IDEMIA

IDmove v4 on Infineon in EAC configuration with AA in option Public Security Target

DOCUMENT REVISION

Date	Revision	Modification
2019/03/21	0.1	Creation
2019/03/25	0.2	Add code of the document in Table 1
2019/03/26	1	Approve Issue 1 of the document
2019/05/24	1.1	§2.1.2: Update OS Commercial Version to 090804 and OS Unique Identifier to 3C1D. §11: Update [IC_ST] reference
2019/06/20	1.2	§10: Update [IC_ST], [IC_CERT] & [IC_PPM] references §10: Add [ISO_9796_2] & [TR_03111] §7.1.2.3: Update FCS_COP.1.1/SIG_GEN referenced standards
2019/07/18	2	Approve Issue 2 of the document
2020/06/26	3	Update for maintenance: §2.1.2: Update OS Commercial Version to 090805, OS Unique Identifier to 3B7D and Preparative Documentation Issue 3. [IC_ST], [IC_CERT] & [IC_PPM] references.
2020/06/30	4	Update for [IC_ST] libraries references.
2020/06/22	5	§ 2.1.1: ST version/date § 2.1.2: Product Name to IDmove v4 on Infineon M02; Update OS Commercial Version to 090806 and OS Unique Identifier to DC71.
19/12/22	6	Updates: chip certificate reference, ANSSI-PG-083

TABLE OF CONTENT

1 GENERAL

1.1 Introduction

This security target describes the security needs induced by the IDmove v4 on Infineon in EAC configuration with AA in option.

The objectives of this Security Target are:

- describe the Target of Evaluation (TOE), its life cycle and to position it in the smart card life cycle,
- 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,
- describe the security objectives of the TOE and its supported environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the product active phases,
- specify the security requirements including the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment,
- describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements,
- 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

IDmove v4 on Infineon is a multi-configuration MRTD product. It provides four configurations, which are:

- IDmove v4 on Infineon in BAC configuration with AA and/or CA in option,
- **IDmove v4 on Infineon in EAC configuration with AA in option,**
- IDmove v4 on Infineon in EAC with PACE configuration with AA in option,
- IDmove v4 on Infineon in PACE configuration with AA and/or CA in option.

IDmove v4 on Infineon Operating System is embedded in the component identified in [IC_ST] manufactured by Infineon.

Mutatis mutandis, the product may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446 supporting EAC and AA, 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.

2 ST INTRODUCTION

2.1 ST reference and TOE reference

2.1.1 ST reference

Title	IDmove v4 on Infineon in EAC configuration with AA in option – Public Security Target
Code	FQR 110 9126
Version	6
Authors	IDEMIA
Publication date	2022/12/19
CC version	3.1 revision 5
EAL	EAL5 augmented with: • ALC_DVS.2 • AVA_VAN.5
PP	See [PP_EAC]

Table 1 - ST reference

2.1.2 TOE reference

Developer name	IDEMIA
Product name	IDMove v4 on Infineon M02
TOE name	IDmove v4 on Infineon in EAC configuration with AA in option
TOE identification	
Integrated Circuit	See Table 3 - IC identification
Embedded Software	Operating System Commercial Version: **090806** Operation System Unique Identifier: **DC71**
User Guidance documentation	Preparative Documentation: **FQR 110 8997 Issue 6** Operational Documentation: **FQR 110 8998 Issue 1**

Table 2 - TOE reference

2.1.3 IC identification

IC certificates	See [IC_CERT]
IC public Security Target	See [IC_ST]

Table 3 - IC identification

2.1.4 TOE Delivered Parts

Part of the TOE	***Format***	***Delivery Method***	***Comment***
Integrated Circuit	See [IC_ST]		
Embedded Software	Specific file containing APDUs allowing the embedded software loading.	Encrypted file in email	The file contains all commands to be used to load the embedded software. These commands are already formatted to ensure the integrity and the confidentiality of the embedded software.
Additional Code	Specific file containing APDUs allowing the additional code loading.	Encrypted file in email	The file contains all commands to be used to load the additional code. These commands are already formatted to ensure the integrity and the confidentiality of the additional code.
Final TOE	ID1 cards, wafers, modules, inlays, ecovers, eDatapage or passeports	Secure transport	Customer can ask for rising of the security of the delivery method.
User Guidance Documentation	Personalized pdf	Encrypted file in email	-

Table 4- TOE delivery parts

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, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO_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 MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This protection profile addresses the Chip Authentication described in [TR_03110] as an alternative to the Active Authentication stated in [ICAO_9303].

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 PP 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. The evaluation and certification process might have taken place in advance or could – more likely – be carried out simultaneously to the current process according the PP in hand.

Application Note1: It is assumed that 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 the EAC-PP. Nevertheless claiming conformance of this (EAC-) PP requires that the TOE meets a (separate) ST conforming to the BAC-PP [PP_BAC]. Moreover, if possible with respect to the applied national scheme there might be one ST and with it one evaluation process merging the claims for [PP_BAC] and this PP at hand.

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

As defined in [ICAO_9303] in §6.1, Active Authentication authenticates the contactless IC by signing a challenge sent by the IFD (inspection system) with a private key known only to the IC. For this purpose the contactless IC contains its own Active Authentication Key pair (KPrAA and KPuAA). A hash representation of Data Group 15 (Public Key (KPuAA) info) is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key (KPrAA) is stored in the contactless IC's secure memory. By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SOD)) in combination with the challenge response, using the eMRTD's Active Authentication Key Pair (KPrAA and KPuAA), the inspection system verifies that the Document Security Object (SOD) has been read from the genuine contactless IC, stored in the genuine eMRTD.

The security target requires the TOE to implement the Chip Authentication defined in [TR_03110]. The Chip Authentication prevents data traces described in [ICAO_9303], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The security target requires the TOE to implement the Extended Access Control as defined in [TR_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.

Mutatis mutandis, the TOE may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446 supporting EAC and AA, 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
DG3	DG7
DG4	DG8
DG15	DG13
MRZ	MRZ or SAI (Scanning area identifier)
Traveler	Holder

2.2.2 TOE type

The TOE is the contactless and/or contact integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control, Active Authentication and Extended Access Control according to the 'ICAO Doc 9303' [ICAO_9303] and BSI TR-03110 [TR_03110].

