CombICAO Applet in EAC Configuration on Cosmo v9

Public Security Target

© IDEMIA. All rights reserved.

Specifications and information are subject to change without notice.

The products described in this document are subject to continuous development and improvement.

All trademarks and service marks referred to herein, whether registered or not in specific countries, are the properties of their respective owners.

- Printed versions of this document are uncontrolled -

DOCUMENT MANAGEMENT

Business Unit – Department	**PSI**
Document type	**Public FQR**
Document Title	**CombICAO Applet in EAC Configuration on Cosmo v9 Public Security Target**
FQR No	**110 9317**
FQR Issue	**3**

DOCUMENT REVISION

Date	Revision	Modification
14/10/2019	1.0	Creation based on the full ST
29/10/2019	2.0	Update AGD version
20/11/2019	3.0	Review and Update

Table of contents

Table of figures

Table of tables

1. GENERAL

1.1 Introduction

This public security target describes the security needs induced by the CombICAO Applet product in EAC configuration on IDEMIA underlying Java Card *ID-ONE Cosmo V9 Essential*, see 2.1.2 .

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 within the security environment, and that the TOE summary specification addresses the requirements.

1.2 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 current ST addresses CombICAO Applet in eMRTD configuration 1) below.
Four configurations are considered (others configurations are out of the scope of this ST):

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

2. ST INTRODUCTION

2.1 Public ST reference and TOE reference

2.1.1 ST reference

Title	CombICAO Applet in EAC configuration on Cosmo V9 – Security Target
ST Identification	FQR 110 9317
ST Version	3
Authors	IDEMIA
ITSEF	Brightsight
Certification Body	TÜV Rheinland Nederland B.V.
EAL	EAL5 augmented with: • AVA_VAN.5 • ALC_DVS.2
PP	[PP_EAC]

Table 1 ST reference

2.1.2 TOE reference

Product Name	CombICAO Applet
TOE Name	CombICAO Applet in EAC configuration on ID-ONE Cosmo V9 Essential
Developer Name	IDEMIA
TOE Identification	SAAAAR code: *203297*
Platform Name	ID-One Cosmo V9 Essential Platform
Platform Identification	089233
Platform Certificate	[PTF_CERT]
Guidance documents	[Applet_Perso_Guide], [Applet_User_Guide] [PTF_AGD_PRE], [PTF_AGD_OPE], [PTF_AGD1], [PTF_AGD2] and [PTF_AGD3]

Table 2 TOE reference

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

2.2 TOE overview

2.2.1 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.

This security target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. Also it addresses the Chip Authentication Version 1 described in [TR_03110] as an alternative to the Active Authentication stated in [ICAO_9303].

During the prepersonalization and 9ersonalization, 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 or CAN	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.

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this ST as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfill the ‘Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application”, Basic Access Control’ [PP_BAC]. Due to the fact that [PP_BAC] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately.

There are separate Security Targets for BAC and EAC. Note, that the claim for conformance to the BAC-PP [PP_BAC] does not require the conformance claim to [PP_EAC]. Nevertheless claiming conformance of [PP_EAC] requires that the TOE meets a (separate) ST conforming to the BAC-PP [PP_BAC].

For BAC, the inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD’s chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO_9303], normative appendix 5.

The Security Target requires the TOE to implement the Extended Access Control as defined in [TR_03110]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol and (ii) the Terminal Authentication Protocol. The Chip Authentication Protocol (i) authenticates the MRTD’s chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication can only be performed if Chip Authentication has been successfully executed. The Terminal Authentication Protocol consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

2.2.2 TOE type

The TOE is a composite product made up of an Embedded Software developed using Java Card technology, composed on a Java Card open platform. Both developed by IDEMIA.

The underlying Java Card open platform has already been certified, please see [PTF_CERT].

The TOE embedded is the dual (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 :

- Extended Access Control (EAC)

Please refer to 2.3.2 TOE delivery section for more details on TOE deliveries

2.2.3 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.

2.3 TOE description

2.3.1 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.

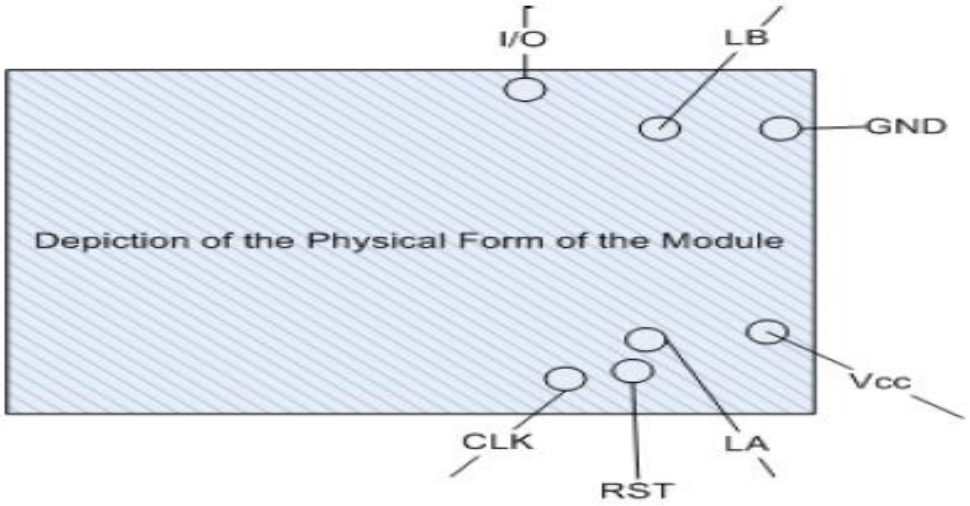

Figure 1 Physical Form of the Module

2.3.2 TOE delivery

The TOE is composed of:

- Circuitry of the MRTD's chip (the IC) :
- 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
- Associated guidance documentation (delivered in electronic version)

This 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_Uder_Guide]		
Underlying platform guidance	[PTF_AGD_OPE] [PTF_AGD1] [PTF_AGD2] [PTF_AGD3] [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

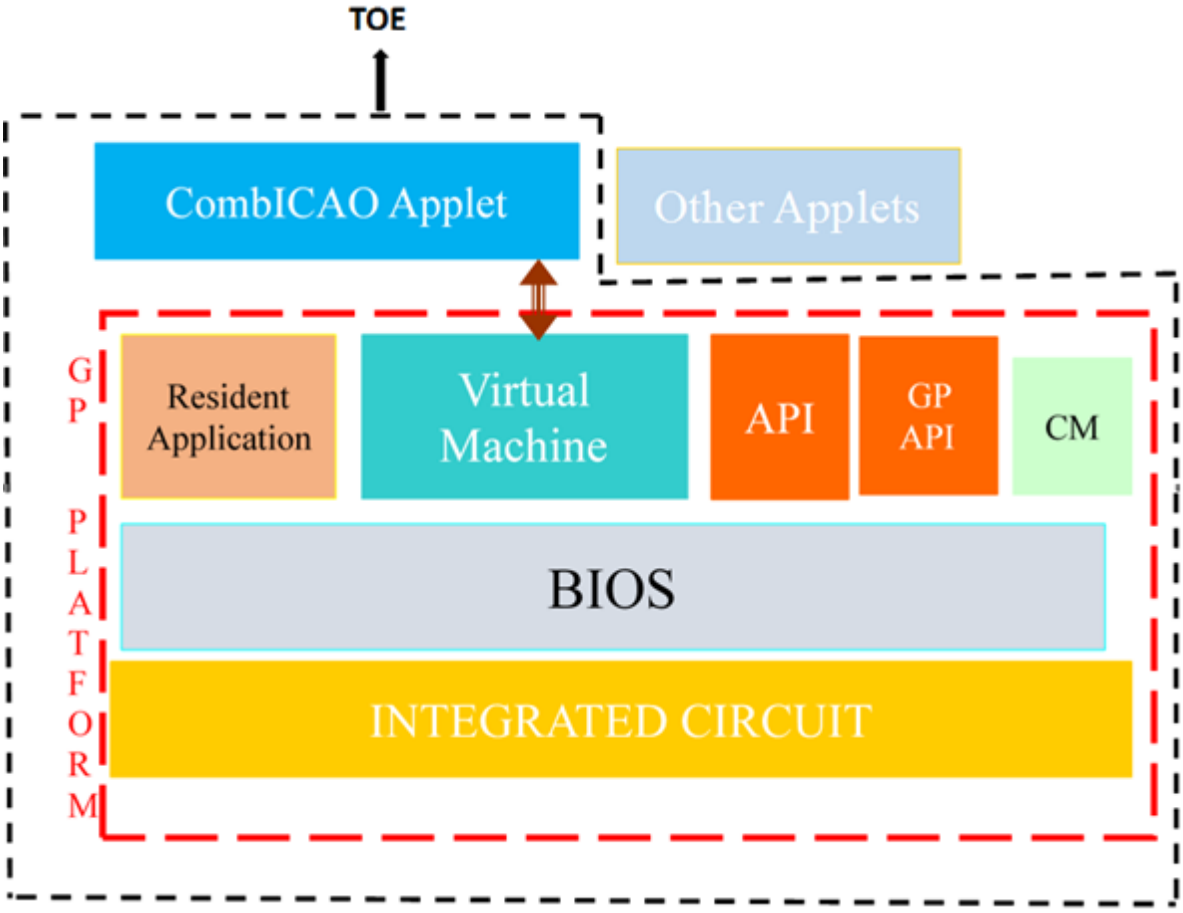

Figure 2 TOE Boundaries

2.3.3 Logical scope of the TOE

The TOE is a smartcard, composed of:

- IC,
- Java Card Open Platform (OS) and
- CombICAO application (logical data structure).

The TOE scope encompasses the following features:

- Chip Authentication
- Terminal Authentication
- Extended Access Control
- Personalization Phase
- Prepersonalization phase

The prepersonalization and personalisation are performed by the Manufacturer and the Personalisation Agent, which controls the TOE. All along this phase, the TOE is self-protected, as it requires the authentication of the Manufacturer and the Personalisation Agent prior to any operation. By being authenticated, the Personalisation Agent 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.

2.3.4 Authentication Protocols

2.3.4.1 Terminal Authentication (TA)

This protocol enables the MRTD chip to verify that the terminal is entitled to access sensitive data. As the terminal may access sensitive data afterwards, all further communication MUST be protected appropriately. Terminal Authentication therefore also authenticates an ephemeral public key chosen by the terminal that was used to set up Secure Messaging with Chip Authentication. The MRTD chip MUST bind the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key of the terminal.

