a>		
<a href="#">OE.AA MRTD</a>		

<a href="#">OE.Passive Auth Verif</a>		
<a href="#">OE.Prot Logical MRTD</a>		

**Table 4 Security Objectives and OSPs - Coverage**

Assumptions	Security Objectives for the Operational Environment	Rationale
<a href="#">A.MRTD Manufact</a>	<a href="#">OE.MRTD Manufact</a>	<a href="#">Section 4.3.3</a>
<a href="#">A.MRTD Delivery</a>	<a href="#">OE.MRTD Delivery</a>	<a href="#">Section 4.3.3</a>
<a href="#">A.Pers Agent</a>	<a href="#">OE.Personalization</a>	<a href="#">Section 4.3.3</a>
<a href="#">A.Pers Agent AA</a>	<a href="#">OE.Personalization</a>	<a href="#">Section 4.3.3</a>
<a href="#">A.Insp Sys</a>	<a href="#">OE.Exam MRTD</a> , <a href="#">OE.Prot Logical MRTD</a>	<a href="#">Section 4.3.3</a>
<a href="#">A.BAC-Keys</a>	<a href="#">OE.BAC-Keys</a>	<a href="#">Section 4.3.3</a>

**Table 5 Assumptions and Security Objectives for the Operational Environment – Coverage**

Security Objectives for the Operational Environment	Assumptions	Rationale
<a href="#">OE.MRTD Manufact</a>	<a href="#">A.MRTD Manufact</a>	
<a href="#">OE.MRTD Delivery</a>	<a href="#">A.MRTD Delivery</a>	
<a href="#">OE.Personalization</a>	<a href="#">A.Pers Agent</a> , <a href="#">A.Pers Agent AA</a>	
<a href="#">OE.Pass Auth Sign</a>		
<a href="#">OE.BAC-Keys</a>	<a href="#">A.BAC-Keys</a>	
<a href="#">OE.Auth Key MRTD</a>		
<a href="#">OE.Exam MRTD</a>	<a href="#">A.Insp Sys</a>	
<a href="#">OE.AA MRTD</a>		
<a href="#">OE.Passive Auth Verif</a>		
<a href="#">OE.Prot Logical MRTD</a>	<a href="#">A.Insp Sys</a>	

**Table 6 Security Objectives for the Operational Environment and Assumptions - Coverage**

## 5 EXTENDED REQUIREMENTS

### 5.1 DEFINITION OF THE FAMILY FAU\_SAS

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

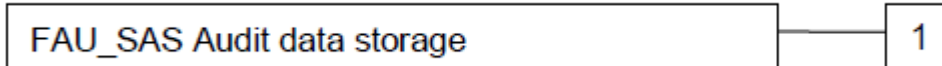
The family "Audit data storage (FAU\_SAS)" is specified as follows.

#### 5.1.1 FAU\_SAS Audit data storage

Family behavior

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

Component leveling



FAU\_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU\_SAS.1  
There are no management activities foreseen.

Audit: FAU\_SAS.1  
There are no actions defined to be auditable.

#### FAU\_SAS.1 Audit Storage

Hierarchical to: No other components.

Dependencies: No dependencies.

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

### 5.2 DEFINITION OF THE FAMILY FCS\_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS\_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS\_RND is not limited to generation of cryptographic keys unlike the component FCS\_CKM.1. The similar component FIA\_SOS.2 is intended for non-cryptographic use.

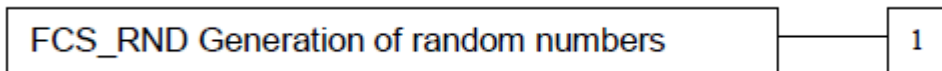
The family "Generation of random numbers (FCS\_RND)" is specified as follows.

### 5.2.1 FCS\_RND Generation of random numbers

Family behavior

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

Component leveling:



FCS\_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS\_RND.1  
There are no management activities foreseen.

Audit: FCS\_RND.1  
There are no actions defined to be auditable.

#### **FCS\_RND.1 Quality Metric for Random Numbers**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

### 5.3 DEFINITION OF THE FAMILY FIA\_API

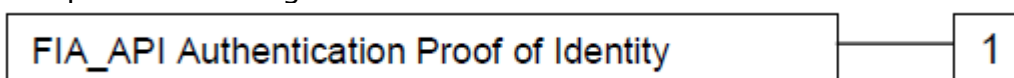
To describe the IT security functional requirements of the TOE a sensitive family (FIA\_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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

#### 5.3.1 FIA\_API Authentication Proof of Identity

Family behavior

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

Component levelling:



FIA\_API.1 Authentication Proof of Identity.  
Management: FIA\_API.1



<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>41/97</b>
--	---

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

**FIA\_API.1 Authentication Proof of Identity**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

**5.4 DEFINITION OF THE FAMILY FMT\_LIM**

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

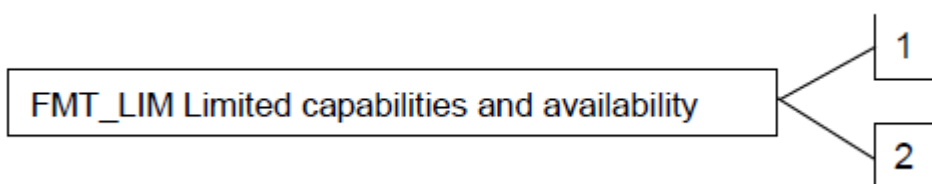
The family "Limited capabilities and availability (FMT\_LIM)" is specified as follows.

**5.4.1 FMT\_LIM Limited capabilities and availability**

Family behavior

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

Component leveling:



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

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

Management: FMT\_LIM.1, FMT\_LIM.2  
 There are no management activities foreseen.

<p><b>SECURITY TARGET LITE</b>  <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b></p>	<p>Ref.: 2017_2000024546  Page: <b>42/97</b></p>
---	--

Audit: FMT\_LIM.1, FMT\_LIM.2  
There are no actions defined to be auditable.

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

The TOE Functional Requirement "Limited capabilities (FMT\_LIM.1)" is specified as follows.

**FMT\_LIM.1 Limited Capabilities**

Hierarchical to: No other components.

Dependencies: FMT\_LIM.2 Limited availability.

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

The TOE Functional Requirement "Limited availability (FMT\_LIM.2)" is specified as follows.

**FMT\_LIM.2 Limited Availability**

Hierarchical to: No other components.

Dependencies: FMT\_LIM.1 Limited capabilities.

**FMT\_LIM.2.1** The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT\_LIM.1)" the following policy is enforced [assignment: Limited capability and availability policy].

**5.5 DEFINITION OF THE FAMILY FPT\_EMSEC**

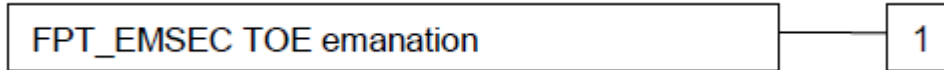
The sensitive family FPT\_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena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

The family "TOE Emanation (FPT\_EMSEC)" is specified as follows.

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT\_EMSEC.1 TOE emanation has two constituents:

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

FPT\_EMSEC.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT\_EMSEC.1  
There are no management activities foreseen.

Audit: FPT\_EMSEC.1  
There are no actions defined to be auditable.

**FPT\_EMS.1 TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

<p><b>SECURITY TARGET LITE</b>  <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b></p>	<p>Ref.: 2017_2000024546  Page: <b>44/97</b></p>
---	--

## 6 SECURITY REQUIREMENTS

### 6.1 SECURITY FUNCTIONAL REQUIREMENTS

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

Definition of security attributes:

security attribute	Values	meaning
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.

#### 6.1.1 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU\_SAS.1)" as specified below. For the extended components definition refer to [BAC-PP] chapter 4.

#### FAU\_SAS.1 Audit Storage

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

*Application Note:*

The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT\_MTD.1/INI\_DIS).

#### 6.1.2 Class Cryptographic Support (FCS)

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

**FCS\_CKM.1 Cryptographic key generation**

**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-9303], Volume 2, Section IV, Appendix 5.**

*Application Note:*

The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [ICAO 9303], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO 9303], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS\_RND.1.

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

*Application Note:*

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

**FCS\_COP.1/SHA Cryptographic operation**

**FCS\_COP.1.1/SHA** The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1, SHA-224, SHA-256, SHA-384, SHA-512** and cryptographic key sizes **none** that meet the following: **FIPS 180-4 [NIST-180-4].**

*Application Note:*

This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA\_UAU.4) according to [ICAO 9303].

**FCS\_COP.1/ENC Cryptographic operation**

**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 [FIPS46] and [ICAO-9303], Volume 2, normative appendix 5, A5.3.**

*Application Note:*

This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS\_CKM.1 and FIA\_UAU.4.

**FCS\_COP.1/AUTH Cryptographic operation**

**FCS\_COP.1.1/AUTH** The TSF shall perform **symmetric authentication - encryption and decryption**

in accordance with a specified cryptographic algorithm **Triple-DES and AES** and cryptographic key sizes **112 bit for Triple-DES and 128, 192 and 256 bit for AES** that meet the following: **FIPS 46-3 [FIPS46] for Triple-DES and [NIST-197]**.

*Application Note:*

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

**FCS\_COP.1/MAC Cryptographic operation**

**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)**.

*Application Note:*

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

**FCS\_COP.1/SIG\_GEN Cryptographic operation**

**FCS\_COP.1.1/SIG\_GEN** The TSF shall perform **digital signature generation** in accordance with a specified cryptographic algorithm **ECDSA and RSA** and cryptographic key sizes **192, 224, 256 and 320 bits for ECDSA and 1024, 1536, 1792 and 2048 bits for RSA** that meet the following: **ISO15946-2 specified in [ISO15946-2] for ECDSA and ISO9796-2 specified in [ISO9796-2] for RSA, in combination with SHA1, SHA224, SHA256, SHA384 and SHA512 digest algorithms specified in [NIST-180-4] for both ECDSA and RSA signatures.**

*Application Note:*

<p><b>SECURITY TARGET LITE</b>  <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b></p>	<p>Ref.: 2017_2000024546  Page: <b>47/97</b></p>
---	--

This SFR has been added to this ST in order to support the signing of challenges generated by the Inspection System as part of the optional Active Authentication protocol specified in [ICAO-9303].

**6.1.3 Random Number Generation (FCS\_RND.1)**

**FCS\_RND.1 Quality Metric for Random Numbers**

**FCS\_RND.1.1** The TSF shall provide a mechanism to generate random numbers that meet **Class PTG.2 according to AIS31 [AIS31]**.

*Application Note:*

Application Note: This SFR was added to the standard set of SFRs to address the requirements of the PACE protocol. The random number generation is provided by the underlying platform.