The TOE comprises at least:

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

Note: The antenna and the form factor are not part of the TOE as they do not have any impact on the security.

2.2.3 TOE life cycle

2.2.3.1 Life cycle overview

The following table presents the TOE subjects and the corresponding responsible:

Subject		Responsible
IC developer		Infineon
TOE developer		IDEMIA
Manufacturer	IC manufacturer	Infineon
	MRTD packaging responsible	IDEMIA or another agent
	Embedded software loading responsible	Infineon (only applying for Scheme 1), or IDEMIA (only applying for Scheme 2) or another agent (only applying for Scheme 3)
	Pre-personalization Agent	IDEMIA or another agent
Personalization Agent		IDEMIA or another agent

Table 5 - Subjects identification on the life cycle

Several life cycles are available, depending when the Flash Code is loaded and who loads the Flash Code. 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:

Scheme 1, MRTD chip Embedded Software loaded by the IC Manufacturer in step 3:

Phase	***Step***	***Subject***	***Emb. Sw. loading***	***Covered by***	***Sites***
1 - Development	1	IC developer	×	IC certification	IC certification
	2	TOE developer	×	ALC R&D sites	Pessac and Courbevoie
2 - Manufacturing	3	IC manufacturer	×	IC certification	IC manufacturer site
		Embedded software loading responsible	✓		
	TOE delivery point				
	4	MRTD packaging responsible	×		Packaging centre
	5	Pre-personalization agent	×	AGD_PRE	
3 - Personalization	6	Personalization agent	×	AGD_PRE	
4 - Operational Use	7	End user	×	AGD_OPE	

Table 6 - Subjects identification following life cycle steps – Scheme 1

Scheme 2, MRTD chip Embedded Software loaded by the Flash Loader with the optional Package 1 (See [IC_ST]) in step 4 before TOE delivery point:

Phase	*Step*	*Subject*	*Emb. Sw. loading*	*Covered by*	*Sites*
1 - Development	1	IC developer	×	IC certification	IC developer site
	2	TOE developer	×	ALC R&D sites	Pessac and Courbevoie
2 - Manufacturing	3	IC manufacturer	×	IC certification	IC manufacturer site
	4	MRTD packaging responsible	×		Packaging centre
		Embedded software loading responsible	✓	ALC Embedded software loading centre	IDEMIA audited sites
	TOE delivery point				
	5	Pre-personalization agent	×	AGD_PRE	
3 - Personalization	6	Personalization agent	×	AGD_PRE	
4 - Operational Use	7	End user	×	AGD_OPE	

Table 7 - Subjects identification following life cycle steps – Scheme 2

Scheme 3, MRTD chip Embedded Software loaded by the Flash Loader with optional Package 2 (See [IC_ST]) in step 4 after Part of TOE (Embedded Software) delivery point:

Phase	*Step*	*Subject*	*Emb. Sw. loading*	*Covered by*	*Sites*
1 - Development	1	IC developer	×	IC certification	IC developer site
	2	TOE developer	×	ALC R&D sites	Pessac and Courbevoie
2 - Manufacturing	3	IC manufacturer	×	IC certification	IC manufacturer site
	4	**Part of TOE (Embedded Software) delivery point**			
		MRTD packaging responsible	×		Packaging centre
		Embedded software loading responsible	✓	AGD_PRE	Embedded software loading centre
	5	Pre-personalization agent	×	AGD_PRE	
3 - Personalization	6	Personalization agent	×	AGD_PRE	
4 - Operational Use	7	End user	×	AGD_OPE	

Table 8 - Subjects identification following life cycle steps – Scheme 3

Regarding schemes 2 and 3, the security of the loading mechanism is ensured by the Flash Loader covered by the IC certificate [IC_CERT].

2.2.3.2 Life cycle phases

The following text was extracted from [PP_BAC]. Due to the previous specified life cycles and to the technology of the IC, some interpretations have to be done by the reader of this ST. The table below indicates how terms shall be read:

Term in [PP_EAC]	Meaning in this ST
Software developer	TOE developer
non-volatile non-programmable memory(ies)	Part of the Flash memory where the Flash Loader and the OS are loaded. This memory is programmable by the IC manufacturer or using the Flash Loader. Once the Flash Loader is blocked, this memory is Read Only Memory
ROM	
non-volatile programmable memory(ies)	Part of the Flash memory where initialization data and user data are written.
EEPROM	

The TOE life cycle is described in terms of the four life cycle phases and subdivided into 7 steps (with respect to the [PP_IC]).

2.2.3.2.1 Phase 1 “Development”

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

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

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

Note: If scheme 1 is applied, the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. For details, please refer to ALC and in particular to [ALC_STM]. If scheme 2 or 3 are applied, the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the MRTD manufacturer. For details, please refer to ALC and in particular to [ALC_SCT].

2.2.3.2.2 Phase 2 “Manufacturing”

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

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

Note: If scheme 2 or 3 are applied, the TOE integrated circuit is produced containing the Flash Loader in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

Note 2: Regarding key management, the Flash Loader usage is protected by successful Km authentication. For details, please refer to [IC_PPM]. This key is securely transferred to IC manufacturer as detailed in ALC and more precisely in [ALC_KM].

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

Note: If scheme 2 or 3 are applied, the MRTD manufacturer (i) loads the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories (ii) adds the parts of the IC Embedded Software in the non-volatile programmable memories.

(Step5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD's chips with pre-personalization Data.

Application Note 2: Creation of the application implies the creation of MF and ICAO.DF.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

2.2.3.2.3 Phase 3 "Personalization of the MRTD"

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

The signing of the Document security object by the Document Signer [ICAO_9303] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Application note 3: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [CC_1] §92) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Basic Authentication Control Key.

Application note 4: This security target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [6]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

2.2.3.2.4 Phase 4 "Operational Use"

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

Application note 5: The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 "Operational Use". This will imply an update of the Document Security Object including the re-signing by the Document Signer.

Application note 6: The intention of this security target is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase 2 or later. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.
Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

2.2.4 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 TOE Architecture

The TOE is composed of an IC and some software components as presented in Figure 1. Each part of the TOE is presented in the following chapters.

