IDEMIA

CombICAO Applet in BAC and CA Configuration on Cosmo v9

Public Security Target

DOCUMENT MANAGEMENT

Business Unit – Department	**PSI**
Document type	**Public FQR**
Document Title	**CombICAO Applet in BAC and CA Configuration on Cosmo v9 Public Security Target**
FQR No	**110 9316**
FQR Issue	**1**

DOCUMENT REVISION

Date	Revision	Modification
14/10/2019	1.0	**Creation from full ST**

TABLE OF CONTENTS

GENERAL

Introduction

This public security target describes the security needs induced by the CombICAO Applet product in BAC and CA configuration (Active authentication protocol is not supported by the TOE) on IDEMIA underlying Java Card *ID-ONE Cosmo V9 Essential*, see 1.1.2 .

The objectives of this Security Target are:

- To describe the Target of Evaluation (TOE), its life cycle and to position it in the smart card life cycle,
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the platform active phases,
- To describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the product active phases,
- To specify the security requirements which include the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment,
- To describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements,

To present evidence that this ST is a complete and cohesive set of requirements that the TOE provides on an effective set of IT security countermeasures.

Product overview

The product is designed to support the following usages:

1. **eMRTD as per [ICAO_9303] and European provisions [TR_03110]; scope of the current ST**
2. ISO compliant driving license as per [ISO/IEC_18013] and [ISO/IEC_19446]; (out of the scope of the current ST)
3. digital identity and electronic services; (out of the scope of the current ST)

It is achieved thanks to a flexible design allowing to “build” during personalization of the applet the required application(s) by configuring accordingly:

- the file system;
- authentication protocols;
- the user authentication credentials;
- access conditions on files.

The product can be personalized to support an eMRTD application compliant with [ICAO_9303] and European provisions [TR_03110].

The TOE can be configured in four configurations ways.
However, The current ST addresses CombICAO Applet in eMRTD configuration 1) below.

1) CombICAO Applet product in **BAC** configuration with **CA**,
2) CombICAO Applet product in **EAC** configuration,
3) CombICAO Applet product in **EAC** with **PACE** configuration,
4) CombICAO Applet product in **PACE** configuration with **CA**.

1 ST INTRODUCTION

1.1 Public ST reference and TOE reference

1.1.1 ST reference

Title	CombICAO Applet in BAC and CA configuration on Cosmo V9 - Public Security Target
Version	1
Reference	FQR 110 9316
Authors	IDEMIA
Certification Body	NSCIB
CC version	3.1 revision 5
EAL	EAL4 augmented with: ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, and ATE_DPT.3
PP	See [PP_BAC]

Table 1 - ST reference

1.1.2 TOE reference

Developer name	IDEMIA
Product name	CombICAO Applet
TOE name	CombICAO Applet in BAC and CA configuration on ID-ONE Cosmo V9 Essential
TOE identification	SAAAAR code: *203297*
Name of Platform	ID-One Cosmo V9 Essential
Platform identification	089233
Platform certification	[PTF_CERT]
Guidance documents	[Applet_Perso_Guide] and [Applet_User_Guide] [PTF_AGD_OPE], [PTF_AGD1], [PTF_AGD2] [PTF_AGD_PRE] and [PTF_AGD_SEC_AC]

Table 2 - TOE reference

In order to assure the authenticity of the card, the product identification shall be verified by analyzing the response of the command GET DATA, see section 4 of [Applet_Perso_Guide]

1.2 TOE overview

1.2.1 Usage and major security features of the TOE

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

The MRTD is viewed as unit of

(a) the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
  (1) the biographical data on the biographical data page of the passport book,
  (2) the printed data in the Machine-Readable Zone (MRZ) and
  (3) the printed portrait.

(b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
  (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  (2) the digitized portraits (EF.DG2),
  (3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
  (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 methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO_9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO_9303].

The Chip Authentication defined in [TR_03110] is a security feature which is optionally supported by the TOE. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

This TOE addresses the Chip Authentication as an alternative to the Active Authentication stated in [ICAO_9303].

During the prepersonalization and personalization, the Personalisation Agent, once authenticated, gets the rights (access control) for (1) reading and writing data,(2) instantiating the application, and (4) writing of personalization data. The Personalisation Agent can so create the file structure (MF / ADF) required for this configuration.

Mutatis mutandis, the TOE may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446 supporting BAP-1 (the same protocol as BAC but used in the context of driving license), AA and CA, as both applications (MRTD and IDL) share the same protocols and data structure organization. Therefore, in the rest of the document, the word "MRTD" MAY be understood either as a MRTD in the sense of ICAO, or a driving license compliant to ISO/IEC 18013 or ISO/IEC TR 19446 depending on the targeted usage envisioned by the issuer.

The table below indicates how terms and concept present in the current document shall be read when considering the TOE to be an ISO driving license:

MRTD	ISO driving licence
MRTD	IDL
ICAO	ISO/IEC
ICAO 9303	ISO/IEC 18013 or ISO/IEC TR 19446
BAC	BAP-1
DG3	DG7
DG4	DG8
DG15	DG13
MRZ	MRZ or SAI (Scanning area identifier)
Traveler	Holder

NB: the ISO driving license is out of the scope of the current ST and not evaluated.

1.2.2 TOE type

The TOE is the contactless and/or contact integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control and the Chip Authentication according to [ICAO_9303].

The TOE comprises at least:

- the circuitry of the MRTD's chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application,
- the associated guidance documentation.

Note: The antenna is not part of the TOE as it does not have any impact on the security.

1.2.3 Required non-TOE hardware/Software/firmware

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.

Note: In particular, the TOE may be used in contact mode, without any inlay or antenna

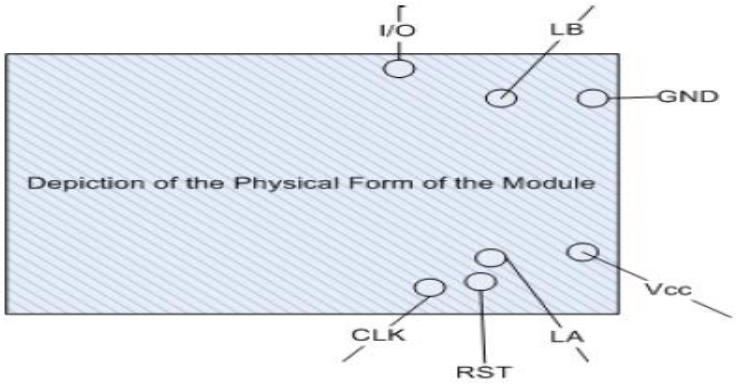
1.3 TOE description

1.3.1 Physical scope of the TOE

The TOE is physically made up of several components hardware and software.
Once constructed, the TOE is a bare microchip with its external interfaces for communication.
The physical medium on which the microchip is mounted is not part of the target of evaluation as it does not alter nor modify any security functions of the TOE.

The TOE may be used on several physical medium within an inlay, or eCover; in a plastic card are not part of the TOE.

The physical form of the module is depicted in Figure below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the following figure



1.3.2 TOE delivery

The TOE is composed of:

- Circuitry of the MRTD's chip (the IC) : see [IC_CERT]

CC ID
IFX_CCI_000005 IFX_CCI_000008 IFX_CCI_000014

- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software ID-ONE Cosmo V9 Essential: see [ST_PTF] and [PTF_CERT]
- CombICAO application: the application can be delivered as part of the OS and loaded in the flash or as Cap-file that can be loaded using the GP-mechanisms implemented
- Associated guidance documentation (delivered in electronic version)

This Public ST Lite version will also be provided as a guidance document along with above-mentioned documents.

TOE Component	Identification	Form Factor of Delivery	Delivery method
CombICAO applet for MRTD	*203297*	ID1 or ID3 Passport booklets ID1 cards or ID3 holder pages Antenna[1] inlays Chip in modules on a reel	CPS tool is used in the case of an Image delivery. Otherwise, trusted courier is used.
Personalizing Agent	[Applet_Perso_Guide]	Electronic doc	PGP-encrypted parts on USB or CD media, off-line registered distribution by trusted courier
End User of the TOE	[Applet_User_Guide]		
Underlying platform guidance	[PTF_AGD_OPE] [PTF_AGD1] [PTF_AGD2] [PTF_AGD_SEC_AC] [PTF_AGD_PRE]		

Form factor and Delivery Preparation:

1. As per the Software Development Process of IDEMIA, upon completion of development activities, particular applet will be uploaded into CPS in CAP file format. Before uploading, the applet will be verified through Oracle verifier and IDEMIA verifier.
2. During Release for Sample as project milestone, status of the applet in CPS will be changed into “Pilot version” to be used further for manufacturing samples.
3. During Software Delivery Review as the final R&D project milestone, status of the applet in CPS will be changed into “Industrial release” to be used further for mass production.

[1] The inlay production including the application of the antenna is not part of the TOE

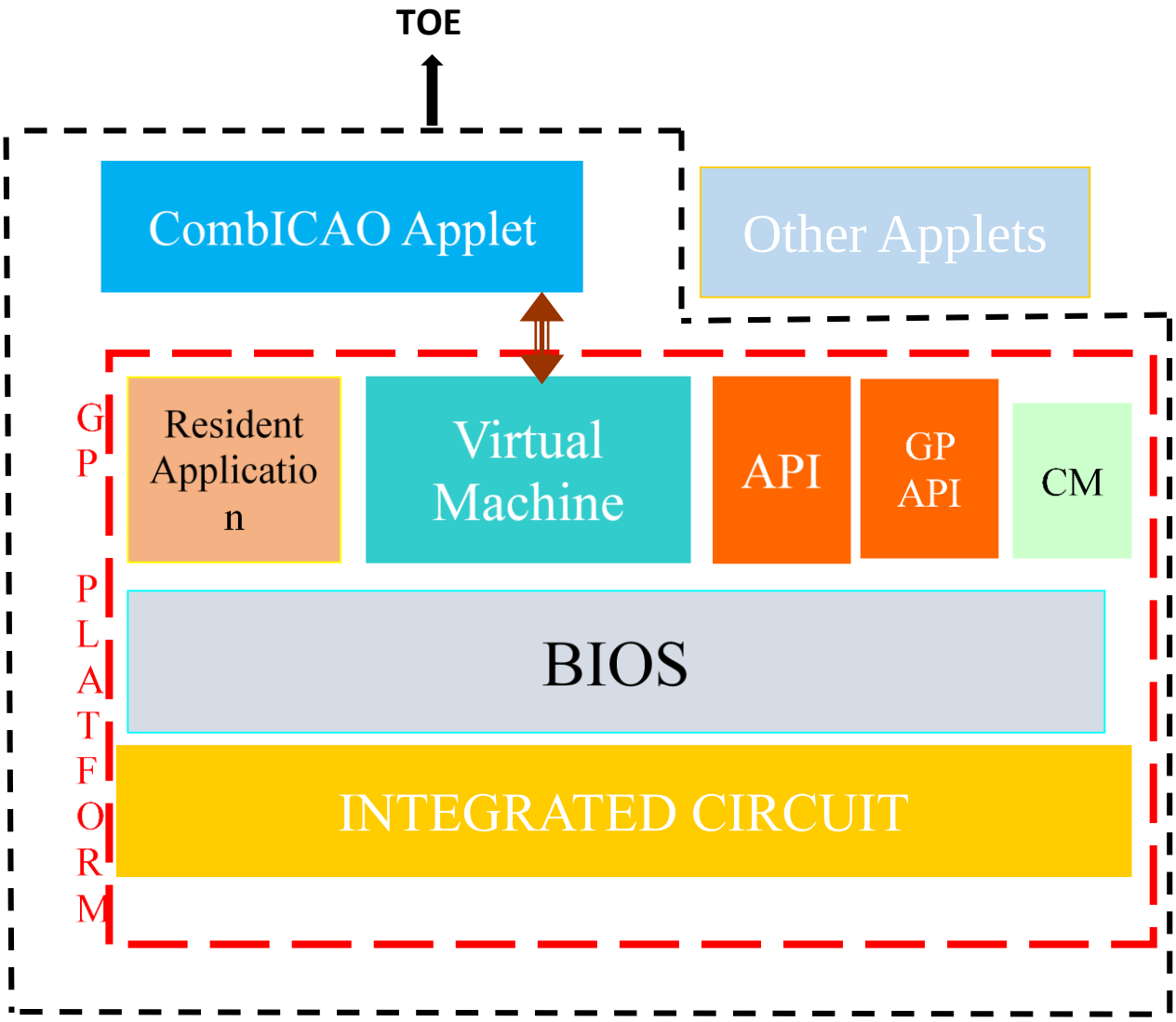


Figure 1: TOE Boundaries

1.3.3 Logical scope of the TOE

The TOE is a smartcard, composed of:

- IC,
- Javacard Open Platform (OS) and
- CombICAO application (data storage file structure)

The TOE scope encompasses the following features:

- Basic Access Control, see 1.3.4.2
- Chip Authentication, see 1.3.4.1
- Prepersonalization phase
- Personalisation phase

The prepersonalization and personalization are performed by the Pre-Personalization Agent and personalization Agent, respectively, which controls the TOE. All along this phase, the TOE is self-protected, as it requires the authentication of the Personalisation Agent prior to any operation. By being authenticated, the Pre-Personalization Agent/Personalisation Agent, respectively, gets the rights (access control) for (1) reading and writing data,(2) instantiating the application, and (4) writing of personalization data. The Personalisation Agent can so create the file structure (MF / ADF) required for this configuration

1.3.4 Authentication Protocols

1.3.4.1 Chip Authentication (**CA**)

The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip.
The protocol establishes Secure Messaging between an MRTD chip and a terminal based on a static key pair stored on the MRTD chip. Chip Authentication is an alternative to the optional ICAO Active Authentication (AA protocol is not supported by the TOE), i.e. it enables the terminal to verify that the MRTD chip is genuine but has two advantages over the original protocol:
Challenge Semantics are prevented because the transcripts produced by this protocol are non-transferable.
Besides authentication of the MRTD chip this protocol also provides strong session keys.