**6.1.4 Class FIA Identification and Authentication**

Application note: The following Table provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO 9303], 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)
Active Authentication	FIA_API.1/AA	RSA and ECDSA (cf. FCS_COP.1/SIG_GEN); RSA: 1536, 1792 and 2048 bits; ECDSA: 192, 224, 256 and 320 bits
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)

**FIA\_UID.1 Timing of identification**

**FIA\_UID.1.1** The TSF shall allow

- o **to read the Initialization Data in Phase 2 'Manufacturing',**
- o **to read the random identifier in Phase 3 'Personalization of the MRTD',**
- o **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.

*Application Note:*

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

In the 'Operational Use' phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip\_ID). Note that the terminal and the MRTD's chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more than one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip\_ID.

### FIA\_UAU.1 Timing of authentication

**FIA\_UAU.1.1** The TSF shall allow

- o **to read the Initialization Data in Phase 2 'Manufacturing',**
- o **to read the random identifier in Phase 3 'Personalization of the MRTD',**
- o **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.

*Application Note:*

The Basic Inspection System and the Personalization Agent authenticate themselves.

### FIA\_UAU.4 Single-use authentication mechanisms

**FIA\_UAU.4.1** The TSF shall prevent reuse of authentication data related to

- o **Basic Access Control Authentication Mechanism,**
- o **Authentication Mechanism based on Triple-DES.**

*Application Note:*

The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.



The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO 9303]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip\_ID.

### **FIA\_UAU.5 Multiple authentication mechanisms**

**FIA\_UAU.5.1** The TSF shall provide

- o **Basic Access Control Authentication Mechanism**
- o **Symmetric Authentication Mechanism based on Triple-DES and AES**

to support user authentication.

**FIA\_UAU.5.2** The TSF shall authenticate any user's claimed identity according to the

- o **the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s):**
  - **the Basic Access Control Authentication Mechanism with the Personalization Agent Keys**
  - **the Symmetric Authentication Mechanism with the Personalization Agent Key.**
- o **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.**

*Application Note:*

The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

### **FIA\_UAU.6 Re-authenticating**

**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.**

*Application Note:*

The Basic Access Control Mechanism specified in [ICAO 9303] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC\_ENC mode each command based on Retail-MAC whether it was sent by the

<p><b>SECURITY TARGET LITE</b>  <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b></p>	<p>Ref.: 2017_2000024546  Page: <b>50/97</b></p>
---	--

successfully authenticated terminal (see FCS\_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

**FIA\_AFL.1 Authentication failure handling**

**FIA\_AFL.1.1** The TSF shall detect when **an administrator configurable positive integer within one to 32767** unsuccessful authentication attempts occur related to **BAC authentication**.

**FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been **met and surpassed**, the TSF shall **wait an administrator configurable time before the next authentication attempt can be performed**.

*Application Note:*

The ST writer may consider the following example for such operations and refinement: FIA\_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 consecutive unsuccessful authentication attempts occur related to BAC authentication protocol. FIA\_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall wait for an administrator configurable time between the receiving the terminal challenge eIFD and sending the TSF response eICC during the BAC authentication attempts. The terminal challenge eIFD and the TSF response eICC are described in [20], Appendix C. The refinement by inclusion of the word 'consecutive' allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the 'consecutive unsuccessful authentication attempts' are count independent on power-on sessions but reset to zero after successful authentication only.

**FIA\_API.1/AA Authentication Proof of Identity**

**FIA\_API.1.1/AA** The TSF shall provide a **Active Authentication Protocol according to [ICAO-9303]** to prove the identity of the **TOE**.

**6.1.5 Class FDP User Data Protection**

Application note: FDP\_UCT.1 and FDP\_UTI.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

### FDP\_ACC.1 Subset 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.**

### FDP\_ACF.1 Security attribute based access control

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

- **Subjects:**
  - **Personalization Agent,**
  - **Basic Inspection System,**
  - **Terminal,**
- **Objects:**
  - **data EF.DG1 to EF.DG16 of the logical MRTD,**
  - **data in EF.COM,**
  - **data in EF.SOD,**
- **Security attributes**
  - **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:

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

**FDP\_ACF.1.3** The TSF shall explicitly 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 following additional rules:

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

### FDP\_UCT.1 Basic data exchange confidentiality

**FDP\_UCT.1.1** The TSF shall enforce the **Basic Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure.

### FDP\_UIT.1 Data exchange integrity

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

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

### 6.1.6 Class FMT Security Management

**Application note:** The SFR FMT\_SMF.1 and FMT\_SMR.1 provide basic requirements to the management of the TSF data.

**Application note:** The SFR FMT\_LIM.1 and FMT\_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

### FMT\_SMF.1 Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions:

- o **Initialization,**
- o **Pre-personalization,**
- o **Personalization.**

### FMT\_SMR.1 Security roles

**FMT\_SMR.1.1** The TSF shall maintain the roles

- o **Manufacturer,**
- o **Personalization Agent,**
- o **Basic Inspection System.**

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles.

### FMT\_LIM.1 Limited Capabilities

**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**

- o **User Data to be disclosed or manipulated**
- o **TSF data to be disclosed or manipulated**
- o **software to be reconstructed and**
- o **substantial information about construction of TSF to be gathered which may enable other attacks.**

### FMT\_LIM.2 Limited Availability

**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**

- o **User Data to be manipulated**
- o **TSF data to be disclosed or manipulated**
- o **software to be reconstructed and**
- o **substantial information about construction of TSF to be gathered which may enable other attacks.**

*Application Note:*

The formulation of 'Deploying Test Features' in FMT\_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT\_LIM.1 and FMT\_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term 'software' in item 3 of FMT\_LIM.1.1 and FMT\_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

### FMT\_MTD.1/INI\_ENA Management of TSF data

**FMT\_MTD.1.1/INI\_ENA** The TSF shall restrict the ability to **write the the Initialization Data and Prepersonalization Data to Manufacturer.**

*Application Note:*

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

### FMT\_MTD.1/INI\_DIS Management of TSF data

**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.**

*Application Note:*

According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 'Manufacturing' but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Prepersonalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU\_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 'personalization' but is not needed and may be misused in the Phase 4 'Operational Use'. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

**FMT\_MTD.1/KEY\_WRITE Management of TSF data**

**FMT\_MTD.1.1/KEY\_WRITE** The TSF shall restrict the ability to **restrict the ability to write** the **Document Basic Access Keys and the Active Authentication keys** to the **Personalization Agent**.

**FMT\_MTD.1/KEY\_READ Management of TSF data**

**FMT\_MTD.1.1/KEY\_READ** The TSF shall restrict the ability to **restrict the ability to read** the **Document Basic Access Keys, the Active Authentication Private Key and Personalization Agent Keys** to **none**.

*Application Note:*

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

**6.1.7 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.

**FPT\_EMS.1 TOE Emanation**

**FPT\_EMS.1.1** The TOE shall not emit **variations in power consumption or timing during command execution** in excess of **non-useful information** enabling access to **Personalization Agent Key(s) and Active Authentication Private Key** and **none**.

**FPT\_EMS.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 Active Authentication Private Key** and **none**.

*Application Note:*

The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip

has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions

### FPT\_FLS.1 Failure with preservation of secure state

**FPT\_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur:

- o **Exposure to out-of-range operating conditions where therefore a malfunction could occur,**
- o **failure detected by TSF according to FPT\_TST.1.**

### FPT\_TST.1 TSF testing

**FPT\_TST.1.1** The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **the TSF**.

**FPT\_TST.1.2** The TSF shall provide 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**.

### FPT\_PHP.3 Resistance to physical attack

**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.

*Application Note:*

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

## 6.2 SECURITY ASSURANCE REQUIREMENTS

The Evaluation Assurance Level is EAL4 augmented with ALC\_DVS.2.



## 6.3 SECURITY REQUIREMENTS RATIONALE

### 6.3.1 Objectives

#### 6.3.1.1 SECURITY OBJECTIVES FOR THE TOE

**OT.AC\_Pers** addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP\_ACC.1 and FDP\_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA\_UAU.4 and FIA\_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS\_CKM.1, FCS\_COP.1/SHA, FCS\_RND.1 (for key generation), and FCS\_COP.1/ENC as well as FCS\_COP.1/MAC) with the personalization key or for reasons of interoperability with the [BSI-PP-0056, Version 1.10, 25th March 2009] by using the symmetric authentication mechanism (FCS\_COP.1/AUTH).

In case of using the BAC mechanism the SFR FIA\_UAU.6 describes the re-authentication and FDP\_UCT.1 and FDP\_UTI.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS\_CKM.1, FCS\_COP.1/SHA, FCS\_RND.1 (for key generation), and FCS\_COP.1/ENC as well as FCS\_COP.1/MAC for the ENC\_MAC\_Mode.

The SFR FMT\_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT\_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT\_MTD.1/KEY\_WRITE as authentication reference data. The SFR FMT\_MTD.1/KEY\_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS\_CKM.4, FPT\_EMS.1, FPT\_FLS.1 and FPT\_PHP.3 the confidentiality of these keys.

**OT.Data\_Int** requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP\_ACC.1 and FDP\_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP\_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP\_ACF.1.4). The SFR FMT\_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT\_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA\_UAU.4, FIA\_UAU.5 and FIA\_UAU.6 using either FCS\_COP.1/ENC and FCS\_COP.1/MAC or FCS\_COP.1/AUTH.

The security objective OT.Data\_Int requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA\_UAU.6, FDP\_UCT.1 and FDP\_UTI.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS\_CKM.1, FCS\_COP.1/SHA, FCS\_RND.1 (for key generation), and FCS\_COP.1/ENC and FCS\_COP.1/MAC for the ENC\_MAC\_Mode. The SFR FMT\_MTD.1/KEY\_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT\_MTD.1/KEY\_READ.

**OT.Data\_Conf** requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA\_UID.1 and FIA\_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data\_Conf. In case of failed authentication attempts FIA\_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the



FDP\_ACC.1 and FDP\_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT\_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT\_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA\_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA\_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA\_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC\_MAC\_Mode by means of the cryptographic functions according to FCS\_COP.1/ENC and FCS\_COP.1/MAC (cf. the SFR FDP\_UCT.1 and FDP\_UIT.1). (for key generation), and FCS\_COP.1/ENC and FCS\_COP.1/MAC for the ENC\_MAC\_Mode. The SFR FCS\_CKM.1, FCS\_CKM.4, FCS\_COP.1/SHA and FCS\_RND.1 establish the key management for the secure messaging keys. The SFR FMT\_MTD.1/KEY\_WRITE addresses the key management and FMT\_MTD.1/KEY\_READ prevents reading of the Document Basic Access Keys.