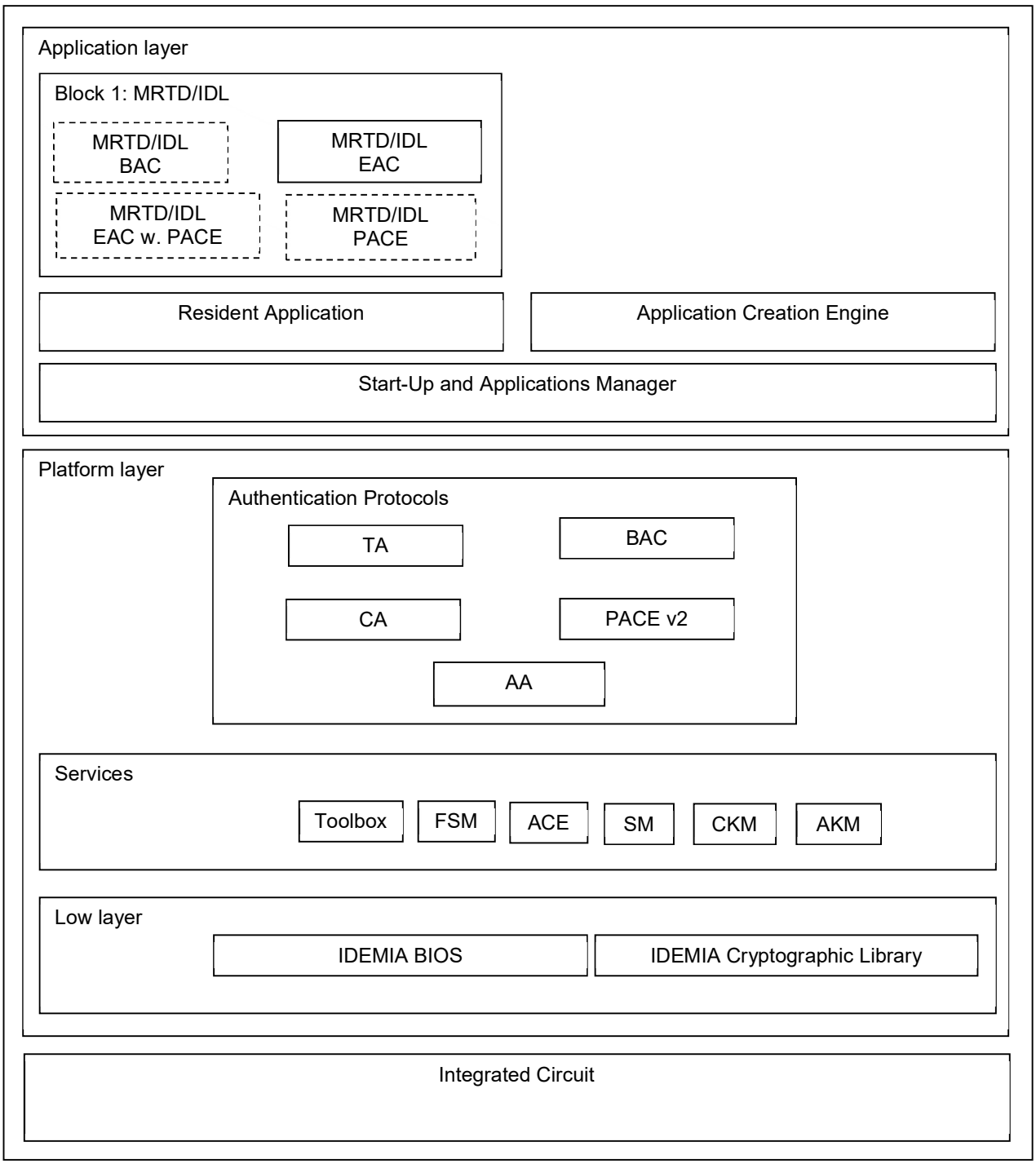

Figure 1 - TOE architecture

2.3.2 Integrated Circuit

The TOE is embedded on Infineon components (cf § 2.1.3). Theses IC comprise the following:

Communication protocols:
- ISO 14443 Type A and Type B defined proximity contactless protocol
- ISO 7816 defined standard contact based communication protocol

Core System:
- Proprietary dual CPU implementation being comparable to the 80251 microcontroller architecture from functional perspective and with enhanced MCS 251 instruction set
- Cache with Post Failure Detection
- Memory Encryption/Decryption Unit (MED)
- Memory Management Unit (MMU)

Memories:
- Read-Only Memory (ROM), not available for the user
- Random Access Memory (RAM)
- SOLID FLASH™ NVM, the flash cell based non-volatile memory

Buses:
- Memory Bus
- Peripheral Bus

Coprocessors:
- Crypto2304T for asymmetric algorithms like RSA and EC
- Symmetric Crypto Coprocessor for AES and 3DES Standards

Control:
- Interface Management Module (IMM)
- Interrupt and Peripheral Event Channel Controller (ITP)
- Clock & Power Management
- Control

System Peripherals
- Sensors & Filters
- User mode Security Life Control (UmSLC)

Peripherals:
- Hybrid Physical True Random Number Generator (HPTRNG) implementing also Deterministic Random Number Generator (DRNG)
- Watchdog and Timers
- Cyclic Redundancy Check module (CRC)
- Universal Asynchronous Receiver/Transmitter (UART)
- Radio Frequency Interface (RF power and signal interface)
- Analogue Contactless Bridge (ACLB)
- Inter-Integrated Circuit module (I2C)
- General Purpose Input Output (GPIO)

The firmware is composed of the:
- Boot-up software (BOS), the Resource Management System (RMS), the Flash Loader (FL) and the RFI supporting functions. The BOS applies the essential configuration, internal testing and the start-up.

- The RMS implements a low level application interface (API) to the Smartcard Embedded Software and provides handling and managing routines for RAM, MMU, Branch table, configuration and further functions.
- The Flash Loader allows downloading user software to the SOLID FLASH™ NVM during the manufacturing process and also at user premises - if ordered.
- The Radio Frequency Interface Application Interface (RFAPI) functions consist of executable code in the ROM which is part of the TOE and a SOLID FLASH™ NVM code part which is delivered separately to the user and which is not part of the TOE.

IC is part of the TOE and also part of the TSF. More information on the chips is given in the related Security Target [IC_ST].