Terminal Authentication v1 is part of the EACv1 procedure defined in [TR_03110].

2.3.4.2 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.

Chip Authentication v1 is part of the EACv1 procedure defined in [TR_03110].

2.3.5 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_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 3 BAC Configuration

2.3.6 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).

2.3.7 Enhanced protection over Sensitive biometric data reading

The access to sensitive biometric data: the fingerprint and iris stored in DG3 and DG4 are protected in accordance with the requirements of the protection profile and specification. Beyond that, the TOE also provides a feature able to ensure a high level of confidentiality when reading these data. The TOE supports a mechanism enforcing to use a minimum cryptographic strength for the confidentiality, integrity and authenticity protection of these sensitive biometric data when being read. This may be useful for issuing authority that do not consider DES algorithm strong enough to ensure a sufficient level of confidentiality. This mechanism allows the TOE to enforce the terminal using a stronger algorithm such as AES 128, or 192 bits, or 256 bits when reading the sensitive biometric data, and deny access to them if this condition is not met (algorithm not strong enough).

The enhanced protection over sensitive biometric data reading is part of the TOE and is also part of the TSF.

2.4 Life Cycle

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

Roles		*Subject*
IC developer		IC Manufacturer
TOE developer		IDEMIA
Manufacturer	IC manufacturer	IC Manufacturer
	MRTD packaging responsible	IDEMIA or another agent
		IDEMIA
	Embedded software loading responsible	IDEMIA
	Pre-personalization Agent (Manufacturer Role)	IDEMIA or another agent
Personalization Agent		IDEMIA or another agent

Table 4 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].

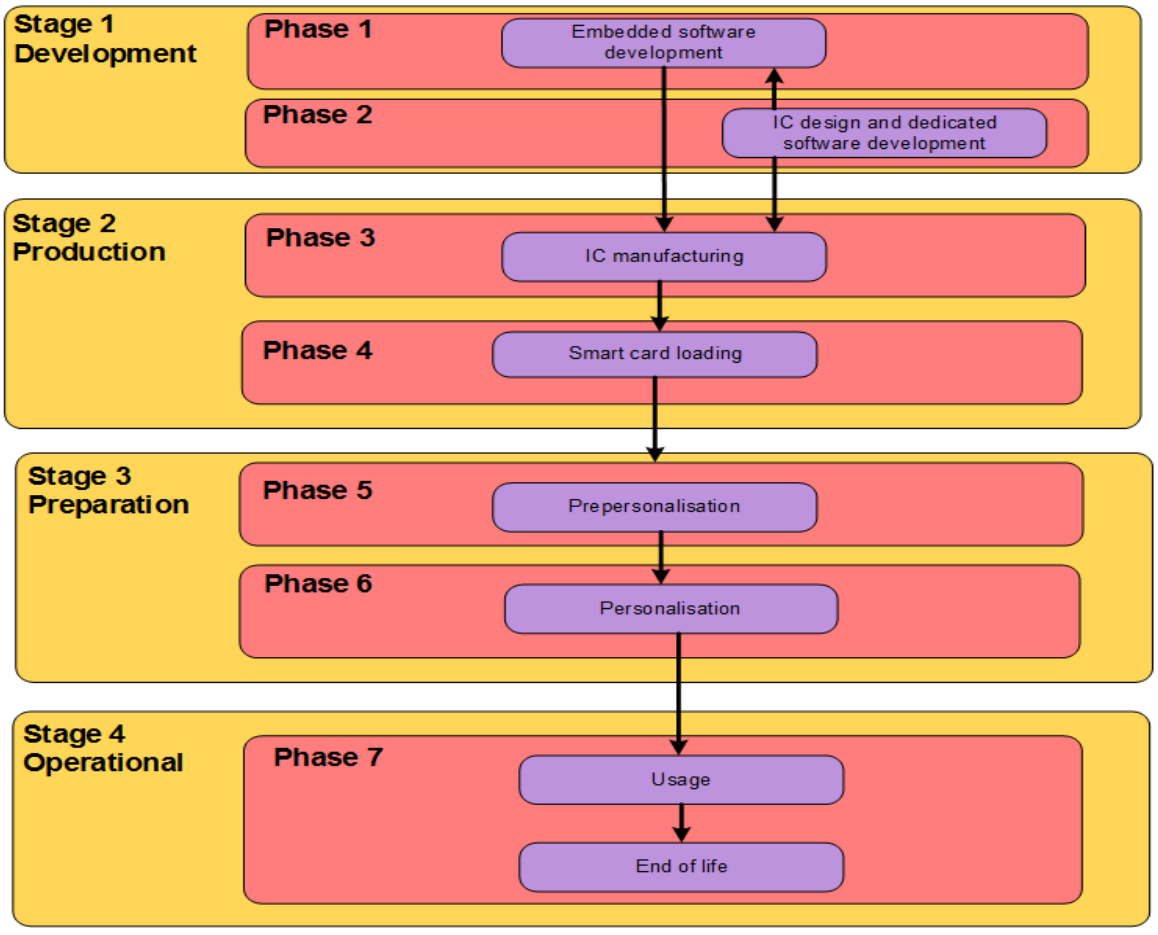

Figure 3 Life cycle Overview

2.4.1 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Java Card 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 (Java Card 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	IC Manufacturer	IC Manufacturer Refer to [PTF_CERT]	ALC

2.4.2 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 Java Card 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 Java Card platform) to be flashed in the IC to the IC manufacturer in the phase 3. Once the Java Card 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 Java Card platform by the smart card loader in phase 4 at IDEMIA audited site.

Or

- **(Option 3)** the developer sends the image (containing both the Java Card 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 platform and applet	manufacturer	IC manufacturer production plants [PTF_CERT]	ALC
Smart card loader	-	-	-	-
TOE Delivery Point				

Table 5 Image containing both Java Card platform and applet is loaded at IC manufacturer (Option 1)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing only Java Card Platform	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 6 Cap file of CombICAO applet is loaded (using GP) (Option 2)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	-	-	-	-
TOE Delivery Point				
Smart card loader	Image containing both the platform and applet	IDEMIA or another agent	Any	AGD

Table 7 Image containing both platform and applet is loaded through the loader of the IC (Option 3)

2.4.3 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].

2.4.4 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 [Applet_User_Guide] of the TOE.

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

.

3. Conformance claims

3.1 Common Criteria conformance

This Public Security Target (ST) claims conformance to [CC_2] and [CC_3].

The conformance to the CC is claimed as follows:

CC	**Conformance Claim**
Part 2	Conformance with extensions: • FAU_SAS.1 *"Audit storage",* • FCS_RND.1 *"Quality metric for random numbers",* • 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 EAL5 augmented with: • ALC_DVS.2 *"Sufficiency of security measures"* defined in [CC_3], • AVA_VAN.5 *"Advanced methodical vulnerability analysis"* defined in [CC_3]

Table 8 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_EAC] has been renamed to FPT_EMS.1, in order to keep the SFR formatting.

3.2 Protection Profile conformance

3.2.1 Overview

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

Title	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control
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-0056

Table 9 Protection Profile conformance

This ST also addresses the Manufacturing and Personalization phases at TOE level (cf. §2.4 TOE life cycle).

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

[2] FIA_API.1 has been added to this security target for the needs of the Chip Authentication Protocol.

The following parts list assumptions, threats, OSP, OT and OE for this TOE (i.e. from [PP_EAC] and additional).

3.2.2 Assumptions

The following Assumptions are assumed for this TOE:

- **A.MRTD_Manufact** *"MRTD manufacturing on steps 4 to 6"* defined in [PP_EAC],
- **A.MRTD_Delivery** *"MRTD delivery during steps 4 to 6"* defined in [PP_EAC],
- **A.Pers_Agent** *"Personalization of the MRTD's chip"* defined in [PP_EAC],
- **A.Insp_Sys** *"Inspection Systems for global interoperability"* defined in [PP_EAC],
- **A.Signature_PKI** *"PKI for Passive Authentication"* defined in [PP_EAC],
- **A.Auth_PKI** *"PKI for Inspection Systems"* defined in [PP_EAC],

3.2.3 Threats

This TOE averts the following threats:

- **T.Read_Sensitive_Data** *"Read the sensitive biometric reference data"* defined in [PP_EAC],
- **T.Forgery** "Forgery of data on MRTD's chip" defined in [PP_EAC],
- **T.Counterfeit** *"MRTD's chip"* defined in [PP_EAC],
- **T.Abuse-Func** "Abuse of Functionality" defined in [PP_EAC],
- **T.Information_Leakage** "Information Leakage from MRTD's chip" defined in [PP_EAC],
- **T.Phys-Tamper** "Physical Tampering" defined in [PP_EAC],
- **T.Malfunction** *"Malfunction due to Environmental Stress"* defined in [PP_EAC],
- **T.Configuration** *"Tampering attempt of the TOE during preparation"* defined in this ST,
- **T.Forgery_Supplemental_Data** *"Forgery of supplemental data stored in the TOE"* defined in this ST.

3.2.4 Organizational Security Policies

This TOE complies with the following OSP:

- **P.BAC-PP** "*Fulfillment of the Basic Access Control Protection Profile"* defined in [PP_EAC],
- **P.Sensitive_Data** *"Privacy of sensitive biometric reference data"* defined in [PP_EAC],
- **P.Manufact** *"Manufacturing of the MRTD's chip"* defined in [PP_EAC],
- **P.Personalization** *"Personalization of the MRTD by issuing State or Organization only"* defined in [PP_EAC]

3.2.5 Security Objectives

The Security Objectives for this TOE are the following:

- **OT.AC_Pers** *"Access Control for Personalization of logical MRTD"* defined in [PP_EAC],
- **OT.Data_Int** *"Integrity of personal data"* defined in [PP_EAC],
- **OT.Sens_Data_Conf** *"Confidentiality of sensitive biometric reference data"* defined in [PP_EAC],
- **OT.Identification** *"Identification and Authentication of the TOE"* defined in [PP_EAC],
- **OT.Chip_Auth_Proof** *"Proof of MRTD's chip authenticity"* defined in [PP_EAC],
- **OT.Prot_Abuse-Func** *"Protection against Abuse of Functionality"* defined in [PP_EAC],
- **OT.Prot_Inf_Leak** *"Protection against Information Leakage"* defined in [PP_EAC],
- **OT.Prot_Phys-Tamper** *"Protection against Physical Tampering"* defined in [PP_EAC],

- **OT.Prot_Malfunction** *"Protection against Malfunctions"* defined in [PP_EAC],
- **OT.Configuration** *"Protection of the TOE preparation"* defined in this ST,
- **OT.Update_File** *"Modification of file in Operational Use Phase"* defined in this ST,
- **OT.AC_SM_Level** *"Access control to sensitive biometric reference data according to SM level"* defined in this ST.