The protocol in version 1 provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys.

The protocol in Version 2 provides explicit authentication of the MRTD chip by verifying the authentication token and implicit authentication of the stored data by performing Secure Messaging using the new session keys.

The TOE addresses the Chip Authentication version 1 part of the EACv1 procedure defined in [TR_03110].

1.3.4.2 Basic Access Control (**BAC**)

It is related to BAC mechanism as defined in [ICAO_9303].

The protocol for Basic Access Control is specified by [ICAO_9303] Basic Access Control checks that the terminal has physical access to the MRTD's data page. This is enforced by requiring the terminal to derive an authentication key from the optically read MRZ of the MRTD. The protocol for Basic Access Control is based on ISO/IEC 11770-2 key establishment mechanism 6. This protocol is also used to generate session keys that are used to protect the confidentiality (and integrity) of the transmitted data.
The Basic Access Control (BAC) is a security feature that is supported by the TOE. The inspection system reads the printed data in the MRZ (for MRTD),authenticates itself as inspection system by means of keys derived from MRZ data. After successful 3DES based authentication, the TOE provides read access to data requiring BAC rights by means of a private communication (secure messaging) with the inspection system.

The purpose of this mechanism is to ensure that the holder gives access to the IS to the logical MRTD (data stored in the chip); It is achieved by a mutual authentication.

Once the mutual authentication is performed, a secure messaging is available to protect the communication between the chip and the IS.

This table lists the supported configurations for BAC protocol:

Configuration	Key Algo	Key Length	Hash Algo	MAC Algo
BAC	3DES 2Key	16-bytes	SHA-1	Retail MAC

Table 1: BAC Configuration

1.3.5 Machine Readable Travel Document (MRTD)

The MRTD is a complete set of commands, which allows the management of MRTD data in the Operational Use phase (data management and authentication process under MRTD ADF).

1.3.6 TOE life cycle

1.3.6.1 Life cycle overview

The following table presents the TOE roles and the corresponding subject:

Roles		***Subject***
IC developer		Infineon (IFX)
TOE developer		IDEMIA
Manufacturer	IC manufacturer	IFX
	MRTD packaging responsible	IDEMIA or another agent
		IDEMIA
	Embedded software loading responsible	IDEMIA
	Pre Personalization (Manufacturer role)	IDEMIA or another agent
Personalization Agent		IDEMIA or another agent

Table 2 Roles identification on the life cycle

Several life cycles are available, depending when the Flash Code is loaded.
The following tables present the subjects following TOE life cycle steps in accordance with the standard smart card life cycle [PP_IC], and describe for each of them, (1) the TOE delivery point and (2) the assurance coverage:

The TOE life cycle in the following figure distinguishes stages for development, production, preparation and operational use in accordance with the standard smart card life cycle [PP_IC].

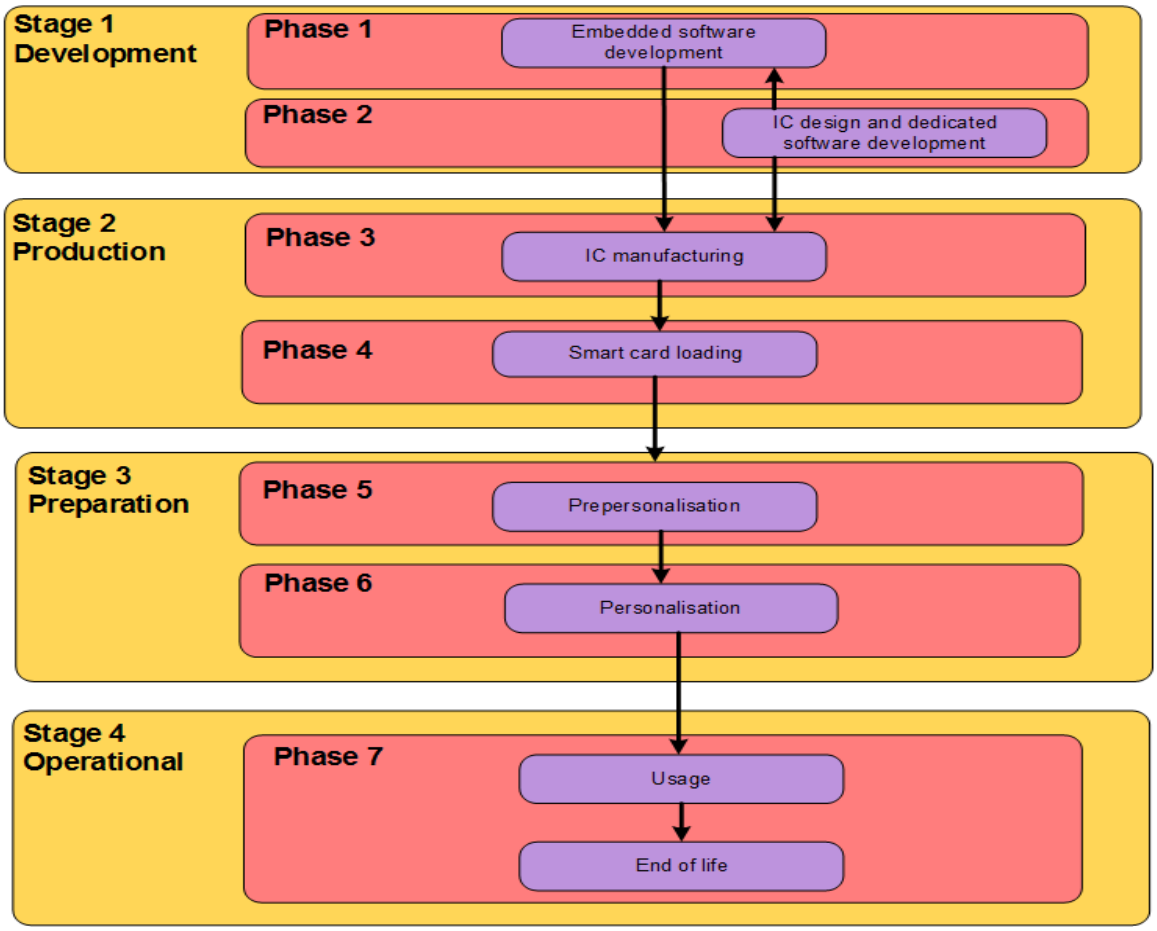


Figure 2 – Life cycle Overview

1.3.7 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Javacard Open Platform components and CombICAO applet)
- Phase 2: IC Development

The IC Embedded Software Developer is in charge of the specification, development and validation of the software (Javacard Open Platform and CombICAO applet).

The IC Developer designs the IC, develops the IC dedicated software and provides information, software or tools to the IC embedded software developer.

Roles, actors, sites and coverage for this environment of the product life-cycle are listed in the table below:

Role	Actor	Site	Covered by
CombICAO Applet Developer	IDEMIA	MANILA and Courbevoie R&D sites	ALC
Platform Developer	IDEMIA	IDEMIA R&D sites Refer to [PTF_CERT]	ALC
IC Developer	Infineon	Infineon R&D sites Refer to [PTF_CERT]	ALC

1.3.8 Production Environment

In this environment, the following two phases take place:

- Phase 3: IC manufacturing
- Phase 4: Smart card loading

The IC manufacturer is responsible for producing the IC (manufacturing, testing, and initialisation). Depending on the intention:

- **(Option 1)** the developer sends the image (containing both the javacard platform and the CombICAO applet) to be flashed in the IC to the IC manufacturer in the phase 3.

Or

- **(Option 2)** the platform developer sends the image (containing only the javacard platform) to be flashed in the IC to the IC manufacturer in the phase 3. Once the javacard platform has been loaded, the package of CombICAO is securely delivered from the applet developer to the smart card loader. The cap file of the applet is then loaded (using GP) in the javacard platform by the smart card loader in phase 4 at IDEMIA audited site.

Or

- **(Option 3)** the developer sends the image (containing both the javacard platform and the CombICAO applet) to be loaded in Flash (using the loader of the IC) to the smart card loader in phase 4.

Several life cycles are available, depending when the Flash Code is loaded. The following tables present roles, actors, sites and coverage for this for this environment of the product life-cycle and describe for each of them the TOE delivery point.

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing both javacard platform and applet	manufacturer	IC manufacturer production plants [PTF_CERT]	ALC
Smart card loader	-	-	-	-
TOE Delivery Point				

Table 3 Image containing both javacard platform and applet is loaded at IC manufacturer (Option 1)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing only javacard Platform	IC manufacturer	IC manufacturer production plants Refer to [PTF_CERT]	ALC
Smart card loader	Cap file of the applet	IDEMIA	IDEMIA plant (Shenzhen, Haarlem, Vitré)	ALC
TOE Delivery Point				

Table 4 Cap file of CombICAO applet is loaded through the loader of the smart card (Option 2)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	-	-	-	-
TOE Delivery Point				
Smart card loader	Image containing only javacard and applet	IDEMIA or another agent	IDEMIA plants or others sites	AGD

Table 5 Image containing both javacard platform and applet is loaded after point of delivery (Option 3)

1.3.9 Preparation Environment

In this environment, the following two phases take place:

- Phase 5: Prepersonalisation of the applet
- Phase 6: Personalisation

The preparation environment may not necessarily take place in a manufacturing site, but may be performed anywhere. All along these two phases, the TOE is self-protected as it requires the authentication of the prepersonalisation agent or personalisation agent prior to any operation.

The CombICAO applet is prepersonalised and personalised according to [Applet_Perso_Guide].

At the end of phase 6, the TOE is constructed. These two phases are covered by [Applet_Perso_Guide] tasks of the TOE and [PTF_AGD_OPE] tasks of [PTF_CERT].

1.3.9.1 Operational Environment

The TOE is under the control of the User (Signatory and/or Administrator).

During this phase, the TOE may be used as described in AGD of the TOE.

This phase is covered by [Applet_User_Guide] tasks of the TOE and [PTF_AGD_OPE] tasks of [PTF_CERT].

2 Conformance claims

2.1 Common Criteria conformance

This Public Security Target (ST) claims conformance to the Common Criteria (CC) version 3.1 revision 5.

The conformance to the CC is claimed as follows:

CC	**Conformance Claim**
Part 1	Strict conformance
Part 2	Conformance with extensions: • FAU_SAS.1 *"Audit storage",* • FCS_RND.1 *"Random number generation",* • FMT_LIM.1 *"Limited capabilities",* • FMT_LIM.2 *"Limited availability",* • FPT_EMS.1 *"TOE Emanation",* • FIA_API.1[2] *"Authentication Proof of Identity",*
Part 3	Conformance with package EAL4 augmented[3] with: • ALC_DVS.2 *"Sufficiency of security measures"* defined in [CC_3], • ADV_FSP.5 *"Complete semi-formal functional specification with additional error information"* defined in [CC_3], • ADV_INT.2 *"Well-structured internals"* defined in [CC_3], • ADV_TDS.4 *"Semiformal modular design"* defined in [CC_3], • ALC_CMS.5 *"Development tools CM coverage"* defined in [CC_3], • ALC_TAT.2 *"Compliance with implementation standards"* defined in [CC_3], • ATE_DPT.3 *"Testing: modular design"* defined in [CC_3].

Table 3 – Common Criteria conformance claim

Remark:
For interoperability reasons it is assumed the receiving state cares for sufficient measures against eavesdropping within the operating environment of the inspection systems. Otherwise the TOE may protect the confidentiality of some less sensitive assets (e.g. the personal data of the TOE holder which are also printed on the physical TOE) for some specific attacks only against enhanced basic attack potential (AVA_VAN.3).

FPT_EMSEC.1 from [PP_BAC] has been renamed to FPT_EMS.1, in order to keep the SFR formatting.

2.2 Protection Profile conformance

2.2.1 Overview

This ST claims strict conformance to the following Protection Profile (PP):

Title	Protection Profile – Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP)
CC Version	3.1 (Revision 2)
Assurance Level	The minimum assurance level for this PP is EAL4 augmented
Version Number	1.10
Registration	BSI-CC-PP-0055

[2] FIA_API.1 has been added to this security target for the needs of the Chip Authentication Protocol.
3 This EAL and its augmentations correspond to an EAL5 + ALC_DVS.2 where AVA_VAN level is downgraded to AVA_VAN.3 following constraint of MRZ entropy described in [ICAO_9303].