2.3.3 Low layer

2.3.3.1 IDEMIA Basic Input/Output System (**BIOS**)

The BIOS module provides access management (read/write) functionalities to upper-layer application. It also provides exception and communication functionalities.

The BIOS module is part of the TOE and is also part of the TSF.

2.3.3.2 IDEMIA Cryptographic library (**Crypto**)

The Cryptography module provides secure cryptographic functionalities to upper-layer applications.

The Crypto module is part of the TOE and is also part of the TSF.

2.3.4 Platform layer

2.3.4.1 Services

2.3.4.1.1 File System Management (**FSM**)

The FSM module manages files and data objects according to ISO 7816-4 and 7816-9. It also manages the Digitally Blurred Image process, allowing for blurring a JPG or JPEG2000 image stored in a transparent file. This feature is covered by a patent owned by IDEMIA.

The FSM module is part of the TOE and is also part of the TSF.

2.3.4.1.2 Secure Messaging (**SM**)

The SM module provides functionalities to encrypt/decrypt data for secure communication in Manufacturing, Personalization and Operational Use phases (steps 5, 6 and 7). A Secure Messaging session begins after a successful authentication (GP authentication for Pre-personalization and Personalization phases, BAC or CA for Operational Use phase).

The SM module is part of the TOE and is also part of the TSF.

2.3.4.1.3 Cryptography Key Management (**CKM**)

The CKM module is responsible for asymmetric cryptography key management and asymmetric cryptography operations.

The CKM module is part of the TOE and is also part of the TSF.

2.3.4.1.4 Authentication and Key Management (**AKM**)

This module supplies:

- Symmetric Key management (read, write, access control),
- Services to manage Global Platform authentication and secure messaging.

The AKM module is part of the TOE and is also part of the TSF.

2.3.4.1.5 Access Condition Engine (**ACE**)

The ACE module is in charge of the verification of the Access Conditions of an object (files and keys) when an application tries to access this object.

The ACE module is part of the TOE and is also part of the TSF.

2.3.4.1.6 Toolbox (**TBX**)

The Toolbox module provides different kind of services to other modules.

- Services to manage APDU,
- Services to handle BER-TLV constructed data object,
- Services to process specific cryptographic operations,
- Services to handle Object Identifier,
- Services to manage MRZ (personalization and misuse management),
- Services to handle data in a secure way.

The TBX module is part of the TOE but and is also part of the TSF.

2.3.5 Authentication Protocols

2.3.5.1 Terminal Authentication (**TA**)

The TA module processes the Terminal Authentication (v1 and v2) mechanism. Terminal Authentication v1 is part of the EACv1 procedure defined in [TR_03110].

The TA module is part of the TOE and also part of the TSF.

2.3.5.2 Chip Authentication (**CA**)

The CA module processes the Chip Authentication (v1 and v2) mechanism. Chip Authentication v1 is part of the EACv1 procedure defined in [TR_03110].

The CA module is part of the TOE and also part of the TSF.

2.3.5.3 Password Authenticated Connection Establishment (**PACE v2**)

The PACE module provides functionalities to process the PACE v2 mechanism as defined in [TR_03110].

*The PACE v2 module is part of the TOE but is **NOT** part of the TSF.*

2.3.5.4 Active Authentication (**AA**)

The AA module provides functionalities to process the AA mechanism as defined in [ICAO_9303].

The AA module is part of the TOE and is also part of the TSF.

2.3.6 Application layer

2.3.6.1 Start-Up and Applications Manager (**Boot**)

The Boot module is responsible to manage the start-up of the applications (MRTD, RA and ACRE).

The Boot module is part of the TOE and is also part of the TSF

2.3.6.2 Application Creation Engine (**ACRE**)

The Application Creation Engine is a complete set of commands used to (pre-)personalize the card and its application(s). It includes:

- Additional Code loading,
- Creation of application,
- Import and Generation of the Active Authentication key (ECC and RSA keys),
- Import and Generation of multiple Chip Authentication keys under the ADF (supporting ECC and RSA Keys),
- Storage of CVCA Keys under each ADF.

The Additional Code Loading process is as follow:

1. Additional Code's Secure Messaging keys (authenticity and confidentiality) calculation,
2. Additional Code loading,
3. Additional Code activation.

The ACRE module is part of the TOE and is also part of the TSF.

2.3.6.3 Resident Application (**RA**)

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

The RA module is part of the TOE and is also part of the TSF.

2.3.6.4 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).

The MRTD module is part of the TOE and is also part of the TSF.

2.3.7 Other features

2.3.7.1 Automatic BAC phasing out

The TOE also supports a mechanism allowing the automatic deactivation of the BAC protocol after the current date (of the TOE) has reached a reference date - chosen by the issuer and configured by the personalization Agent. The current date is the internal date updated through the EAC protocol. Thanks to this feature, it is possible to issue MRTD supporting both PACE and BAC as needed for interoperability reasons and perform smooth phasing out of the BAC protocol in the medium term (due to its cryptographic weaknesses) during the life time of the issued MRTD, without having to wait for the complete renewal of issued MRTD (> 10 years).

The automatic BAC phasing out is part of the TOE and is also part of the TSF.

2.3.7.2 Enhanced protection over Sensitive biometric data reading

The access to sensitive biometric data (such as 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. If this condition is not met (algorithm not strong enough), the access to the sensitive data is denied.

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

2.3.7.3 Automatic DES SM phasing out

The TOE allows for the automatic deactivation of the DES algorithm, in the scope of secure channel protection, after the current date has reached a target date - chosen by the issuer and configured by the Personalization Agent. The current date is the internal date updated through the EAC protocol. This mechanism enables smooth phasing out of the DES protocol in the medium term (due to its cryptographic weaknesses) during the lifetime of the issued MRTDs, without having to wait for the complete renewal of issued MRTD (> 10 years).

The automatic DES SM phasing out is part of the TOE and is also part of the TSF.