The Security Objectives for the environment of this TOE are the following:

- **OE.MRTD_Manufact** *"Protection of the MRTD Manufacturing"* defined in [PP_EAC],
- **OE.MRTD_Delivery** *"Protection of the MRTD delivery"* defined in [PP_EAC],
- **OE.Personalization** *"Personalization of logical MRTD"* defined in [PP_EAC],
- **OE.Pass_Auth_Sign** *"Authentication of logical MRTD by Signature"* defined in [PP_EAC],
- **OE.Auth_Key_MRTD** *"MRTD Authentication Key"* defined in [PP_EAC],
- **OE.Authoriz_Sens_Data** *"Authorization for Use of Sensitive Biometric Reference Data"* defined in [PP_EAC],
- **OE.BAC_PP** *"Fulfillment of the Basic Access Control Protection Profile"* defined in [PP_EAC],
- **OE.Exam_MRTD** *"Examination of the MRTD passport book"* defined in [PP_EAC],
- **OE.Passive_Auth_Verif** *"Verification by Passive Authentication"* defined in [PP_EAC],
- **OE.Prot_Logical_MRTD** *"Protection of data from the logical MRTD"* defined in [PP_EAC],
- **OE.Ext_Insp_Systems** *"Authorization of Extended Inspection Systems"* defined in [PP_EAC].

3.3 CC conformance and usage in real life

In the real life, for interoperability purposes, the MRTD will most likely support BAC, PACE and EAC.

- If the terminal reads the content of the MRTD by performing BAC then EAC, the security of the MRTD will be covered by the security evaluation of (1) the TOE described by the ST claiming compliance to [PP_BAC] and (2) the TOE described by the ST claiming compliance to [PP_EAC], assuming PACE is not supported (as not used for the inspection procedure)
- If the terminal reads the content of the MRTD by performing PACE then EAC, the security of the MRTD will be covered by the security evaluation of the TOE described by the ST claiming compliance to [PP_EACwPACE], assuming BAC is not supported (as not used for the inspection procedure).

4. Security Problem Definition

4.1 Assets

Logical MRTD sensitive User Data

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

Application Note:

Due to interoperability reasons the 'ICAO Doc 9303' [ICAO_9303] requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG16. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [PP_BAC]).

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.

4.2 Users / Subjects

Manufacturer

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

Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [ICAO_9303].

Country Verifying Certification Authority

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

Document Verifier

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

Terminal

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

Inspection system (IS)

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

MRTD Holder

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

Traveler

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

Attacker

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

Application Note:

Note that an attacker trying to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD) is not considered by this ST since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys that is covered by [PP_BAC]. The same holds for the confidentiality of the user data EF.DG1, EF.DG2, EF.DG5 to EF.DG16 as well as EF.SOD and EF.COM.

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

4.3 Threats

T.Read_Sensitive_Data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [PP_BAC]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document

Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.

Threat agent: having high attack potential, knowing the Document Basic Access Keys, being in possession of a legitimate MRTD

Asset: confidentiality of sensitive logical MRTD (i.e. biometric reference) data,

T.Forgery

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 high attack potential, being in possession of one or more legitimate MRTDs

Asset: authenticity of logical MRTD data,

T.Counterfeit

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,

T.Abuse-Func

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

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

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

T.Information_Leakage

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 high attack potential, being in possession of a legitimate MRTD

Asset: confidentiality of logical MRTD and TSF data

T.Phys-Tamper

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 high attack potential, being in possession of a legitimate MRTD

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

T.Malfunction

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 high attack potential, being in possession of a legitimate MRTD

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

T.Configuration

Adverse action: An attacker may access to the TOE at Manufacturing and Personalization phases (steps 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

T. Forgery_Supplemental_Data

Adverse action: An attacker alters fraudulently the data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object. This may lead the extended inspection system (EIS) using these data to be deceived.

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

Asset: authenticity of data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object

4.4 Organisational Security Policies

P.BAC-PP

The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the [ICAO_9303] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP_BAC] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

Application Note:

The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [ICAO_9303] is addressed by the [PP-BAC] (cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG3 and EF.DG4 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [PP-BAC]). The TOE shall protect the sensitive biometric reference data in EF.DG3 and EF.DG4 against attacks with high attack potential. Due to the different resistance the protection of EF.DG3 and EF.DG4 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 are addressed separated protection profiles, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates (cf. also to application note 1).

P.Sensitive_Data

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the MRTD holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the MRTD is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The MRTD's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication.

P.Manufact

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

P.Personalization

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.

4.5 Assumptions

A.MRTD_Manufact

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

A.MRTD_Delivery

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

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

A.Pers_Agent

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

A.Insp_Sys

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. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports 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.

A.Signature_PKI

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.

A.Auth_PKI

The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their MRTD's chip.

5. Security Objectives

5.1 Security Objectives for the TOE

OT.AC_Pers

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.DG3 to EF.DG16 are added.

Application Note:

The OT.AC_Pers implies that

(1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,

(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

OT.Data_Int

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 the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

OT.Sens_Data_Conf

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

OT.Identification

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre- Personalization data includes writing of the Personalization Agent Key(s).

OT.Chip_Auth_Proof

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [TR_03110]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

Application Note:

The OT.Chip_Auth_Proof implies the MRTD's chip to have (i) a unique identity as given by the MRTD's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [ICAO_9303] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

OT.Prot_Abuse-Func

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE. Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.Prot_Inf_Leak

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

Application Note:

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

OT.Prot_Phys-Tamper

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 high attack potential by means of

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

with a prior

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

OT.Prot_Malfunction

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.

Application Note:

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

OT.Configuration

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.

OT.Update_File

During Operational Use phase, the TOE must allow the modification of Updatable Data if the write access to these objects is fulfilled by the Terminal.

OT.AC_SM_Level

During Operational Use phase, the TOE must allow read access to sensitive biometric data only if the Secure Messaging level reaches or exceeds the one specified in the biometric data Access Conditions data object.

5.2 Security Objectives for the Operational Environment

5.2.1 Issuing State or Organization

OE.MRTD_Manufact

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

OE.MRTD_ Delivery

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.

OE.Personalization

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

OE.Pass_Auth_Sign

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 to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO_9303].

OE.Auth_Key_MRTD

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data

The issuing State or Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of MRTD's holders to authorized receiving States or Organizations. The Country Verifying Certification Authority of the issuing State or Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

OE.BAC_PP

It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP_BAC]. This is necessary to cover the BAC mechanism ensuring the confidentiality of

standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

5.2.2 Receiving State or Organization

OE.Exam_MRTD

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 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]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

OE.Passive_Auth_Verif

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

OE.Prot_Logical_MRTD

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

Application Note:

The figure 2.1 in [TR_03110] supposes that the GIS and the EIS follow the order (i) running the Basic Access Control Protocol, (ii) reading and verifying only those parts of the logical MRTD that are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key), (iii) running the Chip Authentication Protocol, and (iv) reading and verifying the less-sensitive data of the logical MRTD after Chip Authentication. The supposed sequence has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. The inspection system will prevent additionally eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. Note that reading the lesssensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this ST. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

OE.Ext_Insp_Systems

The Document Verifier of receiving States or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical MRTD. The Extended Inspection System authenticates themselves to the MRTD's chip for access to the sensitive biometric

reference data with its private Terminal Authentication Key and its Inspection System Certificate.

5.3 Security Objectives Rationale

5.3.1 Threats

T.Read_Sensitive_Data The threat T.Read_Sensitive_Data "Read the sensitive biometric reference data" is countered by the TOE-objective OT.Sens_Data_Conf "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by OE.Authoriz_Sens_Data "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems".

This threat is also covered by OT.AC_SM_Level "Access control to sensitive biometric reference data according to SM level" that enhences this protection by allowing the issuing State or Organization to require the usage of a secure messaging with a minimum security level for accessing the sensitive biometric reference data. The strength of the secure messaging is tightly bound to the underlying block Cipher involved (DES, AES-128/192/256). This objective allows an issuing State or Organization to set a secure messaging level it considers as sufficient to ensure a long term confidentiality of the sensitive biometric data of its citizen when being read.

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. 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".

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 authentication" 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_Key_MRTD "MRTD Authentication Key". According to OE.Exam_MRTD "Examination of the MRTD

passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip.

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

T.Information_Leakage The threat T.Information_Leakage "Information Leakage from MRTD's chip", is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Prot_Inf_Leak "Protection against Information Leakage".

T.Phys-Tamper The threat T.Phys-Tamper "Physical Tampering" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Prot_Phys-Tamper "Protection against Physical Tampering".

T.Malfunction The threat T.Malfunction "Malfunction due to Environmental Stress" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Prot_Malfunction "Protection against Malfunctions".

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".

T. Forgery_Supplemental_Data The threat T. Forgery_Supplemental_Data "Forgery of supplemental data stored in the TOE" addresses the fraudulent alteration of Updatable Data. The TOE protects the update of these data thanks to OT.Update_File "Modification of file in Operational Use Phase" that ensures inspection system are authenticated and data to be updated are sent through a secure channel ensuring integrity, authenticity and confidentiality.

5.3.2 Organisational Security Policies

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

P.Sensitive_Data The OSP P.Sensitive_Data "Privacy of sensitive biometric reference data" is fulfilled by the TOE-objective OT.Sens_Data_Conf "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by OE.Authoriz_Sens_Data "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems".

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.

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.

5.3.3 Assumptions

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

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

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.

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" which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip. The security objectives for the TOE environment OE.Prot_Logical_MRTD "Protection of data from the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

A.Signature_PKI The assumption A.Signature_PKI "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment OE.Pass_Auth_Sign "Authentication of logical MRTD by Signature" covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by OE.Exam_MRTD "Examination of the MRTD passport book".