Table 4 – Protection Profile conformance

This ST also addresses the Manufacturing and Personalization phases at TOE level (cf. section 1.2.3)
Additional functionalities
The additional functionality of the Chip Authentication v1 (CA) protocol available in operational use phase has been added to the TOE with:

- (i) additional threads (T.Configuration, T.Counterfeit)
- (ii) additional assumptions (A.Insp_Sys_Chip_Auth and A.Signature_PKI)
- (iii) additional objectives for the TOE (OT.Chip_Auth_Proof *and* OT.Configuration*)*
- (iv) additional objectives for the environment (OE.Auth_MRTD and OE.Exam_Chip_Auth)

The additions do not contradict any of the threats, assumptions, organizational policies, objectives or SFRs stated in the [PP_BAC] that covers the advanced security methods BAC in operational use phase.

3 Security problem definition

3.1 Assets

3.1.1 Logical MRTD data

The following table presents the assets of the TOE and their corresponding phase(s) according to section 1.2.3

Asset	Phase		
	5	6	7
Personal Data	×	✓	✓
Biometric Data	×	✓	✓
EF.COM	×	✓	✓
EF.SOD	×	✓	✓
CA_PK	×	✓	✓
CA_SK	×	✓	✓
Perso_K	×	✓	×
BAC_K	×	✓	✓
Session_K	✓	✓	✓
LCS	✓	✓	✓

Table 6 Assets of the TOE and their corresponding phase(s)

3.1.1.1 Personal Data

The Personal Data are the logical MRTD standard User Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16).

3.1.1.2 Biometric Data

The Biometric Data are the sensitive biometric reference data (EF.DG3, EF.DG4)[4].

3.1.1.3 EF.COM

The EF.COM is an elementary file containing the list of the existing elementary files (EF) with the user data.

3.1.1.4 EF.SOD

The elementary file Document Security Object is used by the inspection system for Passive Authentication of the logical MRTD.

3.1.1.5 Chip Authentication Public Key (CA_PK)

The Chip Authentication Public Key (contained in EF.DG14) is used by the inspection system for the Chip Authentication.

3.1.1.6 Chip Authentication Private Key (CA_SK)

The Chip Authentication Private Key is used by the application to process Chip Authentication.

[4] cf.[ICAO_9303] for accessing EF.DG3 and EF.DG4 under EAC

3.1.1.7 Personalization Agent keys (Perso_K)

This key set used for mutual authentication between the Personalization agent and the chip, and secure communication establishment.

3.1.1.8 BAC keys (BAC_K)

This key set used for secure communication establishment between the Terminal and the chip.

3.1.1.9 Secure Messaging session keys (Session_K)

Session keys are used to secure communication in confidentiality and authenticity.

3.1.1.10 TOE Life Cycle State (LCS)

This is the Life Cycle State related to the Prepersonalization, Personalisation and use phase of the application.

3.1.2 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 Subjects

3.2.1 Overview

The following table presents the assets of the TOE and their corresponding phase(s) according to §1.3.6 TOE description

Subject	Description	Phase				
		3	4	5	6	7
IC manufacturer (Manufacturer role)	§ 3.2.2	✓	×	×	×	×
MRTD packaging responsible (Manufacturer role)	§ 3.2.3	×	✓	×	×	×
Embedded software loading responsible (Manufacturer role)	§ 3.2.4	×	✓	×	×	×
Pre-personalization Agent (Manufacturer role)	§ 3.2.5	×	×	✓	×	×
Personalization Agent	§ 3.2.6	×	×	×	✓	×
Terminal	§ 3.2.7	×	×	✓	✓	✓
Inspection System	§ 3.2.8	×	×	×	×	✓
MRTD Holder	§ 3.2.9	×	×	×	×	✓
Traveler	§ 3.2.10	×	×	×	×	✓
Attacker	§ 3.2.11	✓	✓	✓	✓	✓

Table 7 Assets of the TOE and their corresponding phase(s)

3.2.2 IC manufacturer

This additional subject is a refinement of the role Manufacturer as described in [PP_BAC]. It is the manufacturer of the IC.

If the IC Manufacturer loads the TOE at phase 3, this subject is responsible for the embedded software downloading in the IC. This subject does not use Flash loader, even if it is embedded in the IC.

3.2.3 MRTD packaging responsible

This additional subject is a refinement of the role Manufacturer as described in [PP_BAC]. This subject is responsible for the combination of the IC with hardware for the contactless and/or contact interface.

3.2.4 Embedded software loading responsible

This additional subject is a refinement of the role Manufacturer as described in [PP_BAC]. This subject is responsible for the embedded software loading when the TOE is loaded by the OS loader in phase 4 before TOE delivery point This subject does not exist if the TOE is loaded by the IC Manufacturer . This subject used the Flash loader embedded in the IC.

3.2.5 Pre-personalization Agent

This additional subject is a refinement of the role Manufacturer as described in [PP_BAC]. This subject is responsible for the preparation of the card, i.e. creation of the MF and MRTD ADF. He also sets Personalization Agent keys.

3.2.6 Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling

the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (iv) signing the Document Security Object defined in [ICAO_9303].

3.2.7 Terminal

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

Note: as the TOE may also be used in contact mode, the terminal may also communicate using the contact interface.

3.2.8 Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System (BIS) (i) contains a terminal for the contactless communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

3.2.9 MRTD Holder

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

3.2.10 Traveler

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

3.2.11 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 Assumptions

3.3.1 **A.MRTD_Manufact** *"MRTD manufacturing on phase 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).

3.3.2 **A.MRTD_Delivery** *"MRTD delivery during phase 4 to 6"*

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

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

3.3.3 **A.Pers_Agent** *"Personalization of the MRTD's chip"*

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

3.3.4 **A.Insp_Sys** *"Inspection Systems for global interoperability"*

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO_9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

3.3.5 **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_9303], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

3.3.6 **A.Insp_Sys_Chip_Auth** *"Inspection Systems for global interoperability on chip authenticity"*

The Inspection System implements the following protocol to authenticate the MRTD's chip: Chip Authentication v1 as defined in [TR_03110].

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing 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. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism v1. The General Inspection System reads the logical travel document under BAC and performs the Chip Authentication v1 to verify the logical travel document and establishes a new secure messaging that is different from the BAC one.

3.3.7 **A.Signature_PKI** *"PKI for Passive Authentication"*

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which securely generates stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

3.4 Threats

3.4.1 **T.Chip_ID** *"Identification of MRTD's chip"*

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

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

Asset: Anonymity of user

3.4.2 **T.Skimming** *"Skimming the logical MRTD"*

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

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

Asset: confidentiality of logical MRTD data.

3.4.3 **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.

3.4.4 **T.Forgery** *"Forgery of data on MRTD's chip"*

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

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

Asset: authenticity of logical MRTD data.

3.4.5 **T.Abuse-Func** *"Abuse of Functionality"*

Adverse action: An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

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

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

3.4.6 **T.Information_Leakage** *"Information Leakage from MRTD's chip"*

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

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

Asset: confidentiality of logical MRTD and TSF data.

3.4.7 **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.

3.4.8 **T.Malfunction** *"Malfunction due to Environmental Stress"*

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

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

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

3.4.9 **T.Configuration** *"Tampering attempt of the TOE during preparation"*

Adverse action: An attacker may access to the TOE at Manufacturing and Personalization phases (phase 5 and 6) to try to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

Threat agent: having high attack potential, being in possession of one or more MRTD in Pre-personalization or Personalization phases.

Asset: authenticity of logical MRTD data

3.4.10 **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

3.5 Organisational Security Policies

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

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

3.5.2 **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.

3.5.3 **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)[5] 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].

[5] Note that EF.DG3 and EF.DG4 are only readable after successful EAC authentication, not covered by this ST.

4 Security objectives

This chapter describes the security objectives for the TOE (OT) and the security objectives for the TOE environment (OE). 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.

4.1.1 **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 Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

4.1.2 **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.

4.1.3 **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.

4.1.4 **OT.Identification** *"Identification and Authentication of the TOE"*

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

4.1.5 **OT.Prot_Abuse-Func** *"Protection against Abuse of Functionality"*

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

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

4.1.6 **OT.Prot_Inf_Leak** *"Protection against Information Leakage"*

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

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

4.1.7 **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

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

with a prior

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

4.1.8 **OT.Prot_Malfunction** *"Protection against Malfunctions"*

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

4.1.9 **OT.Chip_Auth_Proof** *"Proof of MRTD's chip authenticity"*

The TOE must support the 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 Chip Authentication as defined in [TR_03110] the chip is genuine and chip and data page belong to each other as defined in [ICAO_9303].The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

4.1.10 OT.Configuration *"Protection of the TOE preparation"*

During Pre-personalization and Personalization phases, the TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions. It must also ensure secure erasing of useless keys.

4.2 Security objectives for the operational environment

4.2.1 Issuing State or Organization

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

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

Appropriate functionality testing of the TOE shall be used in phase 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.

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

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

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

  - origin and shipment details,
  - reception, reception 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.

4.2.1.3 **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.

4.2.1.4 **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].

4.2.1.5 **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_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.

4.2.1.6 **OE.Auth_MRTD** *"MRTD Authentication Key"*

The issuing State or Organization has to establish the necessary public key infrastructure in order to

(i) generate the MRTD's Authentication Key Pair(s), (ii) ensure the secrecy of the MRTD's Authentication Private Key(s), (iii) sign and store the Authentication Public Key(s) in the Authentication Public Key data (i.e in EF.DG14 for Chip Authentication Public Key and (iv) 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 Authentication Public Key by means of the Document Security Object.

4.2.2 Receiving State or Organization

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

4.2.2.1 **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].

4.2.2.2 OE.Exam_Chip_Auth *"Examination of the chip authenticity"*

Additionally to the OE.Exam_MRTD, inspection system performs the Chip Authentication to verify the Authenticity of the presented MRTD's chip.

4.2.2.3 **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.

4.2.2.4 **OE.Prot_Logical_MRTD** *"Protection of data from 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 Introduction

Assumption	Related Security Objective(s)	Rationale
A.MRTD_Manufact	OE.MRTD_Manufact	§ 4.3.2.1
A.MRTD_Delivery	OE.MRTD_Delivery	§ 4.3.2.2
A.Pers_Agent	OE.Personalization	§ 4.3.2.3
A.Insp_Sys	OE.Exam_MRTD OE.Prot_Logical_MRTD	§ 4.3.2.4
A.Insp_Sys_Chip_Auth	OE.Exam_Chip_Auth	§ 4.3.2.5
A.BAC-Keys	OE.BAC-Keys	§ 4.3.2.6
A.Signature_PKI	OE.Pass_Auth_Sign	§ 4.3.2.7

Table 5- Assumptions of the TOE and Security Objectives

Threat	Related Security Objective(s)	Rationale
T.Chip_ID	OT.Identification OE.BAC-Keys	§ 4.3.3.1
T.Skimming T.Eavesdropping	OT.Data_Conf OE.BAC-Keys	§ 4.3.3.2
T.Forgery	OT.AC_Pers OT.Data_Int OT.Prot_Phys-Tamper OE.Exam_MRTD OE.Pass_Auth_Sign OE.Passive_Auth_Verif	§ 4.3.3.3
T.Abuse-Func	OT.Prot_Abuse-Func OE. Personalization	§ 4.3.3.4
T.Information_Leakage T.Phys-Tamper T.Malfunction	OT.Prot_Inf_Leak OT.Prot_Phys-Tamper OT.Prot_Malfunction	§ 4.3.3.5
T.Configuration	OT.Configuration	§ 4.3.3.6
T.Counterfeit	OT.Chip_Auth_Proof OE.Exam_Chip_Auth OE.Auth_MRTD	§ 4.3.3.7

Table 6- Threats of the TOE and Security Objectives

OSP	Related Security Objective(s)	Rationale
P.Manufact	OT.Identification	§ 4.3.4.1
P.Personalization	OE.Personalization OT.AC_Pers OT.Identification	§ 4.3.4.2
P.Personal_Data	OT.Data_Int OT.Data_Conf	§ 4.3.4.3

Table 7- OSP of the TOE and Security Objectives

4.3.2 Rationales for Assumptions

4.3.2.1 A.MRTD_Manufact

The assumption **A.MRTD_Manufact** *"MRTD manufacturing on phase 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.

4.3.2.2 A.MRTD_Delivery

The assumption **A.MRTD_Delivery** *"MRTD delivery during phase 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.

4.3.2.3 A.Pers_Agent

The assumption **A.Pers_Agent** *"Personalization of the MRTD's chip"* is covered by the security objective for the TOE environment **OE.Personalization** *"Personalization of logical MRTD"* including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

4.3.2.4 A.Insp_Sys

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

4.3.2.5 A.Insp_Sys_Chip_Auth

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys_Chip_Auth** *"Inspection Systems for global interoperability on chip authenticity"* is covered by the security objectives for the TOE environment **OE.Exam_Chip_Auth**.

4.3.2.6 A.BAC-Keys

The assumption 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.