3 CONFORMANCE CLAIMS

3.1 Common Criteria conformance

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

The conformance to the CC is claimed as follows:

CC	**Conformance Claim**
Part 1	Strict conformance
Part 2	Conformance with extensions: • FAU_SAS.1 *"Audit storage",* • FCS_RND.1 *"Quality metric for random numbers",* • FIA_API.1 *"Authentication Proof of Identity",* • FMT_LIM.1 *"Limited capabilities",* • FMT_LIM.2 *"Limited availability",* • FPT_EMS.1 *"TOE Emanation"*
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 9 – Common Criteria conformance claim

Remark

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

As product is targeting "Qualification renforcée" all activities for ALC_FLR.3 have been processed. However, this assurance package is not properly claimed in the present security target as the chip does not support it.

3.2 Protection Profile conformance

3.2.1 Overview

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

Title	Protection Profile – Machine Readable Travel Document with ICAO Application, Extended Access Control (PP-MRTD EAC)
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 10 – Protection Profile conformance

This ST also addresses the Manufacturing and Personalization phases at TOE level (cf. §2.2.3 TOE life cycle), as well as the Active Authentication (AA) protocols available in operational use phase. 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.

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],
- **A.Insp_Sys_Chip_Auth** "Inspection Systems for global interoperability on chip authenticity" defined in this ST

A.Insp_Sys_Chip_Auth is additional for Active Authentication protocol which is not in the original scope of the [PP_EAC]. This assumption is only linked to threats for the Active Authentication protocol so these objectives neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the [PP_EAC], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_EAC].

3.2.3 Threats

The following threats are averted by this TOE:

- **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,
- **T. BAC_breaking** "*BAC protocol is broken*" defined in this ST,
- **T.Unauthorized_Load** defined in [JIL_SRCL],

- **T.Bad_Activation** defined in [JIL_SRCL],
- **T.DES_Session_Key_Uncovery** "DES session keys are uncovered" 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.BAC_Expiration** *"Automatic deactivation of BAC protocol"* defined in this ST,
- **OT.AC_SM_Level** *"Access control to sensitive biometric reference data according to SM level"* defined in this ST,
- **OT.Secure_Load_ACode** *"Secure loading of the Additional Code"* defined in [JIL_SRCL]
- **OT.Secure_AC_Activation** *"Secure activation of the Additional Code"* defined in [JIL_SRCL],
- **OT.TOE_Identification** "Secure identification of the TOE" defined in [JIL_SRCL],
- **OT.DES_SM_Expiration** "Automatic deactivation of DES-based secure messaging" 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.Exam_Chip_Auth** *"Examination of the chip authenticity"* defined in this ST,
- **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].

OE.Exam_Chip_Auth is additional for Active Authentication protocol which is not in the original scope of the [PP_EAC]. This assumption is only linked to threats for the Active Authentication protocol so these objectives neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the

[PP_EAC], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [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

4.1.1 Logical MRTD data

The following table presents the assets of the TOE and their corresponding phase(s) according to §2.2.3 TOE life cycle:

Asset	Step 5	Step 6	Step 7
Personal Data	×	✓	✓
Biometric Data	×	✓	✓
EF.COM	×	✓	✓
EF.SOD	×	✓	✓
CA_PK	×	✓	✓
CA_SK	×	✓	✓
AA_PK	×	✓	✓
AA_SK	×	✓	✓
CPLC	✓	✓	✓
TOE_ID	✓	✓	✓
Pre-Perso_K	✓	×	×
Perso_K	×	✓	×
Session_K	✓	✓	✓
LCS	✓	✓	✓
Configuration data	✓	✓	✓
Updatable Data	×	✓	✓
Additional Code	✓	✓	✓
LSK	✓	×	×
DIV_LSK	✓	×	×

Table 11 – Assets of the TOE and their corresponding phase(s)

4.1.1.1 Personal Data

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

4.1.1.2 Biometric Data

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

4.1.1.3 EF.COM

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

4.1.1.4 EF.SOD

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

4.1.1.5 Chip Authentication Public Key (CA_PK)

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

4.1.1.6 Chip Authentication Private Key (CA_SK)

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

4.1.1.7 Active Authentication Public Key (AA_PK)

The Active Authentication Public Key (contained in EF.DG15) is used by the inspection system for the Active Authentication.

4.1.1.8 Active Authentication Private Key (AA_SK)

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

4.1.1.9 CPLC

The CPLC Data are the Card Production Life Cycle data. They are considered as user data as they enable to track the holder. These data are filled during steps 4, 5 and 6 by subjects.

4.1.1.10 TOE_ID

These data allow the identification of the TOE. These data are part of the IC Embedded Software in the non-volatile non-programmable memory. If Additional Code is loaded, then the TOE_ID contains Additional Code Identification Data.

4.1.1.11 Pre-personalization Agent keys (Pre-perso_K)

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

4.1.1.12 Personalization Agent keys (Perso_K)

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

4.1.1.13 Secure Messaging session keys (Session_K)

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

4.1.1.14 TOE Life Cycle State (LCS)

This is the Life Cycle State of the TOE.

4.1.1.15 Configuration Data

These specific data set the configuration of the TOE in terms of security features and security functions. These configuration data can be set in Manufacturing and Personalization phases (Steps 5 and 6) after authentication of the relevant agent with the relevant key set.

4.1.1.16 Updatable Data

Data other than Personal Data, Biometric Data, EF.COM, EF.SOD, CA_PK, CA_SK, AA_PK, AA_SK, CPLC, TOE_ID, Pre-Perso_K, Perso_K, Session_K, LCS and Configuration Data which can be modified in Operational Use phase.

4.1.1.17 Additional Code

This is the Additional Code to be loaded on the Initial TOE during Pre-personalisation by the Pre-personalization Agent. The result of this operation is the Final TOE.

4.1.1.18 Load Secure Key (LSK) and Diversified LSK (DIV_LSK)

This Load Secure Key (LSK) is the secret key used to calculate the Diversified LSK (DIV_LSK). The Diversified LSK is a session key used to verify the Additional Code confidentiality and integrity.