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

5.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Read_Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems, OT.AC_SM_Level	Section 5.3.1
T.Forgery	OT.AC_Pers, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Pass_Auth_Sign, OE.Exam_MRTD, OE.Passive_Auth_Verif	Section 5.3.1
T.Counterfeit	OT.Chip_Auth_Proof, OE.Auth_Key_MRTD, OE.Exam_MRTD	Section 5.3.1
T.Abuse-Func	OT.Prot_Abuse-Func	Section 5.3.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 5.3.1
T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 5.3.1
T.Malfunction	OT.Prot_Malfunction	Section 5.3.1
T.Configuration	OT.Configuration	Section 5.3.1
T. Forgery_Supplemental_Data	OT.Update_File	Section 5.3.1

Table 10 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.AC_Pers	T.Forgery
OT.Data_Int	T.Forgery
OT.Sens_Data_Conf	T.Read_Sensitive_Data
OT.Identification	
OT.Chip_Auth_Proof	T.Counterfeit
OT.Prot_Abuse-Func	T.Abuse-Func
OT.Prot_Inf_Leak	T.Information_Leakage
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper
OT.Prot_Malfunction	T.Malfunction
OT.Configuration	T.Configuration
OT.Update_File	T. Forgery_Supplemental_Data
OT.AC_SM_Level	T.Read_Sensitive_Data
OE.MRTD_Manufact	
OE.MRTD_ Delivery	
OE.Personalization	
OE.Pass_Auth_Sign	T.Forgery
OE.Auth_Key_MRTD	T.Counterfeit
OE.Authoriz_Sens_Data	T.Read_Sensitive_Data
OE.BAC_PP	
OE.Exam_MRTD	T.Forgery, T.Counterfeit
OE.Passive_Auth_Verif	T.Forgery
OE.Prot_Logical_MRTD	
OE.Ext_Insp_Systems	T.Read_Sensitive_Data

Table 11 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.BAC-PP	OE.BAC_PP	Section 5.3.2
P.Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 5.3.2
P.Manufact	OT.Identification	Section 5.3.2
P.Personalization	OT.AC_Pers, OT.Identification, OE.Personalization	Section 5.3.2

Table 12 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.AC_Pers	P.Personalization
OT.Data_Int	
OT.Sens_Data_Conf	P.Sensitive_Data
OT.Identification	P.Manufact, P.Personalization
OT.Chip_Auth_Proof	
OT.Prot_Abuse-Func	
OT.Prot_Inf_Leak	
OT.Prot_Phys-Tamper	
OT.Prot_Malfunction	
OT.Configuration	
OT.Update_File	
OT.AC_SM_Level	
OE.MRTD_Manufact	
OE.MRTD_ Delivery	
OE.Personalization	P.Personalization
OE.Pass_Auth_Sign	
OE.Auth_Key_MRTD	
OE.Authoriz_Sens_Data	P.Sensitive_Data
OE.BAC_PP	P.BAC-PP
OE.Exam_MRTD	
OE.Passive_Auth_Verif	
OE.Prot_Logical_MRTD	
OE.Ext_Insp_Systems	P.Sensitive_Data

Table 13 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.MRTD_Manufact	OE.MRTD_Manufact	Section 5.3.3
A.MRTD_Delivery	OE.MRTD_ Delivery	Section 5.3.3
A.Pers_Agent	OE.Personalization	Section 5.3.3
A.Insp_Sys	OE.Exam_MRTD, OE.Prot_Logical_MRTD	Section 5.3.3
A.Signature_PKI	OE.Pass_Auth_Sign, OE.Exam_MRTD	Section 5.3.3
A.Auth_PKI	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 5.3.3

Table 14 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.MRTD_Manufact	A.MRTD_Manufact
OE.MRTD_ Delivery	A.MRTD_Delivery
OE.Personalization	A.Pers_Agent
OE.Pass_Auth_Sign	A.Signature_PKI
OE.Auth_Key_MRTD	
OE.Authoriz_Sens_Data	A.Auth_PKI
OE.BAC_PP	
OE.Exam_MRTD	A.Insp_Sys, A.Signature_PKI
OE.Passive_Auth_Verif	
OE.Prot_Logical_MRTD	A.Insp_Sys
OE.Ext_Insp_Systems	A.Auth_PKI

Table 15 Security Objectives for the Operational Environment and Assumptions - Coverage

6. Extended Requirements

6.1 Extended Families

6.1.1 Extended Family FPT_EMS - TOE Emanation

6.1.1.1 Description

The additional 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 SCD 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, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

6.1.1.2 Extended Components

Extended Component FPT_EMS.1

Description

This family defines requirements to mitigate intelligible emanations.

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.

Definition

FPT_EMS.1 TOE Emanation

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].

Dependencies: No dependencies.

6.1.2 Extended Family FMT_LIM - Limited capabilities

6.1.2.1 Description

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 abuse of functions by limiting the capabilities of the functions and by limiting their availability.

6.1.2.2 Extended Components

Extended Component FMT_LIM.1

Description

Definition

FMT_LIM.1 Limited capabilities

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

Dependencies: No dependencies.

Extended Component FMT_LIM.2

Description

Definition

FMT_LIM.2 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]

Dependencies: No dependencies.

6.1.3 Extended Family FAU_SAS - Audit data storage

6.1.3.1 Description

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.

6.1.3.2 Extended Components

Extended Component FAU_SAS.1

Description

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

Definition

FAU_SAS.1 Audit storage

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.

Dependencies: No dependencies.

6.1.4 Extended Family FIA_API - Authentication Proof of Identity

6.1.4.1 Description

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.

Application note 10: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [CC_3], chapter 'Explicitly stated IT security requirements (APE_SRE)') from a TOE point of view.

6.1.4.2 Extended Components

Extended Component FIA_API.1

Description

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

Definition

FIA_API.1 Authentication Proof of Identity

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

Dependencies: No dependencies.

6.1.5 Extended Family FCS_RND - Generation of random numbers

6.1.5.1 Description

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

6.1.5.2 Extended Components

Extended Component FCS_RND.1

Description

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

Definition

FCS_RND.1 Quality metric for random numbers

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

Dependencies: No dependencies.

7. Security Requirements

7.1 Security Functional Requirements

7.1.1 Class FAU Security Audit

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

FAU_SAS.1 Audit storage

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

7.1.2 Class FCS Cryptographic Support

FCS_CKM.1/CA Cryptographic key generation

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 [ISO_11770]** and specified cryptographic key sizes **192 to 512 bit** that meet the following: **[TR_03110]**.

Application Note:

ISO-15946 defined in the protection profile has been replaced since Part 3 that dealt with Key Management using Elliptic Curve has been withdrawn and instead revised by [ISO_11770]

FCS_CKM.1/CA_DATA_GEN Cryptographic key generation

FCS_CKM.1.1/CA_DATA_GEN The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below**

Algorithm	Key Size	Standard
Chip Authentication Data Generation using DH keys compliant to PKCS#3	**1024 to 2048 bits in steps of 512 bits**	**PKCS#3**
Chip authentication data generation using ECDH keys compliant to [ISO_15946]	**192 to 512 bits**	**[TR_03111]**

.

FCS_CKM.1/GP Cryptographic key generation

FCS_CKM.1.1/GP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below:**

Key Generation Algorithm	Key Sizes	Standard
Triple-DES in CBC mode	112 bit	[GPC_SPE_034]
AES in CBC mode	128, 192 and 256	[GPC_SPE_014]

.

FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1 and SHA-256** and cryptographic key sizes **none** that meet the following: **[FIPS_180_4]**.

FCS_COP.1/SYM Cryptographic operation

FCS_COP.1.1/SYM The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging-encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[TR-03110]
secure messaging-encryption and decryption	TDES in CBC mode	112 bits	[TR-03110]

.

FCS_COP.1/MAC Cryptographic operation

FCS_COP.1.1/MAC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

Cryptographic Operations	Algorithms	Key sizes	Standard
secure messaging - message authentication code	AES CMAC	128, 192 and 256 bits	[TR-03110]
secure messaging - message authentication code	Retail MAC	112 bits	[TR-03110]

.

FCS_COP.1/SIG_VER Cryptographic operation

FCS_COP.1.1/SIG_VER The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

Cryptographic Operation	Algorithm	Key Sizes
digital signature verification	ECDSA with SHA-1, SHA-224 and SHA-256 as defined in [FIPS_186_3]	192 to 512
digital signature verification	RSA PKCS#1 v1.5 with SHA-1, SHA-256 and SHA-512	1024, 1536, 2048
digital signature verification	RSA PKCS#1-PSS with SHA-1, SHA-256 and SHA-512	1024, 1536, 2048

.

FCS_COP.1/GP_ENC Cryptographic operation

FCS_COP.1.1/GP_ENC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

Cryptographic Operation	Algorithm	Key Sizes	Standard
secure messaging (GP) – encryption and decryption	Triple-DES in CBC mode	112 bit	[FIPS_46_3]
secure messaging (GP) – encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[NIST_800_38A]

.

FCS_COP.1/GP_AUTH Cryptographic operation

FCS_COP.1.1/GP_AUTH The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic Operation	Algorithm	Key Sizes	Standard
symmetric authentication – message authentication code	Full 3DES MAC	112 bit	[ISO_9797_1]
symmetric authentication – message authentication code	AES CMAC	128, 198 and 256 bits	[NIST_800_38B]

.

FCS_COP.1/GP_MAC Cryptographic operation

FCS_COP.1.1/GP_MAC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

Cryptographic Operation	Algorithm	Key Size(s)	Standard
secure messaging - message authentication code	Retail MAC	112 bit	[ISO_9797_1]
secure messaging (GP) - encryption and decryption	AES CMAC	128, 192 and 256 bits	[NIST_800_38B

.

FCS_COP.1/GP_KEY_DEC Cryptographic operation

FCS_COP.1.1/GP_KEY_DEC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic Operation	Algorithm	Key Sizes	Standard
key decryption	Triple-DES in ECB mode	112 bit	[FIPS_46_3]
key decryption	AES in CBC mode	128, 192 and 256 bits	[FIPS_197]

.

FCS_RND.1 Quality metric for random numbers

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**.

7.1.3 Class FIA Identification and Authentication

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **to establish the communication channel,**
- **to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS**
- **to carry out the Chip Authentication Protocol**

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.

FIA_UID.1/MP Timing of identification

FIA_UID.1.1/MP The TSF shall allow

- **to carry out the authentication of the Manufacturer and Personalization Agent**

on behalf of the user to be performed before the user is identified.