4.3.2.7 A.Signature_PKI

The assumption is directly covered by the security objective for the TOE environment **OE.Pass_Auth_Sign** *''Authentication of logical MRTD by Signature"* covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs.

4.3.3 Rationales for Threats

4.3.3.1 T.Chip_ID

The threat **T.Chip_ID** *"Identification of MRTD's chip"* addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered as described by the security objective **OT.Identification** *"Identification and Authentication of the TOE"* by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys** *"Cryptographic quality of Basic Access Control Keys"*.

4.3.3.2 T.Skimming and T.Eavesdropping

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

4.3.3.3 T.Forgery

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

4.3.3.4 T.Abuse-Func

The threat **T.Abuse-Func** *"Abuse of Functionality"* addresses attacks using the MRTD's chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by **OT.Prot_Abuse-Func** *"Protection against Abuse of Functionality"*. Additionally this objective is supported by the security objective for the TOE environment: **OE.Personalization** *"Personalization of logical MRTD"* ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

4.3.3.5 T.Information_Leakage, T.Phys-Tamper and T.Malfunction

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

4.3.3.6 T.Configuration

The threat **T.Configuration** *"Tampering attempt of the TOE* **during preparation**" addresses attacks in Pre-personalization and Personalization phases. The attacker trying to access to unauthorized TOE functions, trying to access or to modify sensitive information exchanged between the TOE and the Personalization system. Protection of the TOE during these two phases is directly addressed by **OT.Configuration** *"Protection of the TOE preparation"***.**

4.3.3.7 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 an identification and authenticity proof required by **OT.Chip_Auth_Proof** *"Proof of MRTD's chip authenticity"* using a authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_MRTD "**MRTD *Authentication Key"*. According to **OE.Exam_Chip_Auth** the inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip.

This threat is also covered by **OE.Auth_MRTD "**MRTD *Authentication Key"* using a authentication key pair to be generated by the issuing State or Organization.

4.3.4 Rationales for Organisational Security Policies

4.3.4.1 P.Manufact

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

4.3.4.2 P.Personalization

The OSP **P.Personalization** *"Personalization of the MRTD by issuing State or Organization only"* addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** *"Personalization of logical MRTD"*, and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** *"Access Control for Personalization of logical MRTD"*. Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** *"Identification and Authentication of the TOE"*. The security objective **OT.AC_Pers** *"Access Control for Personalization of logical MRTD"* limits the management of TSF data and management of TSF to the Personalization Agent.

4.3.4.3 P.Personal_Data

The OSP **P.Personal_Data** *"Personal data protection policy"* requires the TOE (i) to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives **OT.Data_Int** *"Integrity of personal data"* describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT.Data_Conf** *"Confidentiality of personal data"* describes the protection of the confidentiality.

5 Extended components definition

5.1 Extended components definition

5.1.1 Definition of the Family FAU_SAS

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

The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS ***“Audit data storage”***

Family behavior

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

Component leveling

FAU_SAS.1	Requires the TOE to 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.

5.1.2 Definition of the Family FCS_RND

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

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

FCS_RND ***“Generation of random numbers”***

Family 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*].

5.1.3 Definition of the Family FMT_LIM

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

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

FMT_LIM ***"Limited capabilities and availability"***

Family behavior

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

Component leveling:

FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle).
Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

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

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]*.

5.1.4 Definition of the Family FPT_EMS

The sensitive family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of [CC_2].

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS.1	TOE emanation has two constituents:
FPT_EMS.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMS.1.2	Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
Management:	FPT_EMS.1 There are no management activities foreseen.
Audit:	FPT_EMS.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*].

5.1.5 Definition of the Family FIA_API

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

FIA_API ***"Authentication Proof of Identity"***

Family 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 leveling:

FIA_API.1	Authentication Proof of Identity.
Management:	FIA_API.1 The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	There are no actions defined to be auditable.

FIA_API.1 ***"Authentication Proof of Identity"***

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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.

SFR in ST	SFR in [PP_BAC]	Description	Phase			
			Before 5	5	6	7
Class FAU *"Security Audit"*						
FAU_SAS.1.1	FAU_SAS.1.1	6.1.1.1	✓	×	×	×
Class FCS *"Cryptographic Support"*						
FCS_CKM.1.1/BAC	FCS_CKM.1.1	6.1.2.1	×	×	×	✓
FCS_CKM.1.1/GP			×	✓	✓	×
FCS_CKM.1.1/CA	Additional SFR		×	×	×	✓
FCS_CKM.4.1	FCS_CKM.4.1	6.1.2.2	×	✓	✓	✓
FCS_COP.1.1/BAC_SHA	FCS_COP.1.1/BAC_SHA	6.1.2.3	×	×	×	✓
FCS_COP.1.1/BAC_ENC	FCS_COP.1.1/ENC		×	×	×	✓
FCS_COP.1.1/AUTH	FCS_COP.1.1/AUTH		×	×	✓	×
FCS_COP.1.1/BAC_MAC	FCS_COP.1.1/MAC		×	×	×	✓
	Additional SFR		×	✓	×	×
FCS_COP.1.1/GP_ENC			×	✓	✓	×
FCS_COP.1.1/GP_AUTH			×	✓	×	×
FCS_COP.1.1/GP_MAC			×	✓	✓	×
FCS_COP.1.1/GP_KEY_DEC			×	✓	✓	×
FCS_COP.1.1/CA_SHA	Additional SFR		×	×	×	✓
FCS_COP.1.1/CA_ENC			×	×	×	✓
FCS_COP.1.1/CA_MAC			×	×	×	✓
FCS_RND.1.1	FCS_RND.1.1	6.1.2.4	×	✓	✓	✓
Class FIA *"Identification and Authentication"*						
FIA_UID.1.1	FIA_UID.1.1	6.1.3.1	×	✓	✓	✓
FIA_UID.1.2	FIA_UID.1.2		×	✓	✓	✓
FIA_UAU.1.1	FIA_UAU.1.1	6.1.3.2	×	✓	✓	✓
FIA_UAU.1.2	FIA_UAU.1.2		×	✓	✓	✓
FIA_UAU.4.1	FIA_UAU.4.1	6.1.3.3	×	✓	✓	✓
FIA_UAU.5.1/BAC	FIA_UAU.5.1	6.1.3.4	×	×	✓	✓
FIA_UAU.5.2/BAC	FIA_UAU.5.2		×	×	✓	✓
FIA_UAU.5.1/MP	Additional SFR		×	✓	×	×
FIA_UAU.5.2/MP			×	✓	×	×
FIA_UAU.5.1/CA	Additional SFR		×	×	✓	✓
FIA_UAU.5.2/CA			×	×	✓	✓
FIA_UAU.6.1/BAC	FIA_UAU.6.1	6.1.3.5	×	×	×	✓
FIA_UAU.6.1/MP	Additional SFR		×	✓	✓	×
FIA_UAU.6.1/CA	Additional SFR		×	×	×	✓
FIA_AFL.1.1/BAC	FIA_AFL.1.1	6.1.3.6	×	×	×	✓
FIA_AFL.1.2/BAC	FIA_AFL.1.2		×	×	×	✓
FIA_AFL.1.1/MP	Additional SFR		×	✓	✓	×
FIA_AFL.1.2/MP	Additional SFR		×	✓	✓	×
FIA_API.1.1/CA	Additional SFR	6.1.3.7	×	×	×	✓
			×	×	×	✓
Class FDP *"User Data Protection"*						
FDP_ACC.1.1/BAC	FDP_ACC.1.1	6.1.4.1	×	×	✓	✓
FDP_ACC.1.1/CA	Additional SFR		×	×	✓	✓

SFR in ST	SFR in [PP_BAC]	Description	Phase			
			Before 5	5	6	7
FDP_ACF.1.1/BAC	FDP_ACF.1.1	6.1.4.2	×	×	✓	✓
FDP_ACF.1.2/BAC	FDP_ACF.1.2		×	×	✓	✓
FDP_ACF.1.3/BAC	FDP_ACF.1.3		×	×	✓	✓
FDP_ACF.1.4/BAC	FDP_ACF.1.4		×	×	✓	✓
FDP_ACF.1.1/CA	Additional SFR		×	×	✓	✓
FDP_ACF.1.2/CA			×	×	✓	✓
FDP_ACF.1.3/CA			×	×	✓	✓
FDP_ACF.1.4/CA			×	×	✓	✓
FDP_UCT.1.1/BAC	FDP_UCT.1.1	6.1.4.3	×	×	×	✓
FDP_UCT.1.1/CA	Additional SFR		×	×	×	✓
FDP_UIT.1.1/BAC	FDP_UIT.1.1	6.1.4.4	×	×	×	✓
FDP_UIT.1.2/BAC	FDP_UIT.1.2		×	×	×	✓
FDP_UIT.1.1/CA	Additional SFR		×	×	×	✓
FDP_UIT.1.2/CA			×	×	×	✓
Class FMT *"Security Management"*						
FMT_MOF.1.1/PROT	Additional SFR	6.1.5.1	×	✓	✓	×
FMT_SMF.1.1	FMT_SMF.1.1	6.1.5.2	✓	✓	✓	×
FMT_SMR.1.1	FMT_SMR.1.1	6.1.5.3	×	✓	✓	✓
FMT_SMR.1.2	FMT_SMR.1.2		×	✓	✓	✓
FMT_LIM.1.1	FMT_LIM.1.1	6.1.5.4	×	✓	✓	✓
FMT_LIM.2.1	FMT_LIM.2.1	6.1.5.5	×	✓	✓	✓
FMT_MTD.1.1/INI_ENA	FMT_MTD.1.1/INI_ENA	6.1.5.6	×	✓	✓	✓
FMT_MTD.1.1/INI_DIS	FMT_MTD.1.1/INI_DIS		×	✓	✓	✓
FMT_MTD.1.1/KEY_WRITE	FMT_MTD.1.1/KEY_WRITE		×	✓	✓	✓
FMT_MTD.1.1/KEY_READ	FMT_MTD.1.1/KEY_READ		×	✓	✓	✓
FMT_MTD.1.1/CAPK	Additional SFR		×	✓	✓	✓
FMT_MTD.1.1/CAPK_READ			×	✓	✓	✓
FMT_MTD.1.1/LCS_PERS	Additional SFR		×	✓	✓	✓
Class FPT *"Protection of the Security Functions"*						
FPT_EMS.1.1	FPT_EMSEC.1.1	6.1.6.1	×	✓	✓	✓
FPT_EMS.1.2	FPT_EMSEC.1.2		×	✓	✓	✓
FPT_FLS.1.1	FPT_FLS.1.1	6.1.6.2	×	✓	✓	✓
FPT_TST.1.1	FPT_TST.1.1	6.1.6.3	×	✓	✓	✓
FPT_TST.1.2	FPT_TST.1.2		×	✓	✓	✓
FPT_TST.1.3	FPT_TST.1.3		×	✓	✓	✓
FPT_PHP.3.1	FPT_PHP.3.1	6.1.6.4	×	✓	✓	✓
Class FTP *"Trusted path/channels"*						
FTP_ITC.1.1/MP	Additional SFR	6.1.7.1	×	✓	✓	×
FTP_ITC.1.2/MP			×	✓	✓	×
FTP_ITC.1.3/MP			×	✓	✓	×

Table 8 – SFR of the TOE

6.1.1 Class FAU *"Security Audit"*

6.1.1.1 FAU_SAS.1 *"Audit Storage"*

Hierarchical to: No other components.

Dependencies: No dependencies

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

6.1.2 Class FCS *"Cryptographic Support"*

6.1.2.1 FCS_CKM.1 *"Cryptographic key generation"*

Hierarchical to: No other components.

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

FCS_CKM.1.1 / BAC: 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], normative appendix 5**.

FCS_CKM.1.1 / GP: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Algorithm]** and specified cryptographic key sizes **[key sizes]** that meet the following **[standard]**:

Algorithm	key size(s)	standard
Triple-DES in CBC mode	**112 bit**	**[GPC_SPE_034]; appendix E.4.1.**
AES in CBC mode	**128, 192 and 256 bit**	**[GPC_SPE_014]**

FCS_CKM.1.1 / CA: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **based on ECDH compliant to [TR_03110]** and specified cryptographic key sizes **192 to 521 bit** that meet the following: **[ICAO-9303] Part 11.**

6.1.2.2 FCS_CKM.4 *"Cryptographic key destruction"*

Hierarchical to: No other components.

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

FCS_CKM.4.1: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroisation** that meets the following: **none**.

6.1.2.3 FCS_COP.1 *"Cryptographic operation"*

Hierarchical to: No other components.