4.1.2 Authenticity of the MRTD's chip

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

4.2 Subjects

4.2.1 Overview

The following table presents the assets of the TOE and their corresponding phase(s) according to §2.2.3 TOE life cycle:

Subject	Descr.	Step 3	Step 4	Step 5	Step 6	Step 7
IC manufacturer (Manufacturer role)	§ 4.2.2	✓	×	×	×	×
MRTD packaging responsible (Manufacturer role)	§ 4.2.3	×	✓	×	×	×
Embedded software loading responsible (Manufacturer role)	§ 4.2.4	×	✓	×	×	×
Pre-personalization Agent (Manufacturer role)	§ 4.2.5	×	×	✓	×	×
Personalization Agent	§ 4.2.6	×	×	×	✓	×
Country Verifying Certification Authority	§ 4.2.7	×	×	×	×	✓
Document Verifier	§ 4.2.8	×	×	×	×	✓
Terminal	§ 4.2.9	×	×	✓	✓	✓
Inspection System	§ 4.2.10	×	×	×	×	✓
MRTD Holder	§ 4.2.11	×	×	×	×	✓
Traveler	§ 4.2.12	×	×	×	×	✓
Attacker	§ 4.2.13	✓	✓	✓	✓	✓

Table 12 – Subjects of the TOE and their corresponding phase(s)

4.2.2 IC manufacturer

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

If scheme 1 is applied (cf. § 2.2.3), this subject is responsible for the embedded software downloading in the IC. This subject does not use Flash loader, even if it is embedded in the IC.

4.2.3 MRTD packaging responsible

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

4.2.4 Embedded software loading responsible

This additional subject is a refinement of the role Manufacturer as described in [PP_EAC]. This subject is responsible for the embedded software loading when scheme 2 is applied (cf. § 2.2.3). This subject does not exist if scheme 1 is applied (cf. § 2.2.3). This subject uses the Flash loader embedded in the IC.

4.2.5 Pre-personalization Agent

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

4.2.6 Personalization Agent

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

4.2.7 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.

4.2.8 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.

4.2.9 Terminal

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

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

4.2.10 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.

4.2.11 MRTD Holder

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

4.2.12 Traveler

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

4.2.13 Attacker

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

Application note 9: 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 PP since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys that is covered by [25]. 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

Application note 10: 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 Assumptions

4.3.1 **A.MRTD_Manufact** *"MRTD manufacturing on steps 4 to 6"*

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

Note: for scheme 3, MRTD means the Integrated Circuit and its embedded Loader and the Loader associated keys, the Embedded Software to be loaded and the Logical MRTD data.

4.3.2 **A.MRTD_Delivery** *"MRTD delivery during steps 4 to 6"*

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

- 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.

Note: for scheme 3, MRTD means the Integrated Circuit and its embedded Loader and the Loader associated keys, the Embedded Software to be loaded and the Logical MRTD data.

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

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

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

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing 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.

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

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which securely generates stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the

Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

4.3.6 **A.Auth_PKI** *"PKI for Inspection Systems"*

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.

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

The Inspection System implements Active Authentication to authenticate the MRTD's chip. The Inspection System uses the signature returned by the TOE during Active Authentication as proof of authenticity.

4.4 Threats

Application note 11: The threats T.Chip_ID and T.Skimming (cf. [25]) are averted by the mechanisms described in the BAC PP [25] (cf. P.BAC-PP) which cannot withstand an attack with high attack potential thus these are not addressed here. T.Chip_ID addresses the threat of tracing the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. T.Skimming addresses the threat of imitating the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Both attacks are conducted by an attacker who cannot read the MRZ or who does not know the physical MRTD in advance.

4.4.1 **T.Read_Sensitive_Data** *"Read the sensitive biometric reference 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.

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

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

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

Asset: authenticity of logical MRTD data.

4.4.3 **T.Counterfeit** *"MRTD's chip"*

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

data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

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

Asset: authenticity of logical MRTD data.

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

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

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

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

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

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

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

Asset: confidentiality of logical MRTD and TSF data.

4.4.6 **T.Phys-Tamper** "Physical Tampering"

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

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

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

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

Adverse action: An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE of (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

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

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

4.4.9 **T. Forgery_Supplemental_Data** *"Forgery of supplemental data stored in the TOE"*

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

4.4.10 **T. BAC_breaking** "*BAC protocol is broken*"

Adverse action: An attacker manages to break the BAC protocol using cryptanalysis means and powerful computation capacity leading to threaten (1) the non traceability and (2) confidentiality of data.
The attacker is able to intercept and record a log of BAC transaction during inspection at a border control. Then using computation capacity, he is able to perform reverse engineering over the logs, to break the protocol within a few minutes or less and get (1) the MRZ value, and (2) the log of plain text exchanged between the MRTD and the inspection system.
This leads the attacker to (1) get the holder information and use it, and (2) trace the holder in real time.

Threat agent: having high attack potential, being able to intercept transaction with MRTDs.

Asset: confidentiality of data read from the MRTD, traceability of the MRTD

4.4.11 **T.Unauthorized_Load**

Adverse action: An attacker tries to load an additional code that is not intended to be assembled with the initial TOE, i.e. the evidence of authenticity or integrity is not correct.

Threat agent: having high attack potential, knowing the MSK, LSK and derivation data, being in possession of a legitimate MRTD

Asset: Logical MRTD data

4.4.12 **T.Bad_Activation**

Adverse action: An attacker tries to perturbate the additional code activation such as the final TOE is different than the expected one (initial TOE or perturbed TOE).

Threat agent: having high attack potential, knowing the MSK, LSK and derivation data, being in possession of a legitimate MRTD, being in possession of an additional code that is authorized to be loaded.

Asset: Logical MRTD data

4.4.13 **T.DES_Session_Key_Uncovery** "DES session keys are uncovered"

Adverse action: An attacker manages to uncover the DES session keys protecting the exchanges between the TOE and the Inspection System using passive analysis, cryptanalysis means and powerful computation capacity leading to threaten (1) the confidentiality, (2) the integrity and (3) the authenticity of data exchanged during the session.
The attacker is able to monitor protected data exchanged between the TOE and the Inspection System through a secure channel previously established by the TOE and the Inspection System. Then due to the DES algorithm being vulnerable to known-plaintext attacks, the attacker is able to determine the values of the session keys using computational capacity and (1) reveal, (2) alter or (3) counterfeit exchanged data within the active secure messaging session.

Threat agent: having high attack potential, being able to monitor exchanges between the TOE and the Inspection System.