Note, neither the security objective OT.Data\_Conf nor the SFR FIA\_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

**OT.Identification** addresses the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU\_SAS.1.

Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 'Operational Use'. The SFR FMT\_MTD.1/INI\_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT\_MTD.1/INI\_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 'Operational Use' violates the security objective OT.Identification. The SFR FIA\_UID.1 and FIA\_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts FIA\_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

**OT.Chip\_Auth\_Proof** The security objective OT.Chip\_Auth\_Proof "Proof of MRTD's chip authenticity" is ensured by Active Authentication provided by FIA\_API.1/AA proving the identity of the TOE.

The Active Authentication defined by FCS\_COP.1/SIG\_GEN for the generation of the RSA and ECDSA Signature is performed using a TOE internally stored confidential private key as required by FMT\_MTD.1/KEY\_WRITE and FMT\_MTD.1/KEY\_READ. According to FDP\_ACF.1, only the successfully authenticated Basic, Generic and Extended Inspection Systems are allowed to request active authentication (FDP\_ACF.1.2, rule 2).

**OT.Prot\_Abuse-Func** is ensured by the SFR FMT\_LIM.1 and FMT\_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

**OT.Prot\_Inf\_Leak** requires the TOE to protect confidential TSF data stored and/or processed in the MRTD's chip against disclosure

- o by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT\_EMS.1,
- o by forcing a malfunction of the TOE, which is addressed by the SFR FPT\_FLS.1 and FPT\_TST.1, and/or

- o by a physical manipulation of the TOE, which is addressed by the SFR FPT\_PHP.3.

**OT.Prot\_Phys-Tamper** is covered by the SFR FPT\_PHP.3.

**OT.Prot\_Malfunction** is covered by (i) the SFR FPT\_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT\_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

### 6.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
<a href="#">OT.AC Pers</a>	<a href="#">FPT EMS.1</a> , <a href="#">FCS CKM.4</a> , <a href="#">FCS RND.1</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FMT SMF.1</a> , <a href="#">FIA UAU.6</a> , <a href="#">FIA UAU.4</a> , <a href="#">FIA UAU.5</a> , <a href="#">FMT SMR.1</a> , <a href="#">FMT MTD.1/KEY WRITE</a> , <a href="#">FCS CKM.1</a> , <a href="#">FCS COP.1/SHA</a> , <a href="#">FCS COP.1/ENC</a> , <a href="#">FCS COP.1/AUTH</a> , <a href="#">FCS COP.1/MAC</a> , <a href="#">FDP ACC.1</a> , <a href="#">FDP ACF.1</a> , <a href="#">FDP UCT.1</a> , <a href="#">FDP UIT.1</a> , <a href="#">FPT PHP.3</a> , <a href="#">FPT FLS.1</a>	<a href="#">Section 6.3.1</a>
<a href="#">OT.Data Int</a>	<a href="#">FCS RND.1</a> , <a href="#">FMT SMF.1</a> , <a href="#">FCS COP.1/SHA</a> , <a href="#">FIA UAU.6</a> , <a href="#">FIA UAU.4</a> , <a href="#">FIA UAU.5</a> , <a href="#">FDP UCT.1</a> , <a href="#">FDP UIT.1</a> , <a href="#">FMT SMR.1</a> , <a href="#">FCS CKM.1</a> , <a href="#">FDP ACC.1</a> , <a href="#">FDP ACF.1</a> , <a href="#">FCS COP.1/ENC</a> , <a href="#">FCS COP.1/AUTH</a> , <a href="#">FCS COP.1/MAC</a> , <a href="#">FMT MTD.1/KEY WRITE</a> , <a href="#">FMT MTD.1/KEY READ</a>	<a href="#">Section 6.3.1</a>
<a href="#">OT.Data Conf</a>	<a href="#">FCS CKM.4</a> , <a href="#">FCS RND.1</a> , <a href="#">FMT SMF.1</a> , <a href="#">FIA UAU.1</a> , <a href="#">FIA UAU.6</a> , <a href="#">FIA UAU.4</a> , <a href="#">FIA UAU.5</a> , <a href="#">FDP UCT.1</a> , <a href="#">FDP UIT.1</a> , <a href="#">FMT SMR.1</a> , <a href="#">FCS CKM.1</a> , <a href="#">FIA UID.1</a> , <a href="#">FDP ACC.1</a> , <a href="#">FDP ACF.1</a> , <a href="#">FCS COP.1/SHA</a> , <a href="#">FCS COP.1/ENC</a> , <a href="#">FCS COP.1/MAC</a> , <a href="#">FIA AFL.1</a> , <a href="#">FMT MTD.1/KEY WRITE</a> , <a href="#">FMT MTD.1/KEY READ</a>	<a href="#">Section 6.3.1</a>
<a href="#">OT.Identification</a>	<a href="#">FAU SAS.1</a> , <a href="#">FMT MTD.1/INI ENA</a> , <a href="#">FMT MTD.1/INI DIS</a> , <a href="#">FIA UID.1</a> , <a href="#">FIA AFL.1</a> , <a href="#">FIA UAU.1</a>	<a href="#">Section 6.3.1</a>
<a href="#">OT.Chip Auth Proof</a>	<a href="#">FCS COP.1/SIG GEN</a> , <a href="#">FIA API.1/AA</a> , <a href="#">FDP ACF.1</a> , <a href="#">FMT MTD.1/KEY WRITE</a> , <a href="#">FMT MTD.1/KEY READ</a>	<a href="#">Section 6.3.1</a>
<a href="#">OT.Prot Abuse-Func</a>	<a href="#">FMT LIM.1</a> , <a href="#">FMT LIM.2</a>	<a href="#">Section 6.3.1</a>
<a href="#">OT.Prot Inf Leak</a>	<a href="#">FPT EMS.1</a> , <a href="#">FPT TST.1</a> , <a href="#">FPT FLS.1</a> , <a href="#">FPT PHP.3</a>	<a href="#">Section 6.3.1</a>
<a href="#">OT.Prot Phys-Tamper</a>	<a href="#">FPT PHP.3</a>	<a href="#">Section 6.3.1</a>
<a href="#">OT.Prot Malfunction</a>	<a href="#">FPT TST.1</a> , <a href="#">FPT FLS.1</a>	<a href="#">Section 6.3.1</a>

**Table 7 Security Objectives and SFRs – Coverage**

Security Functional Requirements	Security Objectives	Rationale
<a href="#">FAU SAS.1</a>	<a href="#">OT.Identification</a>	
<a href="#">FCS CKM.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	

<a href="#">FCS_CKM.4</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FCS COP.1/SHA</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FCS COP.1/ENC</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FCS COP.1/AUTH</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a>	
<a href="#">FCS COP.1/MAC</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FCS COP.1/SIG GEN</a>	<a href="#">OT.Chip Auth Proof</a>	
<a href="#">FCS RND.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FIA UID.1</a>	<a href="#">OT.Data Conf</a> , <a href="#">OT.Identification</a>	
<a href="#">FIA UAU.1</a>	<a href="#">OT.Data Conf</a> , <a href="#">OT.Identification</a>	
<a href="#">FIA UAU.4</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FIA UAU.5</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FIA UAU.6</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FIA AFL.1</a>	<a href="#">OT.Data Conf</a> , <a href="#">OT.Identification</a>	
<a href="#">FIA API.1/AA</a>	<a href="#">OT.Chip Auth Proof</a>	
<a href="#">FDP ACC.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FDP ACF.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a> , <a href="#">OT.Chip Auth Proof</a>	
<a href="#">FDP UCT.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FDP UIT.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FMT SMF.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FMT SMR.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a>	
<a href="#">FMT LIM.1</a>	<a href="#">OT.Prot Abuse-Func</a>	
<a href="#">FMT LIM.2</a>	<a href="#">OT.Prot Abuse-Func</a>	
<a href="#">FMT MTD.1/INI ENA</a>	<a href="#">OT.Identification</a>	
<a href="#">FMT MTD.1/INI DIS</a>	<a href="#">OT.Identification</a>	
<a href="#">FMT MTD.1/KEY WRITE</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a> , <a href="#">OT.Chip Auth Proof</a>	
<a href="#">FMT MTD.1/KEY READ</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Int</a> , <a href="#">OT.Data Conf</a> , <a href="#">OT.Chip Auth Proof</a>	
<a href="#">FPT EMS.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Prot Inf Leak</a>	
<a href="#">FPT FLS.1</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Prot Inf Leak</a> , <a href="#">OT.Prot Malfunction</a>	
<a href="#">FPT TST.1</a>	<a href="#">OT.Prot Inf Leak</a> , <a href="#">OT.Prot Malfunction</a>	
<a href="#">FPT PHP.3</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Prot Inf Leak</a> , <a href="#">OT.Prot Phys-Tamper</a>	

**Table 8 SFRs and Security Objectives**

### 6.3.3 Dependencies

#### 6.3.3.1 SFRS DEPENDENCIES

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">FAU_SAS.1</a>	No Dependencies	
<a href="#">FCS_CKM.1</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/ENC</a> , <a href="#">FCS_COP.1/MAC</a>
<a href="#">FCS_CKM.4</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	<a href="#">FCS_CKM.1</a>
<a href="#">FCS_COP.1/SHA</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a>
<a href="#">FCS_COP.1/ENC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS_COP.1/AUTH</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
<a href="#">FCS_COP.1/MAC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS_COP.1/SIG_GEN</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS_RND.1</a>	No Dependencies	
<a href="#">FIA_UID.1</a>	No Dependencies	
<a href="#">FIA_UAU.1</a>	(FIA_UID.1)	<a href="#">FIA_UID.1</a>
<a href="#">FIA_UAU.4</a>	No Dependencies	
<a href="#">FIA_UAU.5</a>	No Dependencies	
<a href="#">FIA_UAU.6</a>	No Dependencies	
<a href="#">FIA_AFL.1</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1</a>
<a href="#">FIA_API.1/AA</a>	No Dependencies	
<a href="#">FDP_ACC.1</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1</a>
<a href="#">FDP_ACF.1</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1</a>
<a href="#">FDP_UCT.1</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1</a>
<a href="#">FDP_UIT.1</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1</a>
<a href="#">FMT_SMF.1</a>	No Dependencies	
<a href="#">FMT_SMR.1</a>	(FIA_UID.1)	<a href="#">FIA_UID.1</a>
<a href="#">FMT_LIM.1</a>	No Dependencies	
<a href="#">FMT_LIM.2</a>	No Dependencies	
<a href="#">FMT_MTD.1/INI_ENA</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1</a>
<a href="#">FMT_MTD.1/INI_DIS</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1</a>

SECURITY TARGET LITE	Ref.: 2017_2000024546
MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION	Page: 61/97

<a href="#">FMT_MTD.1/KEY_WRITE</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1</a>
<a href="#">FMT_MTD.1/KEY_READ</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1</a>
<a href="#">FPT_EMS.1</a>	No Dependencies	
<a href="#">FPT_FLS.1</a>	No Dependencies	
<a href="#">FPT_TST.1</a>	No Dependencies	
<a href="#">FPT_PHP.3</a>	No Dependencies	

**Table 9 SFRs Dependencies**

#### 6.3.3.1.1 RATIONALE FOR THE EXCLUSION OF DEPENDENCIES

**The dependency FCS\_CKM.1 or FDP\_ITC.1 or FDP\_ITC.2 of FCS\_COP.1/SHA is discarded.** The hash algorithm required by the SFR FCS\_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS\_CKM.1) nor an import (FDP\_ITC.1/2) is necessary.