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

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

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

on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.1/MP Timing of authentication

FIA_UAU.1.1/MP The TSF shall allow

- **to carry out the authentication of the Manufacturer and Personalization Agent**

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/MP The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 Single-use authentication mechanisms

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

- **Terminal Authentication Protocol,**
- **Authentication Mechanism based on Triple-DES and AES**.

Application Note:

The authentication mechanisms based on Triple-DES and AES is the authentication process performed in phases 5 and 6

FIA_UAU.5/EAC Multiple authentication mechanisms

FIA_UAU.5.1/EAC The TSF shall provide

- **Terminal Authentication Protocol,**
- **Secure messaging in MAC-ENC mode,**
- **Symmetric Authentication Mechanism based on Triple-DES and AES**

to support user authentication.

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

- **The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with Personalization Agent Key.**
- **After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.**
- **The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism**.

FIA_UAU.6/EAC Re-authenticating

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

FIA_UAU.6/MP Re-authenticating

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**.

FIA_AFL.1/MP Authentication failure handling

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**.

FIA_API.1 Authentication Proof of Identity

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

7.1.4 Class FDP User Data Protection

FDP_ACC.1 Subset access control

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

FDP_ACF.1 Security attribute based access control

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

- **Subjects:**
  - **Personalization Agent,**
  - **Extended Inspection System**

- **Terminal,**
- **Objects:**
  - **data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,**
  - **data EF.DG3 and EF.DG4 of the logical MRTD**
  - **data in EF.COM,**
  - **data in EF.SOD,**
- **Security attributes:**
  - **authentication status of terminals,**
  - **Terminal Authorization**.

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

- **the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,**
- **the successfully authenticated Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD.**
- **the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD**.

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

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

- **A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,**
- **A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,**
- **A terminal authenticated as DV is not allowed to read data in the EF.DG3,**
- **A terminal authenticated as DV is not allowed to read data in the EF.DG4,**
- **A ny terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,**
- **Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD**.

FDP_ACC.1/UPD_FILE Subset access control

FDP_ACC.1.1/UPD_FILE The TSF shall enforce the **UPD_FILE Access Control SFP** on **terminals gaining write, read and modification access to data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

FDP_ACF.1/UPD_FILE Security attribute based access control

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

- **Subjects:**
  - **Personalization Agent,**
  - **Extended Inspection System,**
  - **Terminal,**
- **Objects:**
  - **data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**
- **Security attributes**
  - **authentication status of terminals,**.

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

- **the Personalization Agent is allowed to write, read and modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD,**
- **the successfully authenticated Extended Inspection System with the name corresponding to the one (or beginning of the one) set following FMT_MTD.1.1/UPD_FILE is allowed to modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

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

FDP_ACF.1.4/UPD_FILE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Any Terminal is not allowed to modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

FDP_UCT.1/EAC Basic data exchange confidentiality

FDP_UCT.1.1/EAC [Editorially Refined] The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure **after Chip Authentication**.

FDP_UIT.1/EAC Data exchange integrity

FDP_UIT.1.1/EAC [Editorially Refined] The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors **after Chip Authentication**.

FDP_UIT.1.2/EAC [Editorially Refined] The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred **after Chip Authentication**.

7.1.5 Class FMT Security Management

FMT_SMF.1 Specification of Management Functions

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

- **Initialization**
- **Pre-personalization**
- **Personalization**.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Manufacturer,**
- **Personalization Agent,**
- **Country Verifying Certification Authority,**
- **Document Verifier,**
- **domestic Extended Inspection System**
- **foreign Extended Inspection System**.

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

FMT_LIM.1 Limited capabilities

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

- **User Data to be manipulated,**
- **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,**
- **TSF data to be disclosed or manipulated**
- **software to be reconstructed and**
- **substantial information about construction of TSF to be gathered which may enable other attacks**

FMT_LIM.2 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**

- **User Data to be manipulated,**
- **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,**
- **TSF data to be disclosed or manipulated**
- **software to be reconstructed and**
- **substantial information about construction of TSF to be gath ered which may enable other attacks**

FMT_MTD.1/INI_ENA Management of TSF data

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to **write** the **Initialization Data and Prepersonalization Data** to **the Manufacturer**.

Application Note:

Please refer to F.ACW for details of the data written by the manufacturer.

FMT_MTD.1/INI_DIS Management of TSF data

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to **disable read access for users to** the **Initialization Data** to **the Personalization Agent**.

FMT_MTD.1/CVCA_INI Management of TSF data

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to **write** the

- **initial Country Verifying Certification Authority Public Key,**
- **initial Country Verifying Certification Authority Certificate,**
- **initial Current Date**

to **the Personalization Agent**.

FMT_MTD.1/CVCA_UPD Management of TSF data

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to **update** the

- **Country Verifying Certification Authority Public Key,**
- **Country Verifying Certification Authority Certificate**

to **Country Verifying Certification Authority**.

FMT_MTD.1/DATE Management of TSF data

FMT_MTD.1.1/DATE The TSF shall restrict the ability to **modify** the **current date** to

- **Country Verifying Certification Authority,**
- **Document Verifier,**
- **domestic Extended Inspection System**.

FMT_MTD.1/KEY_WRITE Management of TSF data

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to **write** the **Document Basic Access Keys** to **the Personalization Agent**.

FMT_MTD.1/CAPK Management of TSF data

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **load** the **Chip Authentication Private Key** to **the Personalization agent**.

FMT_MTD.1/KEY_READ Management of TSF data

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the

- **Document Basic Access Keys,**
- **Chip Authentication Private Key,**
- **Personalization Agent Keys**

to **none**.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 [Editorially Refined] The TSF shall ensure that only secure values of the certificate chain are accepted for **TSF data of the Terminal Authentication Protocol and the Access Control**.

Refinement:

The certificate chain is valid if and only if

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

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

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

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

FMT_MOF.1/GP Management of security functions behaviour

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

- **transmission of user data in a manner protected from unauthorised disclosure,**
- **reception of user data in a manner protected from unauthorised disclosure,**
- **transmission of user data in a manner protected from modification, deletion, insertion and replay errors,**
- **reception of user data in a manner protected from modification, deletion, insertion and replay errors,** to **the Manufacturer and the Personalization Agent**.

FMT_MTD.1/LCS_PERS Management of TSF data

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**.

FMT_MTD.1/UPD_FILE Management of TSF data

FMT_MTD.1.1/UPD_FILE The TSF shall restrict the ability to **set** the **identifiers of files that can be modified in phase 7(different from EF.COM, EF.SOD, EF.DG1 to EF.DG16)** to **the Personalization Agent**.

FMT_MTD.1/SM_LVL Management of TSF data

FMT_MTD.1.1/SM_LVL The TSF shall restrict the ability to **set** the **minimum Secure Messaging level required to access DG 3 and DG 4** to **the Personalization Agent**.

7.1.6 Class FPT Protection of the Security Functions

FPT_EMS.1 TOE Emanation

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 Key(s) and Chip Authentication Private Key** and

- **Pre-personalization Agent Keys,**
- **Secure Messaging Session Keys**.

FPT_EMS.1.2 The TSF shall ensure **users** are unable to use the following interface **smart card circuit contacts** to gain access to **Personalization Agent Key(s) and Chip Authentication Private Key** and

- **Pre-personalization Agent Keys,**
- **Secure Messaging Session Keys**.

FPT_FLS.1 Failure with preservation of secure state

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

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

FPT_TST.1 TSF testing

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

- **At reset,** to demonstrate the correct operation of **the TSF**.

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

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

FPT_PHP.3 Resistance to physical attack

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

7.1.7 Class FTP Trusted path/channels

FTP_ITC.1/MP Inter-TSF trusted channel

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 (Pre-Perso_K, Perso_K and CA_SK) shall be encrypted**.

7.2 Security Requirements Rationale

7.2.1 Objectives

7.2.1.1 Security Objectives for the TOE

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 FIA_UID.1, FIA_UID.1/MP, FIA_UAU.1, FIA_UAU.1/MP FDP_ACC.1/EAC and FDP_ACF.1/EAC in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control.

The following paragraph is extracted from [PP_EAC] 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/MP. If the Personalization Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA, FCS_CKM.1/CA_DATA_GEN for generation of CA Data in phase 6, FCS_COP.1/SHA (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6/EAC (for the re-authentication). If the Personalization Terminal wants to authenticate itself to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/GP_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

Note: As TA 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/EAC. The Personalization Agent can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_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. 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 SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMS.1 the confidentially of these keys.

SFR FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE define rules to manage files different from the ones managed by FDP_ACC.1/EAC and FDP_ACF.1/EAC.

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/LCS_PERS. Since then it is no more possible to return in Personalization state.

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 SFR FDP_ACC.1/EAC and FDP_ACF.1/EAC in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2/EAC, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4/EAC). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1, FIA_UID.1/MP, FIA_UAU.1 and FIA_UAU.1/MP before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5/EAC and FIA_UAU.6/EAC. The SFR FIA_UAU.6/EAC and FDP_UIT.1/EACA requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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 and FMT_MOF.1/GP requires 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. FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

SFR FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE define rules to manage files different from the ones managed by FDP_ACC.1/EAC and FDP_ACF.1/EAC.

OT.Sens_Data_Conf The security objective OT.Sens_Data_Conf "Confidentiality of sensitive biometric reference data" is enforced by the Access Control SFP defined in FDP_ACC.1/EAC and FDP_ACF.1/EAC allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a validly verifiable certificate according FCS_COP.1/SIG_VER.

The SFR FIA_UID.1 and FIA_UAU.1 requires the identification and authentication of the inspection systems. The SFR FIA_UAU.5/EAC requires the successful Chip Authentication (CA) before any authentication attempt as Extended Inspection System. During the protected communication following the CA the reuse of authentication data is prevented by FIA_UAU.4. The SFR FIA_UAU.6/EAC and FDP_UCT.1/EAC requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret), FCS_CKM.1/CA_DATA_GEN for generation of CA Data in phase 6, FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

The following part is added to integrate the Manufacturing and Personalization phases in the OT_Sens_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, and FMT_MOF.1/GP requires 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. FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

SFR FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE define rules to manage files different from the ones managed by FDP_ACC.1/EAC and FDP_ACF.1/EAC.

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.

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 "Identification and Authentication of the TOE".