Asset: confidentiality and integrity of MRTD data

4.5 Organisational Security Policies

4.5.1 P.BAC-PP “Fulfillment of the Basic Access Control Protection Profile”

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 Doc 9303’ [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 12: The organizational security policy P.Personal_Data drawn from the ‘ICAO Doc 9303’ [ICAO_9303] is addressed by the [PP_BAC]. 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).

4.5.2 P.Sensitive_Data “Privacy of sensitive biometric reference 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

4.5.3 P.Manufact “Manufacturing of the MRTD’s chip”

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

4.5.4 **P.Personalization** *“Personalization of the MRTD by issuing State or Organization only”*

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

5 SECURITY OBJECTIVES

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

5.1 Security objectives for the TOE

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

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

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO_9303] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

5.1.2 **OT.Data_Int** *"Integrity of personal data"*

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

5.1.3 **OT.Sens_Data_Conf** *"Confidentiality of sensitive biometric reference data"*

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.

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

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

Note: for scheme 3, TOE means the Integrated Circuit and its embedded Loader, the Embedded Software to be loaded and the Logical MRTD data. The IC shall be able to authenticate itself to external entities. The Initialisation Data are used for IC authentication verification data.

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

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.

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

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

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

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

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

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

5.1.8 **OT.Prot_Phys-Tamper** *"Protection against Physical Tampering"*

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

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

with a prior

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

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

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

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

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

5.1.11 **OT.Update_File** *"Modification of file in Operational Use Phase"*

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.

5.1.12 **OT.BAC_Expiration** *"Automatic deactivation of BAC protocol"*

During Operational Use phase, the TOE must disable the Basic Access Control protocol if the expiry date of this protocol is exceeded.

5.1.13 **OT.AC_SM_Level** *"Access control to sensitive biometric reference data according to 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.

5.1.14 **OT.Secure_Load_ACode** *"Secure loading of the Additional Code"*

The Loader of the Initial TOE shall check an evidence of authenticity and integrity of the loaded Additional Code.
The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE.
The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE.
During the Load Phase of an Additional Code, the TOE shall remain secure.

5.1.15 **OT.Secure_AC_Activation** *"Secure activation of the Additional Code"*

Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way.
All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation.
If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE such as tearing, integrity violation, error case…), the Initial TOE shall remain in its initial state or fail secure.

5.1.16 **OT.TOE_Identification** "Secure identification of the TOE"

The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data.
After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user must be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.

5.1.17 **OT.DES_SM_Expiration** *"*Automatic deactivation of DES-based secure messaging*"*

During Pre-Personalization phase, Personalization Phase and Operational Use phase, the TOE must not authorize the establishment of a secure messaging session whose security relies on the DES algorithm in the event of the expiry of this algorithm.

5.2 Security objectives for the operational environment

5.2.1 Issuing State or Organization

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

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

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

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

Note: for scheme 3, TOE means the Integrated Circuit and its embedded Loader, the Embedded Software to be loaded and the Logical MRTD data. Therefore, security procedures shall be used to:

1. maintain confidentiality and integrity of the code loading process during Phase 4, Phase 5 and Phase 6,
2. Protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader,
3. Implement the authentication verification mechanism and know authentication reference data of the TOE,
4. Fulfil the access conditions required by the Loader.

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

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

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

  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

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

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

Note: for scheme 3, TOE means the Integrated Circuit and its embedded Loader, the Embedded Software to be loaded and the Logical MRTD data. Therefore, security procedures shall be used to:

5. maintain confidentiality and integrity of the code to be loaded during Phase 4, Phase 5 and Phase 6,
6. realize appropriate Loader key management in the environment (confidentiality must be maintained).

5.2.1.3 **OE.Personalization** *"Personalization of logical MRTD"*

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

5.2.1.4 **OE.Pass_Auth_Sign** *"Authentication of logical MRTD by Signature"*

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO_9303].

5.2.1.5 **OE.Auth_Key_MRTD** *"MRTD Authentication Key"*

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

(i) generate the MRTD's Authentication Key Pair(s), (ii) ensure the secrecy of the MRTD's Authentication Private Key(s), (iii) sign and store the Authentication Public Key(s) in the Authentication Public Key data (i.e in EF.DG14 for Chip Authentication Public Key and in EF.DG15 for Active Authentication Public Key) and (iv) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Authentication Public Key by means of the Document Security Object.

5.2.1.6 OE.Authoriz_Sens_Data *"Authorization for Use of Sensitive Biometric Reference 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.

5.2.1.7 **OE.BAC_PP** *"Fulfillment of the Basic Access Control Protection Profile"*

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

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

5.2.2.1 **OE.Exam_MRTD** *"Examination of the MRTD passport book"*

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing

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.

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

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

5.2.2.3 **OE.Passive_Auth_Verif** *"Verification by Passive Authentication"*

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

5.2.2.4 **OE.Prot_Logical_MRTD** *"Protection of data from the logical MRTD"*

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

5.2.2.5 **OE.Ext_Insp_Systems** *"Authorization of Extended Inspection 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 Introduction

Assumption	Related Security Objective(s)	Rationale
A.MRTD_Manufact	OE.MRTD_Manufact	§ 5.3.2.1
A.MRTD_Delivery	OE.MRTD_Delivery	§ 5.3.2.2
A.Pers_Agent	OE.Personalization	§ 5.3.2.3
A.Insp_Sys	OE.Exam_MRTD OE.Prot_Logical_MRTD	§ 5.3.2.4
A.Insp_Sys_Chip_Auth	OE.Exam_Chip_Auth	§ 5.3.2.5
A.Signature_PKI	OE.Pass_Auth_Sign OE.Exam_MRTD	§ 5.3.2.6
A.Auth_PKI	OE.Auth Key MRTD OE.Ext Insp Systems	§ 5.3.2.7