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

FCS_COP.1.1/ BAC_SHA: The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meets the following **[FIPS_180_3] .**

FCS_COP.1.1/ BAC_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 meets the following **[FIPS_46_3] and [ICAO_9303]; normative appendix 5, A5.3 [ICAO_9303].**

FCS_COP.1.1/ AUTH — The TSF shall perform **symmetric authentication – encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES** and cryptographic key sizes **112 bit** that meets the following **[FIPS_46_3].**

FCS_COP.1.1/ BAC_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 meets the following **[ISO_9797_1] (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).**

FCS_COP.1.1/ GP_ENC — The TSF shall perform **secure messaging (GP) – encryption and decryption** in accordance with a specified cryptographic algorithm [**Algorithm]** and cryptographic key sizes [**key size(s)]** that meets the following [**standard].**

Algorithm	key size(s)	standard
Triple-DES in CBC mode	**112 bit**	**[FIPS_46_3]**
AES in CBC mode	**128, 192 and 256 bit**	**[FIPS_197]**

FCS_COP.1.1/ GP_AUTH — The TSF shall perform **symmetric authentication – encryption and decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[key size(s)]** that meets the following **[standard].**

Algorithm	key size(s)	standard
Triple-DES	**112 bit**	**[FIPS_46_3]**
AES	**128, 192 and 256 bit**	**[FIPS_197]**

FCS_COP.1.1/ GP_MAC — The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[key size(s)]** that meets the following **[standard].**

Algorithm	key size(s)	standard
Retail MAC	**112 bit**	**[ISO_9797_1]**
AES CMAC	**128, 192 and 256 bit**	**[NIST_800_38B]**

FCS_COP.1.1/ GP_KEY_DEC — The TSF shall perform **key decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[key size(s)]** that meets the following **[standard]**.

Algorithm	key size(s)	standard
Triple-DES in CBC mode	**112 bit**	**[FIPS_46_3]**
AES in CBC mode	**128, 192 and 256 bit**	**[FIPS_197]**

FCS_COP.1.1/ CA_SHA — The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1 and SHA-256** and cryptographic key sizes **none** that meets the following **[FIPS_180_3].**

FCS_COP.1.1/ CA_ENC — The TSF shall perform **secure messaging – encryption and decryption** in accordance with a specified cryptographic algorithm **[algorithm]** and cryptographic key sizes **[key size(s)]** that meets the following **[standard].**

Algorithm	key size(s)	standard
Triple-DES in CBC mode	**112 bit**	**[FIPS_46_3]**
AES in CBC mode	**128, 192 and 256 bit**	**[FIPS_197]**

FCS_COP.1.1/ CA_MAC — The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **[algorithm]** and cryptographic key sizes **[key size(s)]** that meets the following **[standard].**

Algorithm	key size(s)	standard
Retail MAC	**112 bit**	**[ISO_9797_1]**
AES CMAC	**128, 192 and 256 bit**	**[NIST_800_38B]**

6.1.2.4 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 **The average Shannon entropy per internal random bit exceeds 0.999**

6.1.3 Class FIA *"Identification and Authentication"*

6.1.3.1 FIA_UID.1 *"Timing of identification"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 **[Editorially Refined]** The TSF shall allow

1. **to read the Initialization Data in Stage 2 "Production",**
2. **to read the random identifier in Stage 3 "Preparation",**
3. **to read the random identifier in Stage 4 "Operational"**

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.

6.1.3.2 FIA_UAU.1 *"Timing of authentication"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.1.1 **[Editorially Refined]** The TSF shall allow

1. to read the Initialization Data in Stage 2 "Production",
2. to read the random identifier in Stage 3 "Preparation",
3. to read the random identifier in Stage 4 "Operational"
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.

6.1.3.3 FIA_UAU.4 "Single-use authentication mechanisms"

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

1. **Basic Access Control Authentication Mechanism,**
2. **Authentication Mechanisms based on :**
   - **Triple-DES**
   - **AES.**

Application Note: The Authentication Mechanisms based on Triple-DES or AES is the authentication process performed in phases 5 and 6.

6.1.3.4 FIA_UAU.5 “Multiple authentication mechanisms”

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/ BAC — The TSF shall provide

1. **Basic Access Control Authentication Mechanism,**
2. **Symmetric Authentication Mechanism based on Triple-DES and AES.**

To support user authentication.

FIA_UAU.5.2/ BAC — The TSF shall authenticate any user’s claimed identity according to the **following rules:**

1. **The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) the Symmetric Authentication Mechanism with the Personalization Agent Key,**
2. **The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.**

FIA_UAU.5.1/ MP — The TSF shall provide

1. **Authentication Mechanism based on Triple-DES and AES.**

To support user authentication.

FIA_UAU.5.2/ MP — The TSF shall authenticate any user’s claimed identity according to the **following rules:**

The TOE accepts the authentication attempt as Manufacturer by the Symmetric Authentication Mechanism with Personalization Agent Key.

FIA_UAU.5.1/ CA — The TSF shall provide

1. **Secure messaging in MAC-ENC mode,**
2. **Key agreement protocol Diffie-Hellman during Chip Authentication Protocol v.1 according to [TR_03110]**

To support user authentication.

FIA_UAU.5.2/ CA — The TSF shall authenticate any user’s claimed identity according to the **following rules:**

1. **After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.**

6.1.3.5 FIA_UAU.6 *"Re-authenticating"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/ BAC: 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.**

FIA_UAU.6.1/ MP: The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful authentication of the terminal with the Symmetric Authentication Mechanism shall be verified as being sent by the authenticated terminal.**

Application note: This requirement applies to the authentication protocol used by (1) the Manufacturer and (2) the Personalization Agent

FIA_UAU.6.1/ CA: The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the inspection system (GIS).**

6.1.3.6 FIA_AFL.1 *"Authentication failure handling"*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1/ BAC: The TSF shall detect when **an administrator configurable positive integer within range of acceptable values 0 to 255 consecutive** unsuccessful authentication attempts occur related to **BAC authentication protocol**.

FIA_AFL.1.2/ BAC: When the defined number of unsuccessful authentication attempts has been **met or surpassed**, the TSF shall **wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the BAC authentication attempts.**

FIA_AFL.1.1/ MP: The TSF shall detect when **1** unsuccessful authentication attempts occur related to **authentication of the Manufacturer and the Personalization Agent.**

FIA_AFL.1.2/ MP: When the defined number of unsuccessful authentication attempts has been **met** the TSF shall **slow down exponentially the next authentication.**

6.1.3.7 FIA_API.1 *"Authentication Proof of Identity"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/ CA: The TSF shall provide a **Chip Authentication protocol according to [TR_03110]** to prove the identity of the **TOE**.

6.1.4 Class FDP *"User Data Protection"*

6.1.4.1 FDP_ACC.1 *"Subset access control"*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ BAC: 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_ACC.1.1/ CA: The TSF shall enforce the **CA Access Control SFP** on **terminals gaining read and modify access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.**

6.1.4.2 FDP_ACF.1 *"Basic Security attribute based access control"*

Hierarchical to: No other components.

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

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

1. Subjects:
- **a. Personalization Agent,**
- **b. Basic Inspection System,**
- **c. Terminal,**

2. Objects:
- **a. data EF.DG1 to EF.DG16 of the logical MRTD,**
- **b. data in EF.COM,**
- **c. data in EF.SOD,**

3. Security attributes
- **a. authentication status of terminals.**

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

1. Subjects:
- a**. General Inspection System,**
- b. **Terminal**,

2. Objects:
- **a. data EF.DG1 to EF.DG16 of the logical MRTD,**
- **b. data in EF.COM,**
- **c. data in EF.SOD,**

3. Security attributes
- **a. authentication status of terminals.**

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

1. the successfully authenticated Personalization Agent is allowed to write and read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,

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

FDP_ACF.1.2/ CA — The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
1. the successfully authenticated General Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.

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

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

FDP_ACF.1.4/ BAC — The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
1.Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
2.Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD,
3.The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.

FDP_ACF.1.4/ CA — The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD,
3. The General Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.

6.1.4.3 FDP_UCT.1 *"Basic data exchange confidentiality"*

Hierarchical to: No other components.

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

FDP_UCT.1.1/ BAC — The TSF shall enforce the **Basic Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorized disclosure.

FDP_UCT.1.1/ CA — The TSF shall enforce the **CA Access Control SFP** to be able to **transmit and receive** user data in a manner protected from unauthorized disclosure **after Chip Authentication.**

6.1.4.4 FDP_UIT.1 *"Data exchange integrity"*

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1/ BAC	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/ BAC	The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.
FDP_UIT.1.1/ CA	The TSF shall enforce the **CA Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors **after Chip Authentication protocol**
FDP_UIT.1.2/ CA	The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred **after Chip Authentication protocol.**

6.1.5 Class FMT *"Security Management"*

6.1.5.1 FMT_MOF *"Management of functions in TSF"*

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1/ PROT: The TSF shall restrict the ability to **enable** the functions

- **Chip Authentication,**

to **the Manufacturer.**

6.1.5.2 FMT_SMF.1 *"Specification of Management Functions"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

1. **Initialization**
2. **Personalization**
3. **Chip Authentication protocol,**

6.1.5.3 FMT_SMR.1 *"Security roles"*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1: The TSF shall maintain the roles:

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

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

Note: This SFR also applies to the refinement of the role Manufacturer.

6.1.5.4 FMT_LIM.1 *"Limited capabilities"*

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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

Deploying Test Features after TOE Delivery does not allow

1. **User Data to be disclosed or manipulated,**
2. **TSF data to be disclosed or manipulated,**

3. **software to be reconstructed and,**
4. **substantial information about construction of TSF to be gathered which may enable other attacks**.

6.1.5.5 FMT_LIM.2 *"Limited availability"*

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced**:**

Deploying Test Features after TOE Delivery does not allow

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

6.1.5.6 FMT_MTD.1 *"Management of TSF data"*

Hierarchical to: No other components.

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

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to **write** the **Initialization Data and Pre-personalization Data** to **the Manufacturer.**
Note	Please refer to F.ACW for details of the data written by the manufacturer.
FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to **disable read access for users to** the **Initialization Data** to **the Personalization Agent.**
FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to **write** the **Document Basic Access Keys** to **the Personalization Agent.**
FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to **read** the **Document Basic Access Keys and Personalization Agent Keys** to **none.**
FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to **write** the **Chip Authentication Keys** to **the Personalization Agent.**
FMT_MTD.1.1/ CAPK_READ	The TSF shall restrict the ability to **read** the **Chip Authentication Private Key** to **none.**
FMT_MTD.1.1/ LCS_PERS	The TSF shall restrict the ability **to switch** the **LCS from phase 6 to phase 7** to **the Personalization Agent.**

6.1.6 Class FPT *"Protection of the Security Functions"*

6.1.6.1 FPT_EMS.1 *"TOE Emanation"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMS.1.1 The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to **Personalization Agent Keys** and :

- **Chip Authentication Private Key,**
- **Personalization Agent Keys,**
- **BAC Keys,**

FPT_EMS.1.2 The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to **Personalization Agent Keys** and:

- **Chip Authentication Private Key,**
- **BAC Keys,**

6.1.6.2 FPT_FLS.1 *"Failure with preservation of secure state"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

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

6.1.6.3 FPT_TST.1 *"TSF testing"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions**

- **At reset,**

To demonstrate the correct operation of **the TSF**.

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

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

6.1.6.4 FPT_PHP.3 *"Resistance to physical attack"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

6.1.7 Class FTP "Trusted path/channels"

6.1.7.1 FTP_ITC.1 *"Inter-TSF trusted channel"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

FTP_ITC.1.1/ MP The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ MP The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/ MP The TSF shall initiate communication via the trusted channel for **loading sensitive data (Perso_K, CA_SK) shall be encrypted.**

6.2 Security assurance requirements

The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following component: ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, and ATE_DPT.3.

6.2.1 EAL rationale

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

6.2.2 EAL augmentation rationale

6.2.2.1 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.

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

6.2.2.2 ADV_FSP.5 "Complete semi-formal functional specification with additional error information"

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

6.2.2.3 ADV_INT.2 "Well-structured internals"

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

6.2.2.4 ADV_TDS.4 "Semiformal modular design"

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

6.2.2.5 ALC_CMS.5 "Development tools CM coverage"

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

6.2.2.6 ALC_TAT.2 “Compliance with implementation standards”

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

6.2.2.7 ATE_DPT.3 “Testing: modular design”

The TOE actually target an EAL5 + ALC_DVS.2 and AVA_VAN.5 and is only limited to EAL4+ due to the restriction of [PP_BAC] on AVA_VAN level.

Other MRTDs TOE are targeting the same physical scope are not affected by this limitation and provide the full EAL5+ set of SARs. This EAL5+ is required to reach a higher level of assurance due to sensitivity of ID documents.