OT.Chip_Auth_Proof The security objective OT.Chip_Auth_Proof "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol provided by FIA_API.1/CA proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Data is generated by using FCS_CKM.1/CA_DATA_GEN. The Chip Authentication Protocol [TR_03110] requires additional TSF according to FCS_COP.1/SHA (for the derivation of the session keys), FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging).

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.

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.

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

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.

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. FTP_ITC.1/MP allows the Manufacturer to communicate with the OS.

Once step 4 is done, the MRTD packaging responsible is allowed to set the Pre-personalization Agent keys according to the SFR FDP_ITC.1/MP and FCS_COP.1/GP_KEY_DEC. The read access to the Pre-personalization keys is prevented by SFRs FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

In step 5, the authentication of the terminal as Manufacturer shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5/EAC. 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 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 Personalization Agent can enable the modification of files in operational use phase according to FMT_MTD.1/UPD_FILE.

The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions setting the Pre-personalization Agent Keys. The read access to the secret key of the Personalization Agent Keys is prevented by the SFRs FCS_CKM.4, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3.

Since then it is no more possible to return in manufacturing state and the role Manufacturer is no longer available as FCS_CKM.4 destroys Manufacturer keys.

OT.Update_File The security objective OT.Update_File deals with the capability to update date in the operational phase after a succesful authentication. This objective is enforced by FMT_MTD.1/UPD_FILE thatensures only the terminal specified by the personalization agent can update the data in the operational phase.

FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE enforce the acccess conditions that are required to be fulfilled before data is updated.

OT.AC_SM_Level The security objective OT.AC_SM_LEVEL is enforced by FMT_MTD.1/SM_LVL that allows the personalization agent to set the SM level required to access to the sensitive data

7.2.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.AC_Pers	FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5/EAC, FIA_UAU.6/EAC, FIA_UAU.6/MP, FIA_AFL.1/MP, FDP_ACC.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1, FDP_ACF.1/UPD_FILE, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FMT_MTD.1/LCS_PERS, FPT_EMS.1, FCS_CKM.1/GP, FCS_COP.1/GP_AUTH, FCS_RND.1, FCS_CKM.1/CA_DATA_GEN, FIA_UID.1/MP, FIA_UAU.1/MP	Section 7.3.1
OT.Data_Int	FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5/EAC,	Section 7.3.1

	FIA_UAU.6/EAC, FIA_UAU.6/MP, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FDP_UIT.1/EAC, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1/GP, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FCS_CKM.1/GP, FCS_RND.1, FIA_UID.1/MP, FIA_UAU.1/MP	
OT.Sens_Data_Conf	FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5/EAC, FIA_UAU.6/EAC, FIA_UAU.6/MP, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FDP_UCT.1/EAC, FMT_MOF.1/GP, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.3, FCS_CKM.1/GP, FCS_RND.1, FCS_CKM.1/CA_DATA_GEN	Section 7.3.1
OT.Identification	FAU_SAS.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS	Section 7.3.1
OT.Chip_Auth_Proof	FCS_CKM.1/CA, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FIA_API.1, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FCS_CKM.1/CA_DATA_GEN	Section 7.3.1
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2	Section 7.3.1
OT.Prot_Inf_Leak	FPT_EMS.1, FPT_FLS.1, FPT_TST.1, FPT_PHP.3	Section 7.3.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 7.3.1
OT.Prot_Malfunction	FPT_TST.1, FPT_FLS.1	Section 7.3.1
OT.Configuration	FCS_CKM.1/GP, FCS_COP.1/GP_ENC, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_MAC, FCS_COP.1/GP_KEY_DEC, FIA_UAU.6/MP, FIA_AFL.1/MP, FCS_CKM.4, FIA_UAU.4, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/UPD_FILE, FPT_EMS.1, FPT_FLS.1, FPT_PHP.3, FCS_RND.1, FIA_UAU.5/EAC, FTP_ITC.1/MP	Section 7.3.1
OT.Update_File	FMT_MTD.1/UPD_FILE, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE	Section 7.3.1
OT.AC_SM_Level	FMT_MTD.1/SM_LVL	Section 7.3.1

Table 16 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FAU_SAS.1	OT.Identification
FCS_CKM.1/CA	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_CKM.1/CA_DATA_GEN	OT.AC_Pers, OT.Sens_Data_Conf,

	OT.Chip_Auth_Proof
FCS_CKM.1/GP	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration
FCS_CKM.4	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration
FCS_COP.1/SHA	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/SYM	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/MAC	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/SIG_VER	OT.AC_Pers, OT.Sens_Data_Conf
FCS_COP.1/GP_ENC	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration
FCS_COP.1/GP_AUTH	OT.AC_Pers, OT.Configuration
FCS_COP.1/GP_MAC	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration
FCS_COP.1/GP_KEY_DEC	OT.Configuration
FCS_RND.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration
FIA_UID.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FIA_UID.1/MP	OT.AC_Pers, OT.Data_Int
FIA_UAU.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FIA_UAU.1/MP	OT.AC_Pers, OT.Data_Int
FIA_UAU.4	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration
FIA_UAU.5/EAC	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration
FIA_UAU.6/EAC	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FIA_UAU.6/MP	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration
FIA_AFL.1/MP	OT.AC_Pers, OT.Configuration
FIA_API.1	OT.Chip_Auth_Proof
FDP_ACC.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FDP_ACF.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FDP_ACC.1/UPD_FILE	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Update_File
FDP_ACF.1/UPD_FILE	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Update_File
FDP_UCT.1/EAC	OT.Sens_Data_Conf

FDP_UIT.1/EAC	OT.Data_Int
FMT_SMF.1	OT.AC_Pers, OT.Data_Int, OT.Configuration
FMT_SMR.1	OT.AC_Pers, OT.Data_Int, OT.Configuration
FMT_LIM.1	OT.Prot_Abuse-Func
FMT_LIM.2	OT.Prot_Abuse-Func
FMT_MTD.1/INI_ENA	OT.Identification
FMT_MTD.1/INI_DIS	OT.Identification
FMT_MTD.1/CVCA_INI	OT.Sens_Data_Conf
FMT_MTD.1/CVCA_UPD	OT.Sens_Data_Conf
FMT_MTD.1/DATE	OT.Sens_Data_Conf
FMT_MTD.1/KEY_WRITE	OT.AC_Pers
FMT_MTD.1/CAPK	OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FMT_MTD.1/KEY_READ	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FMT_MTD.3	OT.Sens_Data_Conf
FMT_MOF.1/GP	OT.Data_Int, OT.Sens_Data_Conf
FMT_MTD.1/LCS_PERS	OT.AC_Pers
FMT_MTD.1/UPD_FILE	OT.Configuration, OT.Update_File
FMT_MTD.1/SM_LVL	OT.AC_SM_Level
FPT_EMS.1	OT.AC_Pers, OT.Prot_Inf_Leak, OT.Configuration
FPT_FLS.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction, OT.Configuration
FPT_TST.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction
FPT_PHP.3	OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper, OT.Configuration
FTP_ITC.1/MP	OT.Configuration

Table 17 SFRs and Security Objectives

7.2.3 Dependencies

7.2.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FAU_SAS.1	No Dependencies	
FCS_CKM.1/CA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/SYM, FCS_COP.1/MAC
FCS_CKM.1/CA_DATA_GEN	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/SIG_VER
FCS_CKM.1/GP	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/CA, FCS_CKM.1/GP
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4
FCS_COP.1/SYM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/SIG_VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/GP_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/GP, FCS_CKM.4
FCS_COP.1/GP_AUTH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/GP, FCS_CKM.4
FCS_COP.1/GP_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/GP, FCS_CKM.4
FCS_COP.1/GP_KEY_DEC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/GP, FCS_CKM.4
FCS_RND.1	No Dependencies	
FIA_UID.1	No Dependencies	
FIA_UID.1/MP	No Dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_UAU.1/MP	(FIA_UID.1)	FIA_UID.1/MP
FIA_UAU.4	No Dependencies	
FIA_UAU.5/EAC	No Dependencies	
FIA_UAU.6/EAC	No Dependencies	
FIA_UAU.6/MP	No Dependencies	
FIA_AFL.1/MP	(FIA_UAU.1)	FIA_UAU.1/MP
FIA_API.1	No Dependencies	
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1
FDP_ACF.1	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1
FDP_ACC.1/UPD_FILE	(FDP_ACF.1)	FDP_ACF.1/UPD_FILE
FDP_ACF.1/UPD_FILE	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/UPD_FILE
FDP_UCT.1/EAC	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1
FDP_UIT.1/EAC	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1
FMT_SMF.1	No Dependencies	

FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_LIM.1	No Dependencies	
FMT_LIM.2	No Dependencies	
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/CVCA_INI	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/CVCA_UPD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/DATE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/CAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD
FMT_MOF.1/GP	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/LCS_PERS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/UPD_FILE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/SM_LVL	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_TST.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FTP_ITC.1/MP	No Dependencies	

Table 18 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/SHA is discarded. The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

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

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

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/EAC is discarded. The SFR FDP_UCT.1/EAC requires the use secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel.

Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/EAC is discarded. The SFR FDP_UIT.1/EAC requires the use secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

7.2.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (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	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

Table 19 SARs Dependencies

7.2.4 Rationale for the Security Assurance Requirements

The EAL5 was chosen to permit a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

7.2.4.1 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 EAL5 has no dependencies to other security requirements.

7.2.4.2 AVA_VAN.5 Advanced methodical vulnerability analysis

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

The component AVA_VAN.5 has the following dependencies:

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

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

8. TOE Summary Specification

8.1 TOE Summary Specification

F.ACR - 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,
- Personalization Agent keys,
- CA private key
- Document basic access keys

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 EAC 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 anytime

F.ACW - 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 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), except for CVCA which can be updated if the "Secure Messaging" access condition is verified by the subjects defined in FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

In the Production and preparation stage:

The Manufacturer can write all the Initialization data and data for the Pre-personalization. The Personalization Agent can write through a valid secure channel all the data and Document Basic Access Keys, Chip Authentication Private Key and Country Verifying Certification Authority Public Key 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-personalizaiton agent. the Pre-personalization agent (which is seen as a sub-role of thep Personalization agent) will refresh this key.