Table 13- Assumptions of the TOE and Security Objectives

Threat	Related Security Objective(s)	Rationale
T.Read_Sensitive_Data	OT.Sens Data Conf OE.Authoriz Sens Data OE.Ext Insp Systems OT.AC_SM_level	§ 5.3.3.1
T.Forgery	OT.AC_Pers OT.Data_Int OT.Prot_Phys-Tamper OE.Pass_Auth_Sign OE.Exam MRTD OE.Passive_Auth_Verif	§ 5.3.3.2
T.Counterfeit	OT.Chip_Auth_Proof OE.Auth_Key_MRTD OE.Exam_MRTD OE.Exam_Chip_Auth	§ 5.3.3.3
T.Abuse-Func	OT.Prot_Abuse-Func	§ 5.3.3.4
T.Information_Leakage	OT.Prot_Inf_Leak	§ 5.3.3.5
T.Phys-Tamper	OT.Prot_Phys-Tamper	
T.Malfunction	OT.Prot_Malfunction	
T.Configuration	OT.Configuration OT.TOE_Identification	§ 5.3.3.6
T.Forgery_Supplemental_Data	OT.Update_File	§ 5.3.3.7
T.BAC_breaking	OT.BAC_Expiration	§ 5.3.3.8
T.Unauthorized_Load	OT.Secure_Load_ACode OT.TOE_Identification	§ 5.3.3.9
T.Bad_Activation	OT.Secure_AC_Activation OT.TOE_Identification	§ 5.3.3.10
T.DES_Session_Key_Uncovery	OT.DES_SM_Expiration	§ 5.3.3.11

Table 14- Threats of the TOE and Security Objectives

OSP	Related Security Objective(s)	Rationale
P.BAC-PP	OE.BAC-PP	§ 5.3.4.1
P.Manufact	OT.Identification	§ 5.3.4.2
P.Personalization	OT.AC_Pers OT.Identification OE.Personalization	§ 5.3.4.3

P.Sensitive_Data	OT.Sens Data Conf OE.Authoriz Sens Data OE.Ext Insp Systems	§5.3.4.4

Table 15- OSP of the TOE and Security Objectives

5.3.2 Rationales for Assumptions

5.3.2.1 A.MRTD_Manufact

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

5.3.2.2 A.MRTD_Delivery

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

5.3.2.3 A.Pers_Agent

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

5.3.2.4 A.Insp_Sys

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** *"Inspection Systems for global interoperability"* is covered by the security objectives for the TOE environment **OE.Exam_MRTD** *"Examination of the MRTD passport book"* 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

5.3.2.5 A.Insp_Sys_Chip_Auth

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

5.3.2.6 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"*.

5.3.2.7 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.

5.3.3 Rationales for Threats

5.3.3.1 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.

5.3.3.2 T.Forgery

The threat **T.Forgery** "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** *"Access Control for Personalization of logical MRTD"* requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. **OE.Personalization** *"Personalization of logical MRTD"*). 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"*.

5.3.3.3 T.Counterfeit

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

This threat is also covered by **OE.Auth_Key_MRTD** *"MRTD Authentication Key"* using a authentication key pair to be generated by the issuing State or Organization. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects. According to **OE.Exam_Chip_Auth** *"Examination of the chip authenticity"* the inspection system has to perform the Active Authentication Protocol to verify the authenticity of the MRTD's chip.

5.3.3.4 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.

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

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

5.3.3.6 T.Configuration

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

5.3.3.7 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.

5.3.3.8 T.BAC_breaking

The threat **T. BAC_breaking** "*BAC protocol is broken*" addresses the attack aiming at breaking the BAC protocol. The protection of the TOE against this threat is addressed by security objective **OT.BAC_Expiration** *"Automatic deactivation of BAC protocol"* which is directly related to it. It prevents an attacker to perform offline dictionary attacks on transaction log, in order to preserve confidentiality of data and avoid citizen traceability.

5.3.3.9 T.Unauthorized_Load

The threat **T.Unauthorized_Load** addresses the attack of loading an unauthorized code on the smart card product, when the loader (additional code loader) is available, that means in phase 5. Although this threat is mitigated by the conditions of loading in a secure environment, the TOE scope considers this attack as the TOE delivery point is end of phase 3. This threat is mitigated by the authentication of the Pre-personalization Agent with MSK and the calculation of the DIV_LSK which constitutes in itself the proof of authenticity and integrity of the additional code to be loaded. The objective **OT.Secure_Load_ACode** *"Secure loading of the Additional Code"* covers then this threat. Furthermore, the objective **OT.TOE_Identification** also covers this threat allowing to identify uniquely the Final TOE.

5.3.3.10 T.Bad_Activation

The threat **T.Bad_Activation** addresses the attack of perturbation of activation an allowed source code. We consider that the source code allowance for this threat is correct, that means that this threat only covers allowed source code. The attacker perturbates the activation such as to invalidate the additional source code activation or obtaining a bad TOE. This threat is mitigated by the objective **OT.Secure_AC_Activation** *"Secure activation of the Additional Code"* which requires the TOE protects this activation. This activation is performed within one LOAD_SECURE command. Furthermore, the objective **OT.TOE_Identification** also covers this threat allowing to identify uniquely the Final TOE.

5.3.3.11 T.DES_Session_Key_Uncovery

The threat **T.DES_Session_Key_Uncovery** "DES session keys are uncovered" addresses the attack aiming at uncovering the session keys from an already established secure channel, whose security relies on the DES algorithm. The security objective **OT.DES_SM_Expiration** *"*Automatic deactivation of DES-based secure messaging*"* assures the protection of the TOE against this threat as it prevents establishment of a DES-based secure channel from the moment the DES algorithm has been revoked.

5.3.4 Rationales for Organisational Security Policies

5.3.4.1 P.BAC-PP

The OSP **P.BAC-PP** *"Fulfillment of the Basic Access Control Protection Profile"* is directly addressed by the **OE.BAC_PP** *"Fulfillment of the Basic Access Control Protection Profile"*.

5.3.4.2 P.Manufact

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

5.3.4.3 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.

5.3.4.4 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"*

6 EXTENDED COMPONENTS DEFINITION

6.1 Extended components definition

6.1.1 Definition of the Family FAU_SAS

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

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

FAU_SAS ***“Audit data storage”***

Family behavior

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

Component leveling

FAU_SAS.1	Requires the TOE to the possibility to store audit data
Management:	FAU_SAS.1
	There are no management activities foreseen.
Audit:	FAU_SAS.1
	There are no actions defined to be auditable.

FAU_SAS.1 ***“Audit storage”***

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.2 Definition of the Family FCS_RND

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

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

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

Family behavior

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

Component leveling:

FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.

FCS_RND.1 ***“Quality metric for random numbers”***

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.3 Definition of the Family FIA_API

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

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

Family behavior

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