**The dependency FCS\_CKM.1 or FDP\_ITC.1 or FDP\_ITC.2 of FCS\_COP.1/AUTH is discarded.** The SFR FCS\_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT\_MTD.1/INI\_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS\_CKM.1 or FDP\_ITC. Since the key is permanently stored within the TOE there is no need for FCS\_CKM.4, too.

**The dependency FCS\_CKM.4 of FCS\_COP.1/AUTH is discarded.** The SFR FCS\_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT\_MTD.1/INI\_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS\_CKM.1 or FDP\_ITC. Since the key is permanently stored within the TOE there is no need for FCS\_CKM.4, too.

**The dependency FMT\_MSA.3 of FDP\_ACF.1 is discarded.** The access control TSF according to FDP\_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT\_MSA.1 and FMT\_MSA.3) is necessary here.

**The dependency FTP\_ITC.1 or FTP\_TRP.1 of FDP\_UCT.1 is discarded.** The SFR FDP\_UCT.1 requires the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP\_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP\_TRP.1 is not applicable here.

**The dependency FTP\_ITC.1 or FTP\_TRP.1 of FDP\_UIT.1 is discarded.** The SFR FDP\_UIT.1 requires the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP\_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP\_TRP.1 is not applicable here.

#### 6.3.3.2 SARS DEPENDENCIES

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">ADV_ARC.1</a>	(ADV_FSP.1) and (ADV_TDS.1)	<a href="#">ADV_FSP.4</a> , <a href="#">ADV_TDS.3</a>

<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>62/97</b>
--	---

<a href="#">ADV_FSP.4</a>	(ADV_TDS.1)	<a href="#">ADV_TDS.3</a>
<a href="#">ADV_IMP.1</a>	(ADV_TDS.3) and (ALC_TAT.1)	<a href="#">ADV_TDS.3</a> , <a href="#">ALC_TAT.1</a>
<a href="#">ADV_TDS.3</a>	(ADV_FSP.4)	<a href="#">ADV_FSP.4</a>
<a href="#">AGD_OPE.1</a>	(ADV_FSP.1)	<a href="#">ADV_FSP.4</a>
<a href="#">AGD_PRE.1</a>	No Dependencies	
<a href="#">ALC_CMC.4</a>	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	<a href="#">ALC_CMS.4</a> , <a href="#">ALC_DVS.2</a> , <a href="#">ALC_LCD.1</a>
<a href="#">ALC_CMS.4</a>	No Dependencies	
<a href="#">ALC_DEL.1</a>	No Dependencies	
<a href="#">ALC_DVS.2</a>	No Dependencies	
<a href="#">ALC_LCD.1</a>	No Dependencies	
<a href="#">ALC_TAT.1</a>	(ADV_IMP.1)	<a href="#">ADV_IMP.1</a>
<a href="#">ASE_CCL.1</a>	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	<a href="#">ASE_ECD.1</a> , <a href="#">ASE_INT.1</a> , <a href="#">ASE_REQ.2</a>
<a href="#">ASE_ECD.1</a>	No Dependencies	
<a href="#">ASE_INT.1</a>	No Dependencies	
<a href="#">ASE_OBJ.2</a>	(ASE_SPD.1)	<a href="#">ASE_SPD.1</a>
<a href="#">ASE_REQ.2</a>	(ASE_ECD.1) and (ASE_OBJ.2)	<a href="#">ASE_ECD.1</a> , <a href="#">ASE_OBJ.2</a>
<a href="#">ASE_SPD.1</a>	No Dependencies	
<a href="#">ASE_TSS.1</a>	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	<a href="#">ADV_FSP.4</a> , <a href="#">ASE_INT.1</a> , <a href="#">ASE_REQ.2</a>
<a href="#">ATE_COV.2</a>	(ADV_FSP.2) and (ATE_FUN.1)	<a href="#">ADV_FSP.4</a> , <a href="#">ATE_FUN.1</a>
<a href="#">ATE_DPT.1</a>	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	<a href="#">ADV_ARC.1</a> , <a href="#">ADV_TDS.3</a> , <a href="#">ATE_FUN.1</a>
<a href="#">ATE_FUN.1</a>	(ATE_COV.1)	<a href="#">ATE_COV.2</a>
<a href="#">ATE_IND.2</a>	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	<a href="#">ADV_FSP.4</a> , <a href="#">AGD_OPE.1</a> , <a href="#">AGD_PRE.1</a> , <a href="#">ATE_COV.2</a> , <a href="#">ATE_FUN.1</a>
<a href="#">AVA_VAN.3</a>	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	<a href="#">ADV_ARC.1</a> , <a href="#">ADV_FSP.4</a> , <a href="#">ADV_IMP.1</a> , <a href="#">ADV_TDS.3</a> , <a href="#">AGD_OPE.1</a> , <a href="#">AGD_PRE.1</a> , <a href="#">ATE_DPT.1</a>

**Table 10 SARs Dependencies**

### 6.3.4 Rationale for the Security Assurance Requirements

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 TARGET LITE**

Ref.: 2017\_2000024546

**MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION**Page: **63/97**

security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

### **6.3.5 ALC\_DVS.2 Sufficiency of security measures**

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.

## 7 TOE SUMMARY SPECIFICATION

### 7.1 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

The TOE provides security features which can be associated into following groups:

- Identification and Authentication mechanisms
- Cryptographic functions support
- Access control /Storage and protection of logical MRTD data
- Secure messaging
- Security and Life-cycle management

Moreover the TOE will protect itself against interference, logical tampering and bypass. The security functionality of the TOE respectively the MICA0 1.3.69 on IDEalCitiz 2.1.1, BAC configuration applet will be externally available to the user by APDU commands according to the access conditions specified by the according policies considering the life cycle state, user role and security state.

Remark: The numbering of the security functions is consistent with the Security Target [ST-SAC-EAC], where its supports in addition to BAC and Active Authentication also PACEV2 and Extended Access Control (EACv1) in accordance with respectively [ICAO-SAC] and [TR-03110-1] and [TR-03110-3].

#### 7.1.1 SF.IA Identification and Authentication

The different authentication mechanisms are supported by APDU commands and parameters using the cryptographic functions provided by the platform. The authentication mechanisms are enforced by protocols and APDU methods as specified in the functional specification.

The TOE supports the following authentication mechanisms:

- Basic Access Control Authentication mechanism (BAC)
- Authentication of the Personalization Agent with a personalisation key set based on a symmetric authentication mechanism.
- Active Authentication

#### 7.1.2 SF.CF Cryptographic functions support

Cryptographic function support is provided by the underlying IDEalCitiz 2.1.1 platform, i.e. the TOE relies on the underlying platform for performing its required cryptographic operations.

SF.CF Cryptographic functions include:

- 3DES and AES cipher operations for secure messaging
- Digest calculations (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512)
- Signature generation (ECDSA, RSA)
- Cryptographic key generation



- Key Destruction
- True Random Number generation

### 7.1.3 SF.ILTB Protection against interference, logical tampering and bypass

#### SF.ILTB.1

##### Protection against interference, logical tampering and bypass

Security domains are supported by the Java Card platform used by the TOE underlying IDEalCitiz 2.1.1 open platform. The IDEalCitiz 2.1.1 platform provides protection against physical attack and performs self-tests as described in [PLTF-ST].

The platform protects the TOE against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.

The MICA0 on IDEalCitiz 2.1.1, BAC configuration Applet uses transient memory where a hardware reset always reverts the MICA0 on IDEalCitiz 2.1.1, BAC configuration Applet into an unauthenticated state.

### 7.1.4 SF.AC Access control / Storage and protection of logical travel document data

#### SF.AC.1

##### Access control / Storage and protection of logical travel document data

The TOE provided access control, storage and protection of logical travel document data including access control to MRTD data. The TOE implements the subjects, objects, security attributes and rules according to the security attribute based access control. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

### 7.1.5 SF.SM Secure Messaging

#### SF.SM.1

##### Secure Messaging

Secure messaging MAC and ENC operations are performed by the TOE's platform.

In PERSONALISATION life-cycle state the TOE supports 3DES or AES secure messaging in ENC\_MAC mode, after a successful mutual authentication between TOE and Personalisation Agent terminal have been accomplished (see SF.I&A.4):

- o ICAO secure messaging protocol defined in [ICAO-9303] for 112 bits 3DES with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.
- o ISO18013 BAP secure messaging defined in [ISO18013-3] for AES-128, 192 or 256 bits using AES secure messaging (CMAC, IV value, tags etc.) as specified in EAC TR-03110 [TR-03110-1] with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.

In OPERATIONAL life-cycle state the TOE runs secure messaging in ENC\_MAC mode uses 112 bit Triple-DES in CBC mode only after successful BAC authentication. The MAC is calculated according to the Retail MAC cryptographic algorithm specified in [ISO9797], MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2. Secure messaging in ENC\_MAC mode is established during BAC.

## SF.SM.2

### Secure Messaging – Re-authentication

In OPERATIONAL life-cycle state, the Retail MAC for 3DES is part of every APDU command/response when secure messaging is active after a successful BAC authentication has been accomplished. Re-authentication after reset of the SM protocol is assured by accepting only valid mandatory MAC cryptograms.

In PERSONALISATION life-cycle state either the Retail MAC for 3DES or the CMAC for AES are part of every APDU command/response when secure messaging is active after a successful mutual authentication between TOE and Personalisation Agent has been accomplished. Re-authentication after reset of the SM protocol is assured by accepting only valid (mandatory) MAC or CMAC cryptograms.