6.2.3 Dependencies

SAR	Dependencies	Support of the Dependencies
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	ADV_FSP.5 ADV_TDS.4
ADV_FSP.5	ADV_TDS.1 ADV_IMP.1	ADV_TDS.4 ADV_IMP.1
ADV_IMP.1	ADV_TDS.3 ALC_TAT.1	ADV_TDS.4 ALC_TAT.2
ADV_INT.2	ADV_IMP.1 ADV_TDS.3 ALC_TAT.1	ADV_IMP.1 ADV_TDS.4 ALC_TAT.2
ADV_TDS.4	ADV_FSP.5	ADV_FSP.5
AGD_OPE.1	ADV_FSP.1	ADV_FSP.5
AGD_PRE.1	No dependencies	n.a.
ALC_CMC.4	ALC_CMS.1 ALC_DVS.1 ALC_LCD.1	ALC_CMS.5 ALC_DVS.2 ALC_LCD.1
ALC_CMS.5	No dependencies	n.a.
ALC_DEL.1	No dependencies	n.a.
ALC_DVS.2	No dependencies	n.a.
ALC_LCD.1	No dependencies	n.a.
ALC_TAT.2	ADV_IMP.1	n.a.
ASE_CCL.1	ASE_INT.1 ASE_ECD.1 ASE_REQ.1	ASE_INT.1 ASE_ECD.1 ASE_REQ.2
ASE_ECD.1	No dependencies	n.a.
ASE_INT.1	No dependencies	n.a.
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
ASE_REQ.2	ASE_OBJ.2 ASE_ECD.1	ASE_OBJ.2 ASE_ECD.1
ASE_SPD.1	No dependencies	n.a.
ASE_TSS.1	ASE_INT.1 ASE_REQ.1 ADV_FSP.1	ASE_INT.1 ASE_REQ.2 ADV_FSP.5
ATE_COV.2	ADV_FSP.2 ATE_FUN.1	ADV_FSP.5 ATE_FUN.1
ATE_DPT.3	ADV_ARC.1 ADV_TDS.4 ATE_FUN.1	ADV_ARC.1 ADV_TDS.4 ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.2

SAR	Dependencies	Support of the Dependencies
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	ADV_FSP.5 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
AVA_VAN.3	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	ADV_ARC.1 ADV_FSP.5 ADV_TDS.4 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.3

Table 9 - SARs dependencies

6.3 Security requirements rationale

6.3.1 Security Functional Requirements Rationale

6.3.1.1 Overview

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

SFR \ SO	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Chip_Auth_Proof	OT.Configuration
FAU_SAS.1				X						
FCS_CKM.1/BAC		X	X							
FCS_CKM.1/GP	X	X	X							X
FCS_CKM.1/CA		X	X						X	
FCS_CKM.4	X	X	X							X
FCS_COP.1/BAC_SHA		X	X							
FCS_COP.1/BAC_ENC		X	X							
FCS_COP.1/AUTH	X	X								
FCS_COP.1/BAC_MAC		X	X							
FCS_COP.1/GP_ENC	X	X	X							X
FCS_COP.1/GP_AUTH										X
FCS_COP.1/GP_MAC	X	X	X							X
FCS_COP.1/GP_KEY_DEC			X							X
FCS_COP.1/CA_SHA		X	X						X	
FCS_COP.1/CA_ENC		X	X						X	
FCS_COP.1/CA_MAC		X	X						X	
FCS_RND.1	X	X	X						X	X
FIA_UID.1			X	X						
FIA_UAU.1			X	X						
FIA_UAU.4	X	X	X							X
FIA_UAU.5/BAC	X	X	X							
FIA_UAU.5/MP										X
FIA_UAU.5/CA			X							
FIA_UAU.6/BAC		X	X							
FIA_UAU.6/MP	X	X	X							X
FIA_UAU.6/CA		X	X							
FIA_AFL.1/BAC			X	X						
FIA_AFL.1/MP	X									X
FIA_API.1/CA									X	
FDP_ACC.1/BAC	X	X	X							
FDP_ACF.1/BAC	X	X	X							
FDP_UCT.1/BAC		X	X							
FDP_UCT.1/CA		X	X							
FDP_UIT.1/BAC		X	X							
FDP_UIT.1/CA		X	X							
FMT_MOF.1/PROT									X	X
FMT_SMF.1	X	X	X							X
FMT_SMR.1	X	X	X							X
FMT_LIM.1								X		
FMT_LIM.2								X		
FMT_MTD.1/INI_ENA				X						
FMT_MTD.1/INI_DIS				X						
FMT_MTD.1/KEY_WRITE	X	X	X							
FMT_MTD.1/KEY_READ	X	X	X							
FMT_MTD.1/CAPK	X	X	X						X	
FMT_MTD.1/CAPK_READ	X	X	X						X	

SFR \ SO	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Chip_Auth_Proof	OT.Configuration
FMT_MTD.1/LCS_PERS	X									
FPT_EMS.1	X				X					X
FPT_FLS.1	X				X		X			X
FPT_TST.1					X		X			
FPT_PHP.3	X				X	X				X
FTP_ITC.1/MP										X

Table 8 SFRs and Security Objectives

6.3.1.2 OT.AC_Pers

The security objective **OT.AC_Pers** *"Access Control for Personalization of logical MRTD"* addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR ***FDP_ACC.1/BAC*** and ***FDP_ACF.1/BAC*** 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.

The following paragraph is extracted from [PP_BAC] and has been refined according to the technical characteristics of this TOE. The refinement is right after.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/BAC_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 [PP_EAC] by using the symmetric authentication mechanism (FCS_COP.1/ AUTH)[6].

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

Note*: As BAC mechanism is not supported for the authentication of the terminal as Personalization Agent, the following two paragraphs have been added to demonstrate that symmetric authentication used in Personalization phase fulfills the OT.AC_Pers.*

The authentication of the terminal as Personalization Agent is performed by TSF according to SFR ***FIA_UAU.4*** and ***FIA_UAU.5/BAC***. The Personalization Agent can be authenticated by using the symmetric authentication mechanism (***FCS_COP.1/AUTH***) with the personalization key. ***FIA_UAU.6/MP*** describes the re-authentication. In case of failed authentication attempts ***FIA_AFL.1/MP*** enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

As the symmetric authentication is used in Personalization phase, the SFR ***FIA_UAU.6/MP*** describes the re-authentication and the protection of the transmitted data is assumed by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/GP***, ***FCS_RND.1*** (for key generation), and ***FCS_COP.1/GP_ENC*** as well as ***FCS_COP.1/GP_MAC*** for the ENC_MAC_Mode. The SFR ***FCS_CKM.4*** enforces the destruction of Secure Messaging session keys.

[6] As the BAC mechanism is not used during Personalization phase of the TOE, this part is not relevant for this TOE.

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 confidentially of these keys.

The following parts are added to integrate the personalization of the different keys in the OT.AC_Pers.

Only the Personalization Agent is allowed to set the Document Basic Access Keys according to the SFR ***FMT_MTD.1/KEY_WRITE***. The SFR ***FMT_MTD.1/KEY_READ*** prevents read access to the Document Basic Access Keys and ensure together with the SFR ***FCS_CKM.4***, ***FPT_EMS.1***, ***FPT_FLS.1*** and ***FPT_PHP.3*** the confidentially of these keys.

Only the Personalization Agent is allowed to set the Chip Authentication Private Key according to the SFR ***FMT_MTD.1/CAPK***. The SFR ***FMT_MTD.1/CAPK_READ*** prevents read access to the Chip Authentication Private Key and ensure together with the SFR ***FCS_CKM.4***, ***FPT_EMS.1***, ***FPT_FLS.1*** and ***FPT_PHP.3*** the confidentially of these keys.

The Personalization Agent is the only subject allowed to ends Personalization of logical MRTD, setting the TOE Life Cycle State in Operational Use state according to ***FMT_MTD.1.1/LCS_PERS***. Since then it is no more possible to return in Personalization state.

6.3.1.3 OT.Data_Int

The security objective **OT.Data_Int** *"Integrity of personal data"* requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFRs (***FDP_ACC.1/BAC, FDP_ACC.1/CA)*** and (***FDP_ACF.1/BAC, FDP_ACF.1/CA)*** 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/BAC***, 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/BAC***). The SFR ***FMT_SMR.1*** lists the roles (including Personalization Agent) and the SFR ***FMT_SMF.1*** lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR ***FIA_UAU.4***, ***FIA_UAU.5/BAC*** and ***FIA_UAU.6/BAC*** using ***FCS_COP.1/AUTH***.

The security objective **OT.Data_Int** *"Integrity of personal data"* requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR ***FIA_UAU.6/BAC***, ***FDP_UCT.1/BAC*** and ***FDP_UIT.1/BAC*** requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/BAC***, ***FCS_COP.1/BAC_SHA***, ***FCS_RND.1*** (for key generation), and ***FCS_COP.1/BAC_ENC*** and ***FCS_COP.1/BAC_MAC*** for the ENC_MAC_Mode. The SFR ***FMT_MTD.1/KEY_WRITE*** requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to ***FMT_MTD.1/KEY_READ***.

The following part is added to integrate the Manufacturing and Personalization phases in the OT_Data_Int.

Manufacturer and Personalization Agent are also able to detect any modification of the transmitted logical MRTD data by means of the Symmetric Authentication mechanism. The SFR ***FIA_UAU.6/MP*** requires the re-authentication and the protection of the transmitted data is assumed by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/GP, FCS_RND.1*** (for key generation), and ***FCS_COP.1/GP_ENC*** and ***FCS_COP.1/GP_MAC*** for the ENC_MAC_Mode.

The following part is added to integrate the Chip Authentication mechanism in the coverage of the OT.Data_Int.

The inspection system is also able to detect any modification of the transmitted logical MRTD data by means of the Chip Authentication mechanism. The SFR ***FIA_UAU.6/CA***, ***FDP_UCT.1/CA*** and ***FDP_UIT.1/CA*** requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/CA FCS_COP.1/CA_SHA***, ***FCS_RND.1*** (for key generation), and ***FCS_COP.1/CA_ENC*** and ***FCS_COP.1/CA_MAC*** for the ENC_MAC_Mode. The SFR ***FMT_MTD.1/CAPK*** requires the Personalization

Agent to establish the Chip Authentication Private Key in a way that it cannot be read by anyone in accordance to ***FMT_MTD.1/CAPK_READ***. ***FCS_CKM.4*** enforces the destruction of Secure Messaging session keys.

6.3.1.4 OT.Data_Conf

The security objective **OT.Data_Conf** *"Confidentiality of personal data"* requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR ***FIA_UID.1*** and ***FIA_UAU.1*** allow only those actions before identification respective authentication which do not violate **OT.Data_Conf**. In case of failed authentication attempts ***FIA_AFL.1/BAC*** 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/BAC*** and ***FDP_ACF.1.2/BAC***: 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/BAC*** 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/BAC*** 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/BAC_ENC*** and ***FCS_COP.1/BAC_MAC*** (cf. the SFR ***FDP_UCT.1/BAC*** and ***FDP_UIT.1/BAC***). (for key generation), and ***FCS_COP.1/BAC_ENC*** and ***FCS_COP.1/BAC_MAC*** for the ENC_MAC_Mode. The SFR ***FCS_CKM.1/BAC***, ***FCS_CKM.4***, ***FCS_COP.1/BAC_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.

The following part is added to integrate the Manufacturing and Personalization phases in the OT_Data_Conf.

Manufacturer and Personalization Agent are also able to detect any modification of the transmitted logical MRTD data by means of the Symmetric Authentication mechanism. The SFR ***FIA_UAU.6/MP***, ***FDP_UCT.1/*** require the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/GP, FCS_RND.1*** (for key generation), and ***FCS_COP.1/GP_ENC*** and ***FCS_COP.1/GP_MAC*** for the ENC_MAC_Mode.

The following parts are added to integrate the Chip Authentication mechanism and the Symmetric Authentication mechanism used in Personalization phase in the coverage of the OT.Data_Conf.

The SFR ***FIA_UAU.5/CA*** enforces the TOE to accept only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism. Moreover, the SFR ***FIA_UAU.6/CA*** requests secure messaging after successful authentication of the chip which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to ***FCS_COP.1/CA_ENC*** and ***FCS_COP.1/CA_MAC*** (cf. the SFR ***FDP_UCT.1/CA*** and ***FDP_UIT.1/CA***). (for key generation), and ***FCS_COP.1/CA_ENC*** and ***FCS_COP.1/CA_MAC*** for the ENC_MAC_Mode. The SFR ***FCS_CKM.1/CA***, ***FCS_CKM.4***, ***FCS_COP.1/CA_SHA*** and ***FCS_RND.1*** establish the key management for the secure messaging keys. The SFR ***FMT_MTD.1/CAPK*** addresses the key management and ***FMT_MTD.1/CAPK_READ*** prevents reading of the Chip Authentication Private Key.
During Personalization of logical MRTD, the Chip Authentication Private Key is transmitted ciphered and the TSF deciphers these keys according to SFR ***FCS_COP.1/GP_KEY_DEC*** (***FCS_CKM.1/GP*** and ***FCS_RND.1*** for decryption session key generation; ***FCS_CKM.4*** for decryption session key destruction).