F.CLR_INFO - Clear Residual Information

This security function ensures clearing of sensitive information

- Authentication state is securely cleared in case an error is detected or a new authentication is attempted
- Authentication data related to GP authentication and EAC is securely cleared to prevent reuse
- Session keys is securely erased in case an error is detected or the secure communication session is closed

F.CRYPTO - Cryptographic Support

This Security Function provides the following cryptographic features:

- Key Generation based on ECDH with key sizes 192 to 512 bits.
- Key generation for Triple-DES in CBC mode for 112 bits.
- Key generation for AES in CBC mode with key sizes 128, 192 and 256 bits.
- Hashing using SHA-1 and SHA-256 meeting [FIPS_180_4]
- Secure messaging (encryption and decryption)using:
  - Triple-DES in CBC mode (keys size 112 bits)
  - AES in CBC mode (key sizes 128, 192 and 256 bits)
- Secure messaging (message authentication code) using:
  - Retail MAC with key size 112 bits
  - AES CMAC with key sizes 128, 192 and 256 bits
- Digital signature verification using:
  - ECDSA with SHA-1, SHA-224 and SHA-256 with key sizes 192 to 512 bits.
  - RSA PKCS#1v1.5 with SHA-1, SHA-256 and SHA-512 with key sizes 1024, 1536, 2048
  - RSA PKCS#1-PSS with SHA-1, SHA-256 and SHA-512 with key sizes 1024, 1536, 2048
- GP Secure Messaging (encryption and decryption) using:
  - Triple-DES in CBC mode with key size 112 bits as defined in [FIPS_46_3].
  - AES with key sizes 128, 192 and 256 bits as defined in [NIST_800_38A].
- GP Secure Messaging (message authentication code) using:
  - Retail MAC with key size 112 bits as defined in [ISO_9797_1].
  - AES CMAC with key sizes 128, 192 and 256 bits as defined in [NIST_800_38B].
- Symmetric Authentication - encryption and decryption using:
  - Full 3DES MAC with key size 112 bits as defined in [ISO_9797_1].
  - AES CMAC with key sizes 128, 192 and 256 bits as defined in [NIST_800_38B].
- Key decryption using:
  - Triple-DES in ECB mode with key size 112 bits as defined in [FIPS_46_3].
  - AES in CBC mode with key sizes 128, 192 and 256 bits as defined in [FIPS_197].
- Chip Authentication Data Generation using DH, with key sizes 1024 to 2048 bits in steps of 512 bits.
- Chip Authentication Data Generation using ECDH, with key sizes 192 to 512 bits.
- Random number generation that meets the requirement the average Shannon entropy per internal random bit exceeds 0.999.

F.EAC - Extended Access Control, EAC

This TSF provides the Extended Access Control, authentication and session keys generation to be used by F.SM, as described in [TR_03110]. It also provides the following management functions:

- Maintain the roles: Document Verifier, CVCA, Domestic EIS, Foreign EIS
- Limit the ability to update the CVCA Public key and CVCA Certificate to the Country Verifying Certification Authority
- Limit the ability to update the date to CVCA, Document Verifier and Domestic Extended Inspection System.

F.PERS - 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 security function is also responsible for management operations during personalization phase. This function allows to:

- Manage symmetric authentication using Personalization Agent keys,
- Configuration of the TOE
- Compute session keys to be used by F.SM,
- Load user data,
- Configure SM level for biometrical data access,
- Load Chip Authentication keys in encrypted form,
- Chip Authnetication Key Generation,
- Disable read access to Initialization Data,
- Write initial CVCA Public Key, initial CVCA Certificate and initial current date
- Write the document basic access keys,
- Set the files that are allowed to be modified in phase 7,
- Write the Document Security Object (SO d),
- Set TOE life cycle to Operational Use phase

In case the number of consecutive failed authentication attempts crosses 1 the TSF will slow down further authentication attempts.

F.PHY - 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, configuration data and TOE life cycle. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE.

This Security Function also limits any physical emanations from the TOE so as to prevent any information leakge via these emanations that might reveal or provide access to sensitive data.

Furthermore, it prevents deploying test features after TOE delivery.

F.PREP - 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 and AES symmetric authentication mechanism. This function allows to:

- Manage symmetric authentication using Pre-personalization Agent keys,
- Compute session keys to be used by F.SM,
- Initialization of the TOE,
- Load Personalization Agent keys in encrypted form,
- Store the Initialization and Pre-Personalization data in audit records.

In case the number of consecutive failed authentication attempts crosses 1 the TSF will slow down further authentication attempts.

F.SM - 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. CA), a secure channel is established. This security functionality also provides a Secure Messaging (SCP02 and SCP03) for the transmission of user data in 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 or if the session is closed, the session keys are destroyed. This ensures protection against replay attacks as session keys are never reused.

F.SS - Safe State Management

This security functionality ensures that the TOE gets back to a secure state when:

- a tearing occurs (during a copy of data in NVM).
- an error due to self test as defined in FPT_TST.1.
- any physical tampering is detected.

This security functionality ensures that if such a case occurs, the TOE either is switched in the state "kill card" or becomes mute.

F.STST - Self Test

This security function implements self test features through platform functionalities at reset as defined in FPT_TST.1 to ensure the integrity of the TSF and TSF data.

8.2 SFRs and TSS

8.2.1 SFRs and TSS - Rationale

Class FAU Security Audit

FAU_SAS.1 is met by F.PREP - MRTD Pre-personalization

Class FCS Cryptographic Support

FCS_CKM.1/CA is met by F.EAC - Extended Access Control, EAC that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support

FCS_CKM.1/CA_DATA_GEN is met by F.PERS - MRTD Personalization that uses F.CRYPTO - Cryptographic Support to generate Chip Authentication Data.

FCS_CKM.1/GP is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that generate Cryptographic keys as defined in the requirement using F.CRYPTO - Cryptographic Support.

FCS_CKM.4 is met by F.CLR_INFO - Clear Residual Information and F.SM - Secure Messaging that destroys the session keys upon closure of a secure messaging session.

FCS_COP.1/SHA is met by F.CRYPTO - Cryptographic Support.

FCS_COP.1/SYM is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

FCS_COP.1/MAC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

FCS_COP.1/SIG_VER is met by F.EAC - Extended Access Control, EAC that uses F.CRYPTO - Cryptographic Support for Terminal Authentication.

FCS_COP.1/GP_ENC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

FCS_COP.1/GP_AUTH is met by F.PREP - MRTD Pre-personalization and F.PERS - MRTD Personalization that use F.CRYPTO - Cryptographic Supportto perform Symmetric Authentication.

FCS_COP.1/GP_MAC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

FCS_COP.1/GP_KEY_DEC is met by F.PREP - MRTD Pre-personalization and F.PERS - MRTD Personalization that use F.CRYPTO - Cryptographic Support to perform key decryption.

FCS_RND.1 is met by F.CRYPTO - Cryptographic Support

Class FIA Identification and Authentication

FIA_UID.1 is met by F.ACR - Access Control in Reading that manages read access to data based on the current authentication state.

It is also met by F.EAC - Extended Access Control, EAC that allows Chip Authentication.

FIA_UID.1/MP is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that provide semmetric authentication for manufacturer and personalization agent authentication.

FIA_UAU.1 is met by F.ACR - Access Control in Reading that manages read access to data based on the current authentication state.

It is also met by F.EAC - Extended Access Control, EAC that allows Chip Authentication.

FIA_UAU.1/MP is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that provide semmetric authentication for manufacturer and personalization agent authentication.

FIA_UAU.4 is met by F.CLR_INFO Clear Residual Information that ensures all authentication data is securely erased to prevent reuse.

FIA_UAU.5/EAC is met by F.EAC - Extended Access Control, EAC that provides Terminal Authentication.

SFR is also met by F.PERS - MRTD Personalization that provides symmetric authentication.

The SFR is also met by F.PREP - MRTD Pre-personalization that provides manufacturer authentication

Finally, it is also met by F.SM - Secure Messaging that provides a secure messaging session.

FIA_UAU.6/EAC is met by F.SM - Secure Messaging that ensures all messages are sent through the secure communication channel after Chip Authentication.

FIA_UAU.6/MP is met by F.SM - Secure Messaging that ensures all messages are sent through the secure communication channel after Chip Authentication.

FIA_AFL.1/MP is met by F.PREP - MRTD Pre-personalization and F.PERS - MRTD Personalization that ensure that after 3 authentication attempts the Toe increases time taken to respond to a terminal challenge.

FIA_API.1 is met by F.EAC - Extended Access Control, EAC that provides Chip Authentication as defined by [TR_03110]

Class FDP User Data Protection

FDP_ACC.1 is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.EAC - Extended Access Control, EAC and F.PERS - MRTD Personalization

FDP_ACF.1 is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.EAC - Extended Access Control, EAC and F.PERS - MRTD Personalization

FDP_ACC.1/UPD_FILE is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.EAC - Extended Access Control, EAC and F.PERS - MRTD Personalization

FDP_ACF.1/UPD_FILE is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.EAC - Extended Access Control, EAC and F.PERS - MRTD Personalization

FDP_UCT.1/EAC is met by F.SM - Secure Messaging that ensures all data is sent throught the secure communication channel after a successful Chip Authentication.

FDP_UIT.1/EAC is met by F.SM - Secure Messaging that ensures all messages are sent through the secure communication channel after Chip Authentication.

Class FMT Security Management

FMT_SMF.1 is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that utilizeF.ACW - Access Control in Writing to control write access via secure messaging provided by F.SM - Secure Messaging

FMT_SMR.1 is met by F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization. These roles are maintained by

means of the authentication states during the authentication mechanisms provided by the 3 Security Functions

FMT_LIM.1 is met by F.PHY - Physical Protection and F.SS - Safe State Management that ensure that no data can be manipulated or revealed and the TSF assumes a safe state in case any illegal attempts to do so are detected.

FMT_LIM.2 is met by F.PHY - Physical Protection and F.SS - Safe State Management that ensure that no data can be manipulated or revealed and the TSF assumes a safe state in case any illegal attempts to do so are detected.

FMT_MTD.1/INI_ENA is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalization

FMT_MTD.1/INI_DIS is met by F.PERS - MRTD Personalization that allows the personalization agent to disable read access in F.ACR - Access Control in Reading

FMT_MTD.1/CVCA_INI is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalization

FMT_MTD.1/CVCA_UPD is met by F.ACW - Access Control in Writing that controls access to updation of CVCA data by authentication through F.EAC - Extended Access Control, EAC

FMT_MTD.1/DATE is met by F.ACW - Access Control in Writing that controls access to updation of CVCA data by authentication through F.EAC - Extended Access Control, EAC

FMT_MTD.1/KEY_WRITE is met by F.PREP - MRTD Pre-personalization

FMT_MTD.1/CAPK is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalization

FMT_MTD.1/KEY_READ is met by F.ACR - Access Control in Reading that ensures the secret keys are never readable.