### 7.1.6 SF.LCM Security and life cycle management

For the MICA0 1.3.69 on IDEALCITIZ 2.1.1, BAC configuration the following life-cycle phases have been identified:

- 1. Manufacturing phase
- 2. Personalisation phase
- 3. Operational phase
- 4. Termination phase

The life-time phases are reflected within the MICA0 1.3.69 on IDEALCITIZ 2.1.1, BAC configuration applet by an internal life-cycle state machine and supports the following life-cycle states:

- 1. Not instantiated (applet resides in EEPROM or ROM)
- 2. PRE-PERSONALISATION state
- 3. PERSONALISATION state
- 4. OPERATIONAL state
- 5. TERMINATED state (irreversibly)

Each life-cycle phase (or state) has its typical user acting as role holder.

Life cycle phase	Life-cycle state (maintained by applet)	Role
Manufacturing phase	- (Applet not instantiated)	IC Manufacturer
Manufacturing phase	- (Applet not instantiated)	MRTD Manufacturer (Platform initialisation)
Manufacturing phase	PRE-PERSONALISATION	MRTD Manufacturer (Pre-Personalisation)
Personalisation phase	PERSONALISATION	Personalisation Agent
Operational phase	OPERATIONAL	Basic or Extended Inspection System
Terminated phase	TERMINATED	None

All role holders in Manufacturing, Pre-Personalisation and Personalisation phases are identified by cryptographic authentication keys. In Operational phase the BAC password is required to authenticate the Basic or Extended Inspection System in order to get access to the non-sensitive ICAO LDS datagroups.

The MICA0 1.3.69 on IDEalCitiz 2.1.1, BAC configuration Applet maintains the internal life-cycle state the moment that the applet is installed. This state, together with the access control mechanisms force the Terminal into a specific role, for the pre-personalisation and subsequent, personalisation and operational phases. The phases (and corresponding life-cycle states) are controlled by APDU commands. The life-cycle phase and state transitions are irreversible.

### **SF.LCM.1**

#### **Management of phases, roles and MRTD life-cycle states – Manufacturing phase**

This security feature supports the management of roles and life-cycle state during Manufacturing phase.

### **SF.LCM.2**

#### **Management of phases, roles and MRTD life-cycle states – Personalisation phase**

This security feature supports the management of roles and life-cycle state during Personalisation phase.

### **SF.LCM.4**

#### **Protection of test features**

The MICA0 1.3.69 on IDEalCitiz 2.1.1, BAC configuration Applet does not have any dedicated test features implemented. The test features of the IDEalCitiz 2.1.1 platform are protected by ways described in [PLTF-ST] and guidance documentation.

### **SF.LCM.5**

#### **Protection of keys and PACE passwords**

In PRE-PERSONALISATION life-cycle state personalisation Agent Key Set is installed on the TOE's platform and protected by the platform. In all TOE life-cycle states the Personalization Agent Key set (MAC, ENC, KEK), the BAC keys (derived from MRZ) and the Active Authentication Private Key are also protected from disclosure. The MICA0 1.3.69 on IDEalCitiz 2.1.1, BAC configuration Applet only stores keys in Java Card specified Key structures, which are protected by IDEalCitiz 2.1.1 platform.

### **SF.LCM.6**

#### **IC Identification data**

During initialisation the MICA0 1.3.69 on IDEalCitiz 2.1.1, BAC configuration Applet is installed and initiated with the Pre-Personalisation Agent key and the IC Identification data. The INSTALL for INSTALL method of the IDEalCitiz 2.1.1 platform will be used to store the IC Identification data.

## 7.2 SFRS AND TSS

### 7.2.1 SFRs and TSS - Rationale

#### 7.2.1.1 TOE SUMMARY SPECIFICATION

##### 7.2.1.1.1 *SF.IA IDENTIFICATION AND AUTHENTICATION*

The implementation of BAC contributes to:

- o FIA\_UID.1 Timing of Identification
- o FIA\_UAU.1 Timing of Authentication
- o FIA\_UAU.4 Single-use authentication of the Terminal by the TOE
- o FIA\_UAU.5 Multiple authentication mechanisms
- o FIA\_UAU.6 Re-authenticating of Terminal by the TOE
- o FMT\_SMR.1 Security Roles
- o FCS\_COP.1/AUTH
- o FIA\_AFL.1 Authentication Failure Handling

The implementation of the Personalisation Agent Authentication contributes to

- o FIA\_UID.1 Timing of Identification
- o FIA\_UAU.1 Timing of authentication
- o FIA\_UAU.4 Single-use authentication of the Terminal by the TOE
- o FIA\_UAU.5 Multiple authentication mechanisms
- o FMT\_SMR.1 Security Roles

The implementation of Active Authentication contributes to

- o FIA\_API.1/AA Authentication Proof of Identity – MRTD
- o FMT\_MTD.1/KEY\_WRITE, Management of TSF data – Key Write
- o FMT\_MTD.1/KEY\_READ, Management of TSF data – Key Read
- o FCS\_COP.1/SIG\_GEN, Cryptographic operation – Signature generation by travel document (RSA and ECDSA)

##### 7.2.1.1.2 *SF.CF CRYPTOGRAPHIC FUNCTIONS SUPPORT*

The implementation of this security function contributes to:

- o FCS\_COP.1/ ENC Cryptographic operation – Encryption / Decryption Triple DES
- o FCS\_COP.1/ MAC Cryptographic operation Retail MAC
- o FCS\_COP.1/SIG\_GEN
- o FIA\_API.1/AA
- o FCS\_COP.1/SHA Cryptographic operation – Hash for Key Derivation by MRTD and according the application in this ST
- o FCS\_CKM.4 Cryptographic key destruction
- o FCS\_RND.1 Quality metric for random numbers

7.2.1.1.3 *SF.ILTB PROTECTION AGAINST INTERFERENCE, LOGICAL TAMPERING AND BYPASS*

**SF.ILTB.1** The implementation of this security function contributes to:

- o FPT\_FLS.1 Failure with preservation of secure state
- o FPT\_TST.1 TSF testing
- o FPT\_PHP.3 Resistance to physical attack

7.2.1.1.4 *SF.AC ACCESS CONTROL / STORAGE AND PROTECTION OF LOGICAL TRAVEL DOCUMENT DATA*

**SF.AC.1** The implementation of this security function contributes to:

- o FDP\_ACC.1 Subset access control - Basic Access Control
- o FDP\_ACF.1 Security attribute based access control - Basic Access Control
- o FDP\_UIT.1 Data exchange integrity - MRTD
- o FDP\_UCT.1 Basic data exchange confidentiality – MRTD

7.2.1.1.5 *SF.SM SECURE MESSAGING*

**SF.SM.1** The implementation of this security function contributes to::

- o FCS\_COP.1/ENC: Encryption/Decryption 3DES
- o FCS\_COP.1/MAC: Cryptographic operation – Retail MAC
- o FDP\_UCT.1 Basic data exchange confidentiality
- o FDP\_UIT.1 Data exchange integrity

**SF.SM.2** The implementation of this security function contributes to:

- o FIA\_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE

7.2.1.1.6 *SF.LCM SECURITY AND LIFE CYCLE MANAGEMENT*

**SF.LCM.1** The implementation of this security function contributes to:

- o FMT\_SMF.1 Specification of Management Functions (Initialization part)
- o FMT\_SMR.1.1 Security roles (Manufacturer)
- o FMT\_MTD.1/INI\_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data
- o FMT\_MTD.1/INI\_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

**SF.LCM.2** The implementation of this security function contributes to:

- o FMT\_SMF.1 Specification of Management Functions (Personalization)
- o FMT\_SMR.1.1 Security roles (Personalization Agent)
- o FMT\_MTD.1/KEY\_WRITE (Management of TSF data – Key Write) Restriction of the ability to write (load) the Active Authentication Private Key, the BAC keys or refresh the Personalisation Agent Key Set to the Personalisation Agent in PERSONALISATION life-cycle state.

**SF.LCM.4** The platform implementation provides this security function and contributes to:

- o FMT\_LIM.1 Limited capabilities

- o FMT\_LIM.2 Limited availability

**SF.LCM.5** The implementation of this security function contributes to:

- o FMT\_MTD.1/KEY\_READ Management of TSF data – Key Read
- o FPT\_EMS.1 TOE Emanation

**SF.LCM.6**

- o FAU\_SAS.1 Audit storage The audit records are usually write-only-once data of the travel document (see FMT\_MTD.1/INI\_ENA, FMT\_MTD.1/INI\_DIS).

## 8 STATEMENT OF COMPATIBILITY CONCERNING COMPOSITE SECURITY TARGET

### 8.1 SEPARATION OF THE PLATFORM TSF

This section describes the separation of relevant security functionality described in the ST of the platform (IDealCitiz 2.1.1 [PLTF-ST]) being used by this ST.

The following table confronts the relevant security functionality of the platform with those of the composite TOE defined in the present ST

IDealCitiz 2.1.1 Fonctionnalités in [PLTF-ST]	Usage by TOE
F.OPEN	<i>Not relevant</i>
F.CARD_MANAGER	<i>Relevant SF Used by SF.LCM.1, SF.LCM.2, SF.LCM.4, SF.LCM.5 and SF.LCM.6</i>
F.JAVA_CARD_SYSTEM	<i>Not relevant</i>
F.JAVA_API	<i>Relevant SF Used by SF.ILTB.1</i>
F.AUTHENTICATION	<i>Relevant SF Used by SF.IA and SF.SM.1, SF.SM.2</i>
F.MEMORY_PROGRAMMING	<i>Not relevant</i>
F.SECURE_DATA_MANAGER	<i>Relevant SF Used by SF.LCM.5 and SF.AC.1</i>
F.SECRET_DATA_MANAGER	<i>Relevant SF Used by SF.AC.1</i>
F.SYSTEM_MANAGER	<i>Not relevant</i>
F.CRYPTOGRAPHIC_OPERATIONS	<i>Relevant SF Used by SF.CF, SF.SM.1 and SF.SM.2</i>
F.MEMORY_ACCESS	<i>Not relevant</i>
F.MEMORY_CONTROLLER	<i>Not relevant</i>
F.INPUT/OUTPUT_LAYER	<i>Not relevant</i>
F.TRANSPORT_LAYER	<i>Not relevant</i>
F.CRYPTOGRAPHY_SERVICES	<i>Relevant SF Used by SF.CF, and SF.LCM.4</i>
F.SECURITY_CONFIGURATION	<i>Not relevant</i>
F.CPU_MANAGER	<i>Not relevant</i>

<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>72/97</b>
--	---

<b>IDEalCitiz 2.1.1 Fonctionnalités in [PLTF-ST]</b>	<b>Usage by TOE</b>
F.SECURITY_AUDIT	<i>Not relevant</i>
F.CRYPTOGRAPHIC_LIBRARY	<i>Not relevant</i>
F.INTEGRATED_CIRCUIT	<i>Relevant SF</i> Used by SF.ILTB.1

**Table 11: Compatibility between platform Functionalities and the composite ST**



The following tables specify the compatibility between SFRs of the platform ST and the composite ST. It indicates to what extent the IDEalCitiz 2.1.1 platform SFRs are used by the TOE to meet the security requirements of this composite ST.