6.3.1.5 OT.Identification

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

Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 “Operational Use”. The SFR ***FMT_MTD.1/INI_ENA*** allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR ***FMT_MTD.1/INI_DIS*** allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 “Operational Use” violates the security objective **OT.Identification**. The SFR ***FIA_UID.1*** and ***FIA_UAU.1*** do not allow reading of any data uniquely identifying the MRTD’s chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts ***FIA_AFL.1/BAC*** enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

6.3.1.6 OT.Prot_Abuse-Func

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

6.3.1.7 OT.Prot_Inf_Leak

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

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

6.3.1.8 OT.Prot_Phys-Tamper

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

6.3.1.9 OT.Prot_Malfunction

The security objective **OT.Prot_Malfunction** *“Protection against Malfunctions”* is covered by (i) the SFR ***FPT_TST.1*** which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR ***FPT_FLS.1*** which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

6.3.1.10 OT.Chip_Auth_Proof

The security objective **OT.Chip_Auth_Proof** *“Proof of MRTD’s chip authenticity”* is ensured by the Chip Authentication Protocol activated by ***FMT_MOF.1/PROT*** and provided by ***FIA_API.1/CA*** proving the genuineness of the TOE. The Chip Authentication Protocol defined by ***FCS_CKM.1/CA*** is performed using a TOE internally stored confidential private key. Confidentiality of this key is ensured by ***FMT_MTD.1/CAPK*** and ***FMT_MTD.1/CAPK_READ***. The Chip Authentication Protocol [TR_03110] requires additional TSF according to ***FCS_COP.1/CA_SHA*** (for the derivation of the session keys), ***FCS_COP.1/CA_ENC*** and ***FCS_COP.1/CA_MAC*** (for the ENC_MAC_Mode secure messaging).

6.3.1.11 OT.Configuration

The security objective **OT.Configuration** *“Protection of the TOE preparation”* addresses management of the Data Configuration, Pre-personalization Agent keys, Personalization Agent keys and the Life Cycle State of the TOE.

The authentication of the terminal as Manufacturer is performed by TSF according to SFR ***FIA_UAU.4*** and ***FIA_UAU.5/MP***. The Manufacturer can be authenticated by using the symmetric authentication mechanism (***FCS_COP.1/GP_AUTH***) with the Pre-personalization key. ***FIA_UAU.6/MP*** describes the re-authentication. In case

of failed authentication attempts ***FIA_AFL.1/MP*** enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The SFR ***FTP_ITC.1/MP*** allows the Manufacturer to communicate with the OS.

Once phase 4 is done, the MRTD packaging responsible is allowed to set the Pre-personalization Agent keys according to the SFR and ***FCS_COP.1/GP_KEY_DEC***.

In phase 5, the authentication of the terminal as Manufacturer shall be performed by TSF according to SFR ***FIA_UAU.4*** and ***FIA_UAU.5/MP***. The Manufacturer shall be authenticated by using the symmetric authentication mechanism (***FCS_COP.1/GP_AUTH***).

In case of failed authentication attempts ***FIA_AFL.1/MP*** enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack

The SFR ***FIA_UAU.6/MP*** describes the re-authentication and the protection of the transmitted data is assumed by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/GP***, ***FCS_RND.1*** (for key generation), and ***FCS_COP.1/GP_ENC*** as well as ***FCS_COP.1/GP_MAC*** for the ENC_MAC_Mode. The SFR ***FCS_CKM.4*** enforces the destruction of Secure Messaging session keys.

The Manufacturer can enable Chip Authentication functionalities following ***FMT_MOF.1.1/PROT***.

6.3.2 Dependency Rationale

6.3.2.1 Overview

The Table 9 Dependencies between the SFR for the TOE shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1/BAC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/BAC_ENC and FCS_COP.1/BAC_MAC FCS_CKM.4
FCS_CKM.1/GP		FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC FCS_CKM.4
FCS_CKM.1/CA		FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC FCS_CKM.4
FCS_CKM.4	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	FCS_CKM.1/BAC and FCS_CKM.1/GP and FCS_CKM.1/CA
FCS_COP.1/BAC_SHA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	See § 1.1.1.1.1 FCS_CKM.4
FCS_COP.1/BAC_ENC		FCS_CKM.1/BAC FCS_CKM.4
FCS_COP.1/AUTH		FCS_CKM.1/BAC FCS_CKM.4
FCS_COP.1/BAC_MAC		FCS_CKM.1/BAC FCS_CKM.4
FCS_COP.1/GP_ENC		FCS_CKM.1/GP FCS_CKM.4
FCS_COP.1/GP_AUTH		FCS_CKM.1/GP FCS_CKM.4
FCS_COP.1/GP_MAC		FCS_CKM.1/GP FCS_CKM.4
FCS_COP.1/GP_KEY_DEC		FCS_CKM.1/GP FCS_CKM.4
FCS_COP.1/CA_SHA		See § 1.1.1.1.1 FCS_CKM.4
FCS_COP.1/CA_ENC		FCS_CKM.1/BAC FCS_CKM.4
FCS_COP.1/CA_MAC		FCS_CKM.1/BAC FCS_CKM.4
FCS_RND.1	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5/BAC	No dependencies	n.a.
FIA_UAU.5/MP		
FIA_UAU.5/CA		
FIA_UAU.6/BAC	No dependencies	n.a.
FIA_UAU.6/MP		
FIA_UAU.6/CA		
FIA_AFL.1/BAC	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/MP		
FIA_API.1/CA	No dependencies	n.a.
FDP_ACC.1/BAC	FDP_ACF.1	FDP_ACF.1/BAC
FDP_ACF.1/BAC	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/BAC See § 1.1.1.1.2
FDP_UCT.1/BAC	[FTP_ITC.1, or FTP_TRP.1], [FDP_IFC.1, or FDP_ACC.1]	See § 1.1.1.1.3 FDP_ACC.1/BAC
FDP_UCT.1/CA		See § 1.1.1.1.3 FDP_ACC.1/CA
FDP_UIT.1/BAC	[FTP_ITC.1, or FTP_TRP.1], [FDP_IFC.1, or FDP_ACC.1]	See § 1.1.1.1.3 FDP_ACC.1/BAC
FDP_UIT.1/CA		See § 1.1.1.1.3 FDP_ACC.1/CA
FMT_MOF.1/PROT	FMT_SMF.1	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS		
FMT_MTD.1/KEY_WRITE		
FMT_MTD.1/KEY_READ		
FMT_MTD.1/CAPK		
FMT_MTD.1/CAPK_READ		
FMT_MTD.1/LCS_PERS		
FPT_EMS.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FTP_ITC.1/MP	No dependencies	n.a.

Table 9 Dependencies between the SFR for the TOE

6.3.2.2 Rationale for the exclusion of dependencies

1.1.1.1.1 FCS_COP.1/BAC_SHA, FCS_COP.1/CA_SHA

The hash algorithm required by FCS_COP.1/BAC_SHA, FCS_COP.1/MP_SHA and FCS_COP.1/CA_SHA_SM_TDES does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

1.1.1.1.2 FDP_ACF.1/BAC

The access control TSF according to FDP_ACF.1/BAC 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.

1.1.1.1.3 FDP_UCT.1/BAC, FDP_UIT.1/BAC and FDP_UCT.1/CA and FDP_UIT.1/CA

The SFR FDP_UCT.1/BAC, FDP_UIT.1/BAC, FDP_UCT.1/CA and FDP_UIT.1/CA require 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.
.

7 TOE summary specification

7.1 TOE summary specification

7.1.1 Overview

The TOE provides the following Security Functions (TSF):

TSF	Acronym	Descr.	Phase		
			5	6	7
Access Control in Reading	F.ACR	§ 7.1.2	✓	✓	✓
Access Control in Writing	F.ACW	§ 7.1.3	✓	✓	✓
Basic Access Control	F.BAC	§ 7.1.4	×	×	✓
Chip Authentication	F.CA	§ 7.1.5	✓	×	✓
MRTD Personalization	F.PERS	§ 7.1.6	×	✓	×
Physical Protection	F.PHY	§ 7.1.7	✓	✓	✓
MRTD Pre-personalization	F.PREP	§ 7.1.8	✓	×	×
Secure Messaging	F.SM	§ 7.1.9	✓	✓	✓
Self Tests	F.STST	§ 7.1.10	✓	✓	✓

Table 10 - TSF of the TOE

7.1.2 Access Control in Reading

This function controls access to read functions and enforces the security policy for data retrieval. Prior to any data retrieval, it authenticates the actor trying to access the data, and checks the access conditions are fulfilled as well as the life cycle state. It ensures that at any time, the following keys are never readable:

- Pre-personalization Agent keys and Personalization Agent keys,
- BAC keys,
- CA private key

It ensures the access control to specific data as defined in FAU_SAS.1.

Regarding the file structure:
In the Operational Use phase:

The terminal can read user data, the Document Security Object, (EF.COM, EF.SOD, EF.DG1 to EF.DG16) only after BAC or CA respectively authentication and through a valid secure channel.

In the Production and preparation stage:
The Manufacturer can read the Initialization Data in Stage 2 “Production”. The pre-personalization agent and the Personalization Agent can read only the random identifier in Stage 3 “Preparation” stored in the TOE.
Other data-elements can only be read after they are authenticated by the TOE (using their authentication keys).

It ensures as well that no other part of the memory can be accessed at any time.

The implementation contributes to:

- FIA_UID.1, FIA_UAU.1
- FMT_MTD.1/LCS_PERS, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_READ, FMT_MTD.1/CAPK_READ
- FDP_ACF.1/BAC, FDP_ACC.1/BAC, FDP_ACF.1.2/MP

7.1.3 Access Control in Writing

This function controls access to write functions (in NVM) and enforces the security policy for data writing. Prior to any data update, it authenticates the actor, and checks the access conditions are fulfilled as well as the life cycle state.

Regarding the file structure:

In the Production and preparation stage:
The Manufacturer can write all the Initialization and data for the Pre-personalization. The Personalization Agent can write through a valid secure channel all the data Document Basic Access Keys after it is authenticated by the TOE (using its authentication keys).
The Pre-Personalization Agent can write through a valid secure channel data to be used by the personalization agent (after it is authenticated by the TOE using its authentication keys). The Pre-personalization agent is only active after delivery. The key that is written in the TOE for authentication purposes during manufacturing in meant for the pre-personalization agent. The Pre-personalization agent (which is seen as a sub-role of the Personalization agent) will refresh this key.

In the Operational Use phase:
It is not possible to create any files (system or data files). Furthermore, it is not possible to update any files (system or data files).

The implementation contributes to:

- FDP_ACC.1/BAC and FDP_ACF.1/BAC
- FDP_ACC.1/CA and FDP_ACF.1/CA
- FMT_MTD.1/LCS_PERS
- FMT_MTD.1/INI_DIS
- FMT_MTD.1/KEY_WRITE
- FMT_MTD.1/INI_ENA

7.1.4 Basic Access Control

This TSF provides the Basic Access Control, authentication and session keys generation to be used by F.SM, as described in [ICAO_9303].

The BAC Session Keys are derived from the MRZ of the MRTD's chip: this is done using SHA-1 (FCS_COP.1/BAC_SHA). The authentication initialization requires that the MRTD's chip generate 8 bytes challenge (nonce rPICC) that is read by the Basic Inspection System (FIA_UAU.1), and 16 bytes Key (KPICC) (FCS_RND.1). The MRTD BAC authentication stages also require TDES encryption of 32 bytes of concatenated data and a Retail MAC computation over the 32 bytes of encryption output (FCS_COP.1/BAC_MAC). The Basic Inspection System also generated a pair (K_{PCD}, r_{PCD}). The use of challenges enforces a protection against replay (FIA_UAU.4).
Completion of the BAC Authentication protocol means that a Secure Messaging session, in ENC_MAC_Mode (FCS_COP.1/BAC_ENC), is started with the session keys (KENC and KMAC) derived according to [ICAO_9303] from the common master secret KMaster = KPICC⊕KPCD and a Send Sequence Counter SSC derived from r_{PICC} and r_{PCD} (FCS_CKM.1/BAC).
All further communication with the TOE is handled by F.SM, enforcing confidentiality and integrity over transferred data (FIA_UAU.5).
In case the BAC authentication protocol fails (the TOE being unable to identify the Terminal as being a legitimate Basic Inspection System) the TOE records one authentication failure. If the Terminal reaches a pre-defined amount of successive authentication failures, the BAC Authentication Key is blocked (FIA_AFL.1/BAC).
The implementation contributes also to FDP_ACC.1/BAC and by FDP_ACF.1/BAC for read and write access control management and FMT_SMR.1 for security roles.

7.1.5 Chip Authentication

This TSF provides the Chip Authentication, authentication and session keys generation to be used by F.SM, as described in [TR_03110]. The session keys are obtained using SHA-1 or SHA-256 (FCS_COP.1/CA_SHA).
It also provides management of this function in phase 5.
The implementation contributes to:

- FIA_UAU.5.2/CA
- FIA_UAU.6.1/CA
- FIA_API.1.1/CA
- FDP_UCT.1.1/CA
- FDP_UIT.1.1/CA
- FDP_UIT.1.2/CA
- FMT_MOF.1.1/PROT
- FDP_ACC.1.1/CA
- FDP_ACF.1.1/CA

7.1.6 MRTD Personalization

This security functionality ensures that the TOE, when delivered to the Personalization Agent, provides and requires authentication for data exchange. This authentication is based on a Triple DES and AES authentication mechanism. This function allows to:

- Manage symmetric authentication using Personalization Agent keys,
- Compute session keys to be used by F.SM to establish secure channel according to [GPC_SPE_034] and SCP02/SCP03
- Load user data,
- Load Chip Authentication keys in encrypted mode,
- Set TOE life cycle to Operational Use phase.