FMT_MTD.3 is met by F.EAC - Extended Access Control, EAC

FMT_MOF.1/GP is met by F.SM - Secure Messaging that provides a secure meants of transfer of user data after authentication using F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization

FMT_MTD.1/LCS_PERS is met by F.PERS - MRTD Personalization that allows the personalization agent after succesful authentication to switch the lifecycle state from phase 6 to phase 7

FMT_MTD.1/UPD_FILE is met by F.PERS - MRTD Personalization that controls access conditions in F.ACW - Access Control in Writing to allow only the name set by the personalization agent to be able to edit files in Operation Phase

FMT_MTD.1/SM_LVL is met by F.PERS - MRTD Personalization that allows the personalization agent to configure access conditions to DG.3 and DG.4 in F.ACW - Access Control in Writing

Class FPT Protection of the Security Functions

FPT_EMS.1 is met by F.PHY - Physical Protection that prevents emanations beyond permissible limits to prevent any accidental revelation of data.

FPT_FLS.1 is met by F.SS - Safe State Management.

FPT_TST.1 is met by F.STST - Self Test that performs self tests to ensure integrity of the TSF

FPT_PHP.3 is met by F.PHY - Physical Protection that protects the TOE against any physical probing or tampering by using F.SS - Safe State Management in case any physical manipulation is detected.

Class FTP Trusted path/channels

FTP_ITC.1/MP is met by F.SM - Secure Messaging that provides a ssecure channel for communication after authentication as defined in F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization

8.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FAU_SAS.1	F.PREP - MRTD Pre-personalization
FCS_CKM.1/CA	F.EAC - Extended Access Control, EAC, F.CRYPTO - Cryptographic Support
FCS_CKM.1/CA_DATA_GEN	F.CRYPTO - Cryptographic Support, F.PERS - MRTD Personalization
FCS_CKM.1/GP	F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization, F.CRYPTO - Cryptographic Support
FCS_CKM.4	F.SM - Secure Messaging, F.CLR_INFO - Clear Residual Information
FCS_COP.1/SHA	F.CRYPTO - Cryptographic Support
FCS_COP.1/SYM	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_COP.1/MAC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_COP.1/SIG_VER	F.EAC - Extended Access Control, EAC, F.CRYPTO - Cryptographic Support
FCS_COP.1/GP_ENC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support

FCS_COP.1/GP_AUTH	F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization, F.CRYPTO - Cryptographic Support
FCS_COP.1/GP_MAC	F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support
FCS_COP.1/GP_KEY_DEC	F.CRYPTO - Cryptographic Support, F.PREP - MRTD Pre-personalization, F.PERS - MRTD Personalization
FCS_RND.1	F.CRYPTO - Cryptographic Support
FIA_UID.1	F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC
FIA_UID.1/MP	F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization
FIA_UAU.1	F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC
FIA_UAU.1/MP	F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization
FIA_UAU.4	F.CLR_INFO - Clear Residual Information
FIA_UAU.5/EAC	F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization, F.SM - Secure Messaging, F.PREP - MRTD Pre-personalization
FIA_UAU.6/EAC	F.SM - Secure Messaging
FIA_UAU.6/MP	F.SM - Secure Messaging
FIA_AFL.1/MP	F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization
FIA_API.1	F.EAC - Extended Access Control, EAC
FDP_ACC.1	F.ACW - Access Control in Writing, F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization
FDP_ACF.1	F.ACW - Access Control in Writing, F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization
FDP_ACC.1/UPD_FILE	F.ACW - Access Control in Writing, F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization
FDP_ACF.1/UPD_FILE	F.ACW - Access Control in Writing, F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization
FDP_UCT.1/EAC	F.SM - Secure Messaging
FDP_UIT.1/EAC	F.SM - Secure Messaging
FMT_SMF.1	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization, F.SM - Secure Messaging
FMT_SMR.1	F.EAC - Extended Access Control, EAC, F.PERS - MRTD

	Personalization, F.PREP - MRTD Pre-personalization
FMT_LIM.1	F.PHY - Physical Protection, F.SS - Safe State Management, F.STST - Self Test
FMT_LIM.2	F.PHY - Physical Protection, F.SS - Safe State Management
FMT_MTD.1/INI_ENA	F.ACW - Access Control in Writing, F.PREP - MRTD Pre-personalization
FMT_MTD.1/INI_DIS	F.ACR - Access Control in Reading, F.PERS - MRTD Personalization
FMT_MTD.1/CVCA_INI	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FMT_MTD.1/CVCA_UPD	F.ACW - Access Control in Writing, F.EAC - Extended Access Control, EAC
FMT_MTD.1/DATE	F.ACW - Access Control in Writing, F.EAC - Extended Access Control, EAC
FMT_MTD.1/KEY_WRITE	F.PERS - MRTD Personalization
FMT_MTD.1/CAPK	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FMT_MTD.1/KEY_READ	F.ACR - Access Control in Reading
FMT_MTD.3	F.EAC - Extended Access Control, EAC
FMT_MOF.1/GP	F.SM - Secure Messaging, F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization
FMT_MTD.1/LCS_PERS	F.PERS - MRTD Personalization
FMT_MTD.1/UPD_FILE	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FMT_MTD.1/SM_LVL	F.ACW - Access Control in Writing, F.PERS - MRTD Personalization
FPT_EMS.1	F.PHY - Physical Protection
FPT_FLS.1	F.SS - Safe State Management
FPT_TST.1	F.STST - Self Test
FPT_PHP.3	F.PHY - Physical Protection, F.SS - Safe State Management
FTP_ITC.1/MP	F.SM - Secure Messaging, F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization

Table 20 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
F.ACR - Access Control in Reading	FIA_UID.1, FIA_UAU.1, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_READ
F.ACW - Access	FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_SMF.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/CVCA_INI,

Control in Writing	FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/UPD_FILE, FMT_MTD.1/SM_LVL
F.CLR_INFO - Clear Residual Information	FCS_CKM.4, FIA_UAU.4
F.CRYPTO - Cryptographic Support	FCS_CKM.1/CA, FCS_CKM.1/CA_DATA_GEN, FCS_CKM.1/GP, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER, FCS_COP.1/GP_ENC, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_MAC, FCS_COP.1/GP_KEY_DEC, FCS_RND.1
F.EAC - Extended Access Control, EAC	FCS_CKM.1/CA, FCS_COP.1/SIG_VER, FIA_UID.1, FIA_UAU.1, FIA_UAU.5/EAC, FIA_API.1, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_SMR.1, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.3
F.PERS - MRTD Personalization	FCS_CKM.1/CA_DATA_GEN, FCS_CKM.1/GP, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_KEY_DEC, FIA_UID.1/MP, FIA_UAU.1/MP, FIA_UAU.5/EAC, FIA_AFL.1/MP, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_DIS, FMT_MTD.1/CVCA_INI, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/CAPK, FMT_MOF.1/GP, FMT_MTD.1/LCS_PERS, FMT_MTD.1/UPD_FILE, FMT_MTD.1/SM_LVL, FTP_ITC.1/MP
F.PHY - Physical Protection	FMT_LIM.1, FMT_LIM.2, FPT_EMS.1, FPT_PHP.3
F.PREP - MRTD Pre-personalization	FAU_SAS.1, FCS_CKM.1/GP, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_KEY_DEC, FIA_UID.1/MP, FIA_UAU.1/MP, FIA_UAU.5/EAC, FIA_AFL.1/MP, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_ENA, FMT_MOF.1/GP, FTP_ITC.1/MP
F.SM - Secure Messaging	FCS_CKM.4, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FIA_UAU.5/EAC, FIA_UAU.6/EAC, FIA_UAU.6/MP, FDP_UCT.1/EAC, FDP_UIT.1/EAC, FMT_SMF.1, FMT_MOF.1/GP, FTP_ITC.1/MP
F.SS - Safe State Management	FMT_LIM.1, FMT_LIM.2, FPT_FLS.1, FPT_PHP.3
F.STST - Self Test	FMT_LIM.1, FPT_TST.1

Table 21 TSS and SFRs - Coverage

9. GLOSSARY AND ACRONYMS

9.1 Glossary

Term	Definition
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 [ICAO_9303] 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]
Initialization	Process of writing Initialization Data (see below) to the TOE (cf. 1.3.7.2.3 Phase 3: Manufacturing and Testing).
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

Term	Definition
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).
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 [ICAO_9303].
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. 1.3.7.5 Phase 6: TOE Personalization, phase 6).

Term	Definition
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.
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-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf 1.3.7.3.1 Phase 4 and 5: Loading and Pre-personalization , 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 an 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 Personalization Agent from the Manufacturer.

Term	Definition
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 role whose identity is being claimed, to determine whether it matches the role'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.

9.2 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
LCS	Life Cycle State
MF	Master File
OSP	Organizational Security Policy
PT	Personalization Terminal
SAR	Security Assurance Requirements
SFR	Security Functional Requirement
TOE	Target Of Evaluation
TSF	TOE Security Functions

10. REFERENCES

[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.

[PP_IC] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, 2014.

[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

[PP_EACwPACE] Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Application Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5th December 2012

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

[PTF_CERT] NSCIB CC-18-200833

[IC_CERT] Certification Report - BSI-DSZ-CC-0945-V2-2018

[PTF_AGD1] ID-One Cosmo V9 Application Loading Protection Guidance, FQR: 110 8798, Issue 2, IDEMIA

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

[PTF_AGD3] Secure acceptance and delivery of sensitive element - FQR 110 8921 Ed1, 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 AGD PRE, IDEMIA

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, 7th Edition, 2015 – Security Mechanisms for MRTDs

[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_11770] ISO/IEC 11770-3:2015 Information technology -- Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques

[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

[TR_03110] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012. BSI

[TR_03111] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, 17.04.2009

[FIPS_180_4] FIPS 180-4, Federal Information Processing Standards Publication (FIPS PUB) 180-4, Secure Hash Standard, August 2015

[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 2.2.1 – Public Release, January 2011