IDEalCitiz 2.1.1-SFRs in [PLTF-ST]	Usage by TOE / Not used	References /Remarks
<b>1. Firewall Policy</b>		
FDP_ACC.2/FIREWALL Complete Access Control	The Firewall policy rules are indirectly used by the applet to prevent the <b>MICAO 1.3.69 on IDEalCitiz 2.1.1, BAC configuration</b> applet from accidentally changing the state of the JCRE.	-
FDP_ACF.1/FIREWALL Security Attribute based Access Control		
FDP_IFC.1/JCVM Subset Information Flow Control		
FDP_IFF.1/JCVM Simple Security Attributes		
FDP_RIP.1/OBJECTS Subset Residual Information Protection		
FMT_MSA.1/JCRE Management of Security Attributes		
FMT_MSA.1/JCVM Management of Security Attributes		
FMT_MSA.2/FIREWALL_JCVM Secure Security Attributes		
FMT_MSA.3/FIREWALL Static Attribute Initialisation		
FMT_MSA.3/JCVM Static Attribute Initialisation		
FMT_SMF.1 Specification of Management Functions		
FMT_SMR.1 Security roles		

**Table 12: Compatibility between platform SFRs and the composite ST – Firewall Policy**

<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>74/97</b>
--	---

IDealCitiz 2.1.1-SFRs in [PLTF-ST]	Usage by TOE / Used by Not used	Applet	References /Remarks
<b>2. Application Programming Interface</b> The following SFRs are related to the Java Card API			
FCS_CKM.1 Cryptographic Key Generation	Used by TOE for :		SF.CF
FCS_CKM.2 Cryptographic Key Distribution	Used to implement:		This functionality is not provided at the external interface of the TOE.
FCS_CKM.3 Cryptographic Key Access	Used to implement:		This functionality is not provided at the external interface of the TOE.
FCS_CKM.4 Cryptographic Key Destruction	Used by TOE for:		
FCS_COP.1 Cryptographic Operation:	Used by TOE for:		Chapter 7
FDP_RIP.1/ABORT Subset Residual Information Protection	Not directly used by TOE. TOE relies on this platform SFR.		-

<b>IDEalCitiz 2.1.1-SFRs in [PLTF-ST]</b>	<b>Usage by TOE / Used by Applet Not used</b>	<b>Reference s /Remarks</b>
	FDP_RIP.1 in this ST  A deselect by JCRE of Applet instance occurs in case of re-select of the Applet by re-issuing a SELECT BY NAME with ICAO AID. The IDEalCitiz 2.1.1 platform clears the transient memory after the applets deselect() method has been called.	
FDP_RIP.1/APDU Subset Residual Information Protection	Not directly used. TOE relies on this platform SFR.	-
FDP_RIP.1/bArray Subset Residual Information Protection	Not directly used. TOE relies on this platform SFR.	-
FDP_RIP.1/KEYS Subset Residual Information Protection	Not directly used by TOE's implementation of FDP_RIP.1. TOE relies on this platform SFR.	-
FDP_RIP.1/TRANSIENT Subset Residual Information Protection	Not directly used by TOE's implementation of FDP_RIP.1. TOE relies on this platform SFR.	-
FDP_ROL.1/FIREWALL Basic Rollback	Used by TOE during TA trust point update.	-

**Table 13: Compatibility between platform SFRs and the composite ST – Application Programming Interface**

<b>IDEalCitiz 2.1.1-SFRs in [PLTF-ST]</b>	<b>Usage by TOE / Not used</b>	<b>Reference s /Remarks</b>
<b>3. Card Security Management</b>		
FAU_ARP.1 Security Alarms	Not directly used	SF.ILTB.1 <sup>1</sup>
FDP_SDI.2 Stored Data Integrity Monitoring and Action	Not directly used.	SF.ILTB.1
FPR_UNO.1 Unobservability	Not directly used.	SF.ILTB.1
FPT_FLS.1 Failure with Preservation of Secure State	Not directly used.	SF.ILTB.1
FPT_TDC.1 Inter-TSF basic TSF data consistency	Not used.	-

**Table 14: Compatibility between platform SFRs and the composite ST – Card Security Management**

<sup>1</sup>SFR indirectly supports FMT\_LIM.1, FMT\_LIM.2, and FPT\_FLS.1.

<b>SECURITY TARGET LITE</b>	Ref.: 2017_2000024546
<b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Page: <b>76/97</b>

<b>IDEalCitiz 2.1.1-SFRs in [PLTF-ST]</b>	<b>Usage by TOE /</b>	<b>Reference s /Remarks</b>
<b>4. AID Management</b>		
This group consists of the SFRs related to the management of Application Identifiers.		
FIA_ATD.1/AID User Attribute Definition	Not directly used by TOE. Only used during TOE initialisation.	SF.LCM.2
FIA_UID.2/AID User Identification before any Action	Not directly used by TOE.	
FIA_USB.1/AID User-Subject Binding	Not directly used by TOE.	
FMT_MTD.1/JCRE Management of TSF Data	Not directly used by TOE.	
FMT_MTD.3/JCRE Secure TSF Data	Not directly used by TOE.	

**Table 15: Compatibility between platform SFRs and the composite ST – AID Management**

<b>IDEalCitiz 2.1.1-SFRs in [PLTF-ST]</b>	<b>Usage by TOE /</b>	<b>Reference s /Remarks</b>
<b>5. INSTG Security Functional Requirements</b>		
This group consists of the SFRs related to the installation of the applets, which addresses security aspects outside the runtime.		
FDP_ITC.2/Installer Import of User Data with Security Attributes	Not used	-
FMT_SMR.1/Installer Security roles		
FPT_FLS.1/Installer Failure with preservation of secure state		
FPT_RCV.3/Installer Automated recovery without undue loss		

**Table 16: Compatibility between platform SFRs and the composite ST – INSTG Security Functional Requirements**

IDealCitiz 2.1.1-SFRs in [PLTF-ST]	Usage by TOE / Not used	Reference s /Remarks
<b>6. ADELG Security Functional Requirements</b> This group consists of the SFRs related to the deletion of applets and/or packages, enforcing the applet deletion manager (ADEL) policy on security aspects outside the runtime.		
FDP_ACC.2/ADEL Complete access control	Not used	-
FDP_ACF.1/ADEL Security attribute based access control		
FDP_RIP.1/ADEL Subset residual information protection		
FMT_MSA.1/ADEL Management of security attributes		
FMT_MSA.3/ADEL Static attribute Initialisation		
FMT_SMF.1/ADEL Specification of Management Functions		
FMT_SMR.1/ADEL Security roles		
FPT_FLS.1/ADEL Failure with preservation of secure state		

**Table 17: Compatibility between platform SFRs and the composite ST – ADELG Security Functional Requirements**

IDealCitiz 2.1.1-SFRs in [PLTF-ST]	Usage by TOE / Not used	Reference s /Remarks
<b>7. ODELG Security Functional Requirements</b> This group describes the object deletion mechanism. This mechanism is triggered by the applet that owns the deleted objects by invoking a specific API method.		
FDP_RIP.1/ODEL Subset residual information protection	Not used by applet.	-
FPT_FLS.1/ODEL Failure with preservation of secure state	Not used by applet.	-

**Table 18: Compatibility between platform SFRs and the composite ST – ODELG Security Functional Requirements**

<b>SECURITY TARGET LITE</b>	Ref.: 2017_2000024546
<b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Page: <b>78/97</b>

<b>IDEalCitiz 2.1.1-SFRs in [PLTF-ST]</b>	<b>Usage by TOE /</b>	<b>Reference s /Remarks</b>
<b>8. CARG Security Functional Requirements</b>		
This group includes requirements for preventing the installation of packages that has not been byte code verified, or that has been modified after byte code verification.		
FCO_NRO.2/CM Enforced proof of origin	Not directly used.	-
FDP_IFC.2/CM Complete information flow control	The applet has passed byte code verifier.	
FDP_IFF.1/CM Simple security attributes		
FDP_UIT.1/CM Data exchange integrity		
FIA_UID.1/CM Timing of identification		
FMT_MSA.1/CM Management of security attributes		
FMT_MSA.3/CM Static attribute initialisation		
FMT_SMF.1/CM Specification of Management Functions		
FMT_SMR.1/CM Security roles		
FTP_ITC.1/CM Inter-TSF trusted channel		

**Table 19: Compatibility between platform SFRs and the composite ST – CARG Security Functional Requirements**

<b>IDEalCitiz 2.1.1-SFRs in [PLTF-ST]</b>	<b>Usage by TOE /</b>	<b>Reference s /Remarks</b>
<b>9. PACE Functional Requirements</b>		
FCS_CKM.2/PACE Cryptographic key distribution	Not directly used.	
FCS_CKM.3/PACE Cryptographic key access	Not directly used.	
FCS_COP.1/PACE Cryptographic operation	Not directly used.	

**Table 20: Compatibility between platform SFRs and the composite ST – PACE Functional Requirements**

<b>IDEalCitiz 2.1.1-SFRs in [PLTF-ST]</b>	<b>Usage by TOE /</b>	<b>Reference s /Remarks</b>
<b>10. OSG Security Functional Requirements</b>		
FPT_RCV.3/OS Automated recovery without undue loss	Not used	-
FPT_RCV.4/OS Function recovery	Not used	-
FPT_FLS.1/OS Failure with preservation of secure state	Not used	-
FPT_PHP.3/OS Resistance to physical attack	Not used	

**Table 21: Compatibility between platform SFRs and the composite ST - OSG Security Functional Requirements**

<b>IDEalCitiz 2.1.1-SFRs in [PLTF-ST]</b>	<b>Usage by TOE /</b>	<b>Reference s /Remarks</b>
<b>11. CardLifeCycleManagement Security Functional Requirements</b>		
FDP_ACC.1/CardLifeCycleManagement Subset Access Control	Used during TOE initialisation for installing pre-personalisation key set.  Not used by applet.	SF.LCM.2
FDP_ACF.1/CardLifeCycleManagement Security Attribute based Access Control	Used during TOE initialisation for adjusting GP state to SECURED.  Used by applet to move GP state to TERMINATED in case of physical detected attacks detected by applet. (see SFR FPT_PHP.3)	SF.LCM.2
FMT_MSA.1/CardLifeCycleManagement Management of Security Attributes	Not directly used.	-
FMT_MSA.3/CardLifeCycleManagement Static Attribute Initialisation	Not directly used.	-
FTP_ITC.1/CardLifeCycleManagement Inter-TSF trusted channel	Not directly used.	-

**Table 22: Compatibility between platform SFRs and the composite ST - LifeCycle Security Functional Requirements**

## 8.2 COMPATIBILITY BETWEEN THE COMPOSITE SECURITY TARGET AND THE PLATFORM SECURITY TARGET

The following mapping demonstrates the compatibility between the Composite Security Target (the document at hand) and the Platform Security Target [PLTF-ST] regarding security environments, security objectives, and security requirements. There is no conflict between security environments, security objectives, and security requirements of the Composite Security Target and the Platform Security Target.