The implementation contributes to:

- FCS_CKM.1/GP , FCS_RND.1, FCS_COP.1/AUTH, FCS_COP.1/GP_KEY_DEC,
- FIA_UAU.5/BAC, FIA_AFL.1/MP,
- FDP_ACC.1/BAC, FDP_ACF.1/BAC
- FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/CAPK, FMT_MTD.1/LCS_PERS
- FTP_ITC.1/MP
- FIA_UAU.4

7.1.7 Physical Protection

This Security Function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data and TOE life cycle. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE. It furthermore prevents deploying test features after TOE delivery. This SF also preserve a secure state when any failure is detected or a malfunction occurs.

The implementation contributes to: *FPT_EMS.1*, *FPT_FLS.1* and *FPT_PHP.3*

7.1.8 MRTD Pre-personalization

This security functionality ensures that the TOE, when delivered to the Manufacturer, provides and requires an authentication mechanism for data exchange. This authentication is based on Triple DES symmetric authentication mechanism. This function allows to:

- Manage symmetric authentication using Pre-personalization Agent keys,
- Compute session keys to be used by F.SM to establish secure channel according to [GPC_SPE_034] and SCP02/SCP03
- Load Personalization Agent keys in encrypted mode.

The implementation contributes to:
- FCS_CKM.1/GP, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_KEY_DEC, FCS_RND.1
- FIA_UAU.5/MP, FIA_AFL.1/MP,
- FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_ENA,
- FTP_ITC.1/MP

7.1.9 Secure Messaging

This security functionality ensures the confidentiality, authenticity and integrity of the communication between the TOE and the interface device.
In the operational phase, after a successful Authentication Procedure (i.e. BAC or CA), a secure channel is established, based on Triple DES algorithm in case of BAC and based on Triple DES/AES algorithms in case of CA (according to FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC), such that the TOE is able to verify the integrity and authenticity of exchanged data.
This security functionality also provides a Secure Messaging (SCP02 or SCP03) for the Pre-personalization and Personalization phases. The protocols can be configured to protect the exchanges integrity and/or confidentiality. If an error occurs in the secure messaging layer, the session keys are destroyed.

The implementation contributes to:
- FIA_UAU.1, FIA_UAU.6/BAC, FIA_UAU.6/MP, FIA_UAU.6/CA , FIA_UAU.5/CA
- FCS_CKM.4, FCS_COP.1/BAC_ENC, FCS_COP.1/BAC_MAC, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC,FCS_COP.1/CA_ENC , FCS_COP.1/CA_MAC, and FCS_RND.1
- FDP_UCT.1/BAC, FDP_UCT.1/CA,
- FTP_ITC.1/MP
- FDP_UIT.1/BAC, FDP_UIT.1/CA
- FIA_UAU.4

7.1.10 Self Tests

The TOE performs self-tests to verify the integrity of the TSF data:
- At Reset. The implementation contributes to FPT_TST.1

7.2 SFR and TSF

SFR \ TSF	F.ACR	F.ACW	F.BAC	F.CA	F.PERS	F.PHY	F.PREP	F.SM	F.STST
FAU_SAS.1	✓	×	×	×	×	×	×	×	×
FCS_CKM.1/BAC	×	×	✓	×	×	×	×	×	×
FCS_CKM.1/GP	×	×	×	×	✓	×	✓	×	×
FCS_CKM.1/CA	×	×	×	✓	×	×	×	×	×
FCS_CKM.4	×	×	×	×	×	×	×	✓	×
FCS_COP.1/BAC_SHA	×	×	✓	×	×	×	×	×	×
FCS_COP.1/BAC_ENC	×	×	✓	×	×	×	×	✓	×
FCS_COP.1/AUTH	×	×	×	×	✓	×	×	×	×
FCS_COP.1/BAC_MAC	×	×	✓	×	×	×	×	✓	×
FCS_COP.1/GP_ENC	×	×	×	×	×	×	×	✓	×
FCS_COP.1/GP_AUTH	×	×	×	×	×	×	✓	×	×
FCS_COP.1/GP_MAC	×	×	×	×	×	×	×	✓	×
FCS_COP.1/GP_KEY_DEC	×	×	×	×	✓	×	✓	×	×
FCS_COP.1/CA_SHA	×	×	×	✓	×	×	×	×	×
FCS_COP.1/CA_ENC	×	×	×	×	×	×	×	✓	×
FCS_COP.1/CA_MAC	×	×	×	×	×	×	×	✓	×
FCS_RND.1	×	×	✓	×	✓	×	✓	✓	×
FIA_UID.1	✓	×	×	×	×	×	×	×	×
FIA_UAU.1	✓	×	×	×	×	×	×	×	×
FIA_UAU.4	×	×	✓	×	✓	×	×	✓	×
FIA_UAU.5/BAC	×	×	✓	×	✓	×	×	×	×
FIA_UAU.5/MP	×	×	×	×	×	×	✓	×	×
FIA_UAU.5/CA	×	×	×	×	×	×	×	✓	×
FIA_UAU.6/BAC	×	×	×	×	×	×	×	✓	×
FIA_UAU.6/MP	×	×	×	×	×	×	×	✓	×
FIA_UAU.6/CA	×	×	×	×	×	×	×	✓	×
FIA_AFL.1/BAC	×	×	✓	×	×	×	×	×	×
FIA_AFL.1/MP	×	×	×	×	✓	×	✓	×	×
FIA_API.1/CA	×	×	×	✓	×	×	×	×	×
FDP_ACC.1/BAC	✓	✓	✓	×	✓	×	×	×	×
FDP_ACF.1/BAC	✓	✓	✓	×	✓	×	×	×	×
FDP_UCT.1/BAC	×	×	×	×	×	×	×	✓	×
FDP_UCT.1/CA	×	×	×	×	×	×	×	✓	×
FDP_UIT.1/BAC	×	×	×	×	×	×	×	✓	×
FDP_UIT.1/CA	×	×	×	×	×	×	×	✓	×
FMT_MOF.1/PROT	×	×	×	✓	×	×	×	×	×
FMT_SMF.1	×	×	×	✓	✓	×	✓	×	×
FMT_SMR.1	×	×	✓	×	✓	×	✓	×	×
FMT_LIM.1	×	×	×	×	×	✓	×	×	×
FMT_LIM.2	×	×	×	×	×	✓	×	×	×
FMT_MTD.1/INI_ENA	×	✓	×	×	×	×	✓	×	×
FMT_MTD.1/INI_DIS	✓	✓	×	×	✓	×	×	×	×
FMT_MTD.1/KEY_WRITE	×	✓	×	×	✓	×	×	×	×
FMT_MTD.1/KEY_READ	✓	×	×	×	×	×	×	×	×
FMT_MTD.1/CAPK	×	✓	×	×	✓	×	×	×	×
FMT_MTD.1/CAPK_READ	✓	×	×	×	×	×	×	×	×
FMT_MTD.1/LCS_PERS	×	✓	×	×	✓	×	×	×	×
FPT_EMS.1	×	×	×	×	×	✓	×	×	×
FPT_FLS.1	×	×	×	×	×	✓	×	×	×
FPT_TST.1	×	×	×	×	×	×	×	×	✓
FPT_PHP.3	×	×	×	×	×	✓	×	×	×
FTP_ITC.1/MP	×	×	×	×	✓	×	✓	✓	×
FDP_ACC.1/CA	×	✓	×	✓	×	×	×	✓	×
FDP_ACF.1/CA	×	✓	×	✓	×	×	×	✓	×

Table 11- SFR and TSF

8 GLOSSARY AND ACRONYMS

8.1 Glossary

Term	Definition
Active Authentication	Security mechanism defined in [6] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined in [6] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO_9303]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_9303]
Country Signing CA Certificate (Ccsca)	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [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.
Document Security Object (SOD)	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]
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]
Extended Access Control (EAC)	Security mechanism identified in [ICAO_9303] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	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.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO_9303]

Term	Definition
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO_9303]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer (i.e MRTD packaging responsible).
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_9303]
Improperly document person	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]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (cf.1.3.6.1).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO_9303]
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.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]
Issuing State	The Country issuing the MRTD. [ICAO_9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder, (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16). (6) EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).

Term	Definition
Machine Readable Travel Document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_9303]
Machine Readable Visa (MRV)	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [ICAO_9303]
Machine Readable Zone (MRZ)	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]
Machine-verifiable biometrics feature	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]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [ICAO_9303], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14, EF.DG 16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [ICAOT], p. 14.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.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.
Passive authentication	(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.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf.1.3.9).
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (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) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/BAC, FIA_UAU.5/BAC and FIA_UAU.6/BAC.

Term	Definition
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Pre-Personalisation	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the MRTD Application (c.f.1.3.9 Phase 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (i.e IC 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.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier.
Primary Inspection System (PIS)	An inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
random identifier	Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability.
Receiving State	The Country to which the Traveler is applying for entry. [ICAO_9303]
reference data	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.
secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO_9303]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	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.
Travel document	A passport or other official document of identity issued by a State or Organization, which may be used by the rightful holder for international travel. [ICAO_9303]
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE ([CC_1]).
Unpersonalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalisation Agent from the Manufacturer.
User data	Data created by and for the user, that does not affect the operation of the TSF ([CC_1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single 82nrolee whose identity is being claimed, to determine whether it matches the 82nrolee's template.
Verification data	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.

8.2 Acronyms

Acronym	Term
BIS	Basic Inspection System
CC	Common Criteria
EF	Elementary File
GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number
ISK	Issuer Secret Key
MF	Master File
n.a. or N/A	Not applicable
OSP	Organizational Security Policy
PT	Personalization Terminal
SAR	Security Assurance Requirements
SFR	Security Functional Requirement
TOE	Target Of Evaluation
TSF	TOE Security Functions

9 LITERATURE

Common Criteria

[CC_1] Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", April 2017, Version 3.1 revision 5.

[CC_2] "Common Criteria for information Technology Security Evaluation, Part 2: Security Functional component", April 2017, Version 3.1 revision 5.

[CC_3] "Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance components", April 2017, Version 3.1 revision 5.

[CC_EM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

Protection Profiles

[PP_0002] PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

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

[PP_BAC] Machine readable travel documents with “ICAO Application”, Basic Access control – BSI-PP-0055 v1.10 25th march 2009

[PP_EAC] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0056, Version 1.10, 25th March 2009

IC and Platform

[IC_CERT] Certification Report - BSI-DSZ-CC-0945-V2-2018
[PTF_CERT] NSCIB CC-18-200833

[ST_PTF] FQR 110 8959 Ed 3.0 - ID One Cosmo V9 Essential Public ST

[PTF_AGD1] ID-One Cosmo V9 Application Loading Protection Guidance, FQR: 110 8798, Issue 1. IDEMIA

[PTF_AGD2] ID-One Cosmo V9 Applet Security Recommendations, FQR: 110 8794, Issue 4. IDEMIA

[PTF_AGD_OPE] ID One Cosmo V9.0 Essential Reference Guide, 22 October 2018, FQR 110 8823 Ed5. IDEMIA

[PTF_AGD_PRE] ID One Cosmo V9.0 Essential - Pre-Perso Guide, FQR 110 8797 Ed5. IDEMIA

[PTF_AGD_SEC_AC] Secure acceptance and delivery of sensitive element - FQR 110 8921 Ed1, IDEMIA

[Applet_Perso_Guide] FQR 220 1306– CombICAO Applet – Perso Guide Ed 8. IDEMIA

[Applet_User_Guide] FQR 220 1307– CombICAO Applet – User Guide Ed 9. IDEMIA

ICAO

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015 – Security Mechanisms for MRTDs

[ICAOT] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

[ICAO_TR_SAC] ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

ISO

[ISO_9797_1] ISO/IEC 9797-1 Information technology – Security techniques – Message Authentication codes (MACs) – part 1: Mechanisms using a block cipher, Second edition 2011-03-01

[ISO_15946-3] ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment, 2002

IDEMIA

[ALC_KM] Key management for Flash code, I CRD13 2 CRD 512 03, January 2016

[ALC_SCT] ID division: sensitive code transfer, I/R&D/2/SQA 515 01, March 2010

[ALC_STM] Secure transfer of masks, I CRD13 2 CRD 507 04, January 2012

Other

[TR_03110] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[FIPS_180_3] "FIPS PUB 180-3, Secure Hash Standard"
October 2008 , National Institute of Standards and Technology

[FIPS_46_3] FIPS 46-3, Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard (DES), 1999 October 25

[FIPS_186_3] FIPS 186-3, Federal Information Processing Standards Publication (FIPS PUB) 186-3, Digital Signature Standard (DSS), June 2009

[FIPS_197] FIPS 197, Federal Information Processing Standards Publication (FIPS PUB 197), Advanced Encryption Standard (AES)

[NIST_800_38B] NIST Special Publication 800-38B: 2005, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005

[GPC_SPE_034] “GlobalPlatform Card Specification“ Version 2.3 Public Release - October 2015

Document Reference: GPC_SPE_034

[GPC_SPE_014] GlobalPlatform Card Technology - Secure Channel Protocol '03', Card Specification v2.2 – Amendment D Version 1.1.1 - Public Release July 2014

[RGS2_B1] Référentiel Général de Sécurité version 2.0 – Annexe B1 – Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014.