IDEalCitiz 2.1.1 Definition	Pendent in this ST	Remarks
<b>Security objectives for the TOE</b>		
Platform objectives	Pendant in this ST with similar aim	Remarks
O.SID	-	No contradictions
O.FIREWALL	-	No contradictions
O.GLOBAL_ARRAYS_CONFID	-	No contradictions
O.GLOBAL_ARRAYS_INTEG	-	No contradictions
O.NATIVE	-	No contradictions
O.OPERATE	OT.Prot_Malfunction	No contradictions
O.REALLOCATION	-	No contradictions
O.RESOURCES	-	No contradictions
O.ALARM	-	No contradictions
O.CIPHER	OT.Sens_Data_Conf	No contradictions
O.PIN-MNGT	-	No contradictions
O.KEY-MNGT	OT.AC_Pers, OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof	No contradictions
O.TRANSACTION	-	No contradictions
O.DELETION	-	No contradictions
O.LOAD	-	No contradictions
O.INSTALL	-	No contradictions
O.CARD-MANAGEMENT	OT.Prot_Phys-Tamper	No contradictions
O.SCP.RECOVERY	-	No contradictions
O.SCP.SUPPORT	-	No contradictions
O.SCP.IC	OT.Prot_Phys-Tamper	No contradictions
O.BIO-MNGT	-	No contradictions
O.OBJ-DELETION	-	No contradictions
<b>Relevant threats of the Platform ST vs. threats of the Composite-ST.</b>		
Threats of Platform ST	According threats of comp. ST	
T.CONFID-APPLI-DATA	T.Read_Sensitive_Data,	No contradictions
T.CONFID-JCS-DATA	-	No contradictions



<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>81/97</b>
--	---

IDealCitiz 2.1.1 Definition	Pendent in this ST	Remarks
T.INTEG-JCS-DATA	-	No contradictions
T.INTEG-APPLI-DATA	T.Phys-Tamper, T.Forgery	No contradictions
T.INTEG-APPLI-CODE.LOAD	T.Phys-Tamper, T.Forgery	No contradictions
T.INTEG-APPLI-DATA.LOAD	T.Phys-Tamper, T.Forgery	No contradictions
T.CONFID-JCS-CODE	-	No contradictions
T.INTEG-APPLI-CODE	-	No contradictions
T.INTEG-JCS-CODE	-	No contradictions
T.APP_DATA_INTEGRITY	-	No contradictions
T.SID.1	-	No contradictions
T.SID.2	-	No contradictions
T.EXE-CODE.1	-	No contradictions
T.EXE-CODE.2	-	No contradictions
T.NATIVE	-	No contradictions
T.RESOURCES	-	No contradictions
T.DELETION	-	No contradictions
T.INSTALL	-	No contradictions
T.OBJ-DELETION	-	No contradictions
T.UNAUTH_CARD_MNGT	-	No contradictions
T.LIFE_CYCLE	-	No contradictions
T.UNAUTH_ACCESS	-	No contradictions
T.PHYSICAL	T.Phys-Tamper	No contradictions
<b>Assumptions (platform) significant for Composite-ST</b>		
Assumptions of Platform ST	Relevancy for Composite-ST	
A.APPLLET	Guidance of the Platform-Developer for the Applet Developer has to be applied	No contradiction to this ST
A.VERIFICATION	Guidance of the Platform-Developer for the Applet Developer has to be applied	No contradiction to this ST
A.PRODUCTION	Guidance of the Platform-Developer for the Applet Developer has to be applied	No contradiction to this ST
<b>Platform security objectives for the environment and relevancy for the Composite ST</b>		
OE of platform ST	Matching aspects in Composite-ST	Remarks
OE.CODE-EVIDENCE	-	No contradictions
OE.SECURITY-DOMAINS	-	No contradictions
OE.QUOTAS	-	No contradictions
OE.SHARE-CONTROL	-	No contradictions

SECURITY TARGET LITE	Ref.: 2017_2000024546
MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION	Page: 82/97

IDEalCitiz 2.1.1 Definition	Pendent in this ST	Remarks
OE.KEY_GENERATION	-	No contradictions
OE.PRODUCTION	-	No contradictions
OE.VERIFICATION	Guidance of the Platform-Developer for the Applet Developer has to be applied	No contradictions
OE.APPLLET	-	No post-issuance of the applet is intended. No contradictions

**Platform organizational security policies for the environment and relevancy for the Composite ST**

OSP of platform ST	Matching aspects in Composite-ST	Remarks
OSP.VERIFICATION	Guidance of the Platform-Developer for the Applet-Developer and recomandations related to the isolation property of the platform have to be applied in the application code  Not contradictory to any threats of composite ST	No contradictions
OSP.SECURITY_DOMAINS	No correspondance Not contradictory to any threats of composite ST	No contradictions
OSP.QUOTAS	No correspondance Not contradictory to any threats of composite ST	No contradictions
OSP.KEY_GENERATION	Guidance of the Platform-Developer for the Applet-Developer and recomandations related to the Key Generation have to be applied in the application code  Not contradictory to any threats of composite ST	No contradictions
OSP.SHARE-CONTROL	Guidance of the Platform-Developer for the Applet-Developer and recomandations related to the Shareable interface functionality have to be applied in the application code  Not contradictory to any threats of composite ST	No contradictions

**Table 23: Compatibility between platform and composite ST****8.3 COMPATIBILITY OF ASSURANCE REQUIREMENTS**

The level of assurance of the:

- TOE is EAL4 augmented with ALC DVS.2
- Platform is EAL5 augmented with ALC DVS.2 and AVA VAN.5

This shows that the Assurance Requirements of the TOE matches the Assurance Requirements of the underlying Platform.

## 9 ANNEX

### Glossary

Term	Definition
<i>Accurate Terminal Certificate</i>	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [TR-03110-1].
<i>Advanced Inspection Procedure (with PACE)</i>	A specific order of authentication steps between a travel document and a terminal as required by [ICAO-SAC], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SOD and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
<i>Agreement</i>	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
<i>Active Authentication</i>	Security mechanism defined in [ICAO-9303]. Option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of organization.
<i>Application note</i>	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
<i>Audit records</i>	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialisation Data and Pre-personalization Data.
<i>Authenticity</i>	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
<i>Basic Access Control</i>	Security mechanism defined in [ICAO-9303] by which means the MRTD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
<i>Basic Inspection System (BIS)</i>	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.
<i>Biographical data (bio data).</i>	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa.
<i>Biometric reference data</i>	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.

<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>85/97</b>
--	---

Term	Definition
<i>Card Access Number (CAN)</i>	Password derived from a short number printed on the front side of the data-page.
<i>Certificate chain</i>	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
<i>Counterfeit</i>	An unauthorized copy or reproduction of a genuine security document made by whatever means.
<i>Country Signing CA Certificate (CCSCA)</i>	Self-signed certificate of the Country Signing CA Public Key ( $K_{Pu\_CSCA}$ ) issued by CSCA stored in the inspection system.
<i>Country Signing Certification Authority (CSCA)</i>	<p>An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI.</p> <p>The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO-9303], 5.5.1.</p> <p>The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-1].</p>
<i>Country Verifying Certification Authority (CVCA)</i>	<p>An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [TR-03110-1].</p> <p>Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this ST.</p> <p>The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO-9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-1].</p>
<i>Current date</i>	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.

Term	Definition
<i>CV Certificate</i>	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
<i>CVCA Certificate</i> <i>link</i>	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
<i>Document Access Derivation Algorithm</i> <i>Basic Key</i>	The [ICAO-9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
<i>Document Details Data</i>	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
<i>Document Access Keys</i> <i>Basic</i>	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [ICAO-9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
<i>Document Security Object (SO<sub>D</sub>)</i> <i>Object</i>	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [ICAO-9303]
<i>Document Signer (DS)</i>	<p>An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication.</p> <p>A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [TR-03110-1] and [ICAO-9303].</p> <p>This role is usually delegated to a Personalisation Agent.</p>
<i>Document Verifier (DV)</i>	<p>An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [TR-03110-1].</p> <p>Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this ST.</p> <p>There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the</p>

<p><b>SECURITY TARGET LITE</b></p> <p><b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b></p>	<p>Ref.: 2017_2000024546</p> <p>Page: <b>87/97</b></p>
---	--

Term	Definition
	<p>respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer’s privacy policy) <sup>1 2</sup></p>
<i>Eavesdropper</i>	<p>A threat agent with low attack potential reading the communication between the MRTD’s chip and the inspection system to gain the data on the MRTD’s chip.</p>
<i>Enrolment</i>	<p>The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO-9303]</p>
<i>ePassport application</i>	<p><u>[PP-SAC] definition</u>  A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [TR-03110-1].</p> <p><u>[PP-EAC] definition</u>  Non-executable data defining the functionality of the operating system on the IC as the travel document’s chip. It includes</p> <ul style="list-style-type: none"> <li>• the file structure implementing the LDS [ICAO-9303],</li> <li>• the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and</li> <li>• the TSF Data including the definition the authentication data but except the authentication data itself.</li> </ul>
<i>Extended Access Control</i>	<p>Security mechanism identified in [ICAO-9303] by which means the MTRD’s chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.</p>
<i>Extended Inspection System (EIS)</i>	<p>A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.</p>
<i>Forgery</i>	<p>Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.</p>
<i>Global Interoperability</i>	<p>The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO-9303]</p>

<sup>1</sup> The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the current ST in order to reflect an appropriate relationship between the parties involved.

<sup>2</sup> Existing of such an agreement may be technically reflected by means of issuing a CCVCA-F for the Public Key of the foreign CVCA signed by the domestic CVCA.



Term	Definition
<i>IC Dedicated Software</i>	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
<i>IC Dedicated Support Software</i>	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
<i>IC Dedicated Test Software</i>	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
<i>IC Embedded Software</i>	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
<i>IC Identification Data</i>	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
<i>Impostor</i>	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document.
<i>Improperly documented person</i>	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO-9303]
<i>Initialisation</i>	Process of writing Initialisation Data (see below) to the TOE (TOE life-cycle, Phase 2 Manufacturing, Step 3).
<i>Initialisation Data</i>	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
<i>Inspection</i>	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO-9303]
<i>Inspection system (IS)</i>	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
<i>Integrated circuit (IC)</i>	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
<i>Integrity</i>	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
<i>Issuing Organization</i>	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303]
<i>Issuing State</i>	The Country issuing the MRTD. [ICAO-9303]
<i>Logical Data Structure (LDS)</i>	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion



Term	Definition
	technology used is the MRTD's chip.
<i>Logical travel document</i>	Data of the travel document holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) <ol style="list-style-type: none"> <li>1. personal data of the travel document holder</li> <li>2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),</li> <li>3. the digitized portraits (EF.DG2),</li> <li>4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and</li> <li>5. the other data according to LDS (EF.DG5 to EF.DG16).</li> <li>6. EF.COM and EF.SOD</li> </ol>
<i>Machine readable travel document (MRTD)</i>	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO-9303]
<i>Machine readable zone (MRZ)</i>	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO-9303]  The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
<i>Machine-verifiable biometrics feature</i>	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO-9303]
<i>Manufacturer</i>	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
<i>Metadata of a CV Certificate</i>	Data within the certificate body (excepting Public Key) as described in [TR-03110-1]. The metadata of a CV certificate comprise the following elements: <ul style="list-style-type: none"> <li>- Certificate Profile Identifier,</li> <li>- Certificate Authority Reference,</li> <li>- Certificate Holder Reference,</li> <li>- Certificate Holder Authorisation Template,</li> <li>- Certificate Effective Date,</li> <li>- Certificate Expiration Date.</li> </ul>
<i>Optional biometric reference data</i>	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.

Term	Definition
<i>Password Authenticated Connection Establishment (PACE)</i>	A communication establishment protocol defined in [ICAO-SAC]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password $n$ ). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
<i>PACE passwords</i>	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO-SAC],
<i>Passive authentication</i>	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
<i>Personalisation</i>	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. paragraph 1.4.3.3, TOE life-cycle, Phase 3, Step 6).
<i>Personalisation Agent</i>	<p>An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:</p> <ul style="list-style-type: none"> <li>(i) establishing the identity of the travel document holder for the biographic data in the travel document,</li> <li>(ii) enrolling the biometric reference data of the travel document holder,</li> <li>(iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [TR-03110-1],</li> <li>(iv) writing the document details data,</li> <li>(v) writing the initial TSF data,</li> <li>(vi) signing the Document Security Object defined in [ICAO-9303] (in the role of DS).</li> </ul> <p>Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.</p> <p>Generating signature key pair(s) is not in the scope of the tasks of this role.</p>
<i>Personalisation Data</i>	<p>A set of data incl.</p> <ul style="list-style-type: none"> <li>(i) individual-related data (biographic and biometric data) of the travel document holder,</li> <li>(ii) dedicated document details data and</li> <li>(iii) dedicated initial TSF data (incl. the Document Security Object).</li> </ul> <p>Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.</p>

<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>91/97</b>
--	---

Term	Definition
<i>Personalization Agent Authentication Information</i>	TSF data used for authentication proof and verification of the Personalisation Agent.
<i>Personalisation Agent Key</i>	Symmetric cryptographic key or key set (MAC, ENC) used <ul style="list-style-type: none"> <li>(i) by the Personalisation Agent to prove his identity and get access to the logical travel document and</li> <li>(ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE.</li> </ul>
<i>Physical part of the travel document</i>	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) <ul style="list-style-type: none"> <li>1. biographical data,</li> <li>2. data of the machine-readable zone,</li> <li>3. photographic image and</li> <li>4. other data.</li> </ul>
<i>Pre-personalization</i>	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (TOE life-cycle, Phase 2, Step 5)
<i>Pre-personalization Data</i>	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair and Chip Life-Cycle Production data (CPLC data).
<i>Pre-personalised travel document's chip</i>	Travel document's chip equipped with a unique identifier.
<i>Receiving State</i>	The Country to which the MRTD holder is applying for entry. [ICAO-9303]
<i>Reference data</i>	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
<i>RF-terminal</i>	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
<i>Secondary image</i>	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means [ICAO-9303].
<i>Secure messaging in encrypted /combined mode</i>	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
<i>Service Provider</i>	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
<i>Skimming</i>	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
<i>Standard Inspection Procedure</i>	A specific order of authentication steps between an travel document and a terminal as required by [ICAO-SAC], namely <ul style="list-style-type: none"> <li>(i) PACE or BAC and</li> <li>(ii) Passive Authentication with SO<sub>D</sub>.</li> </ul>

<b>SECURITY TARGET LITE</b> <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b>	Ref.: 2017_2000024546 Page: <b>92/97</b>
--	---

Term	Definition
	SIP can generally be used by BIS-PACE and BIS-BAC.
<i>Terminal</i>	<p>A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter.</p> <p>In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE.</p> <p>Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).</p>
<i>Terminal Authorization</i>	Intersection of the Certificate Holder Authorizations of the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be valid for the Current Date.
<i>Terminal Authorisation Level</i>	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
<i>TOE tracing data</i>	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
<i>Travel document</i>	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO-9303] (there "Machine readable travel document").
<i>Travel document (electronic)</i>	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: <i>ePassport</i> .
<i>Travel Document Holder</i>	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
<i>Travel document's Chip</i>	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO-9303], sec III.
<i>Traveler</i>	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
<i>TSF data</i>	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC-1]).
<i>Unpersonalised travel document</i>	The travel document that contains the travel document chip holding only Initialisation Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
<i>User data</i>	All data (being not authentication data) <ol style="list-style-type: none"> <li>(i) stored in the context of the ePassport application of the</li> </ol>

Term	Definition
	<p>(ii) travel document as defined in [5] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE.</p> <p>CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC-1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC-2]).</p>
<i>Verification</i>	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO-9303]
<i>Verification data</i>	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

## Abbreviations

CC	Common Criteria, see [CC]
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
SEF	Security Enforcing Functions
SOF	Strength Of Function
TOE	Target of Evaluation
TSF	TOE Security Functions

## References

Reference	Description
[AIS20V1]	Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 2.0, 02.12.1999
[AIS20V2]	Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitätsklassen und Evaluationsmethodologie fuer deterministische Zufallszahlengeneratoren, Version 2.1, 02.12.2011, Bundesamt fuer Sicherheit in der Informationstechnik.
[AIS31]	BSI - Functionality classes and evaluation methodology for physical random number generators AIS31, Version 3, 2013-05-15
[ANSSI-FRP256V1]	Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français NOR: PRMD1123151V (Le 18 avril 2012)- ANSSI ( <a href="http://www.ssi.gouv.fr/">http://www.ssi.gouv.fr/</a> ).
[BAC-PP]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1:Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2:Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
[CEM]	The Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
[DH]	Rescorla, Eric, RFC 2631: Diffie-Hellman key agreement method, 1999
[EAC-PP-V2]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012, Version 1.3.2, December 5 <sup>th</sup> 2012, BSI
[ICAO-9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, Version Sixth Edition, 2006 (this includes the latest supplemental for ICAO Doc 9303 which also should be considered)
[ICAO-SAC]	International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.02, 8 March 2011
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11
[ISO15946-1]	ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002
[ISO15946-2]	ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.



Reference	Description
[ISO15946-3]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[ISO18013-3]	ISO/IEC 18013-3: Information technology — Personal identification — ISO-compliant driving licence. Part 3: Access control, authentication and integrity validation, 2009-03-01 Including ISO/CEI 18013-3/AC1:2011, TECHNICAL CORRIGENDUM 1, Published 2011-12-01
[ISO7816]	ISO/IEC 7816: Identification cards — Integrated circuit cards, Version Second Edition, 2008
[ISO9796-2]	ISO/IEC 9796-2: 2002, Information Technology - Security Techniques - Digital Signature Schemes giving message recovery - Part 2: Integer factorization based mechanisms
[ISO9797]	ISO/IEC 9797-1:1999, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.
[JAVA-3.0.1]	Application Programming Interface Java Card(tm) Platform, Version 3.0.1, Classic Edition, May 2009, Sun Microsystems, Inc.
[PLTF-PRE]	2014_2000003597 - PRE - IDEalCitiz_v2_1 - Preparative Procedures
[PLTF-ST]	2014_0000002183 Security Target -IDEalCitiz 2.1.1 open platform
[PLTF-OPE]	2014_200004459 - OPE - IDEalCitiz_v2_1 - Operational User Guidance
[KS2011]	A proposal for: Functionality classes for random number generators, Version 2.0, September 18, 2011 - W. Killmann, W. Schindler
[NIST-180-4]	NIST. FIPS 180-4, Secure Hash Standard, February 2011.
[NIST-186-3]	NIST. Digital Signature Standard (DSS), FIPS 186-3, 2009
[NIST-197]	NIST. Specification for the Advanced Encryption Standard (AES), FIPS PUB 197, 2001
[NIST-800-38B]	NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, 2005
[PACE-PP]	Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011, Version 1.0, 2 <sup>nd</sup> November 2011, BSI
[RFC-5639]	Lochter, Manfred; Merkle, Johannes. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, 2010
[RSA-PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[SIC-PP]	Security IC Platform Protection Profile; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007, Version 1.0, June 2007 – BSI
[ST-SAC-EAC]	2016_2000021669 - Security Target MICA0 on IDEalCitiz 2.1.1, SAC-EAC configuration



<p><b>SECURITY TARGET LITE</b>  <b>MICAO 1.3.69 ON IDEALCITIZ 2.1.1 - BAC CONFIGURATION</b></p>	<p>Ref.: 2017_2000024546  Page: <b>97/97</b></p>
---	--

Reference	Description
[ST-IC]	<p>Infineon, Security Target Lite, M7892 B11, Recertification, Including optional Software Libraries RSA - EC - SHA- 2 - Toolbox, Common Criteria CC v3.1 EAL6 augmented (EAL6+), version 0.3 as of 2015-10-13</p> <p>Security Target M7893 B11 Including optional Software Libraries RSA - EC - SHA-2 - Toolbox, Version: 0.2, Date: 31-08-2015, Published by Infineon Technologies AG</p>
[CR-IC]	<p>BSI, Certification Report, BSI-DSZ-CC-0782-V2-2015 for Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware), 03-11-2015</p> <p>BSI, Certification Report, BSI-DSZ-CC-0879-V2-2015 for Infineon Security Controller M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006, SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware), 13-11-2015</p>
[TR-02102]	TR-02102 Technische Richtlinie Kryptographische Algorithmen und Schlüssellängen, Version 2013.02, January 9 <sup>th</sup> 2013 by BSI
[TR-03110-1]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents -Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012 by BSI
[TR-03110-3]	TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents - Part 3: Common Specifications, version 2.10, 2012-03-07 by BSI
[TR-03111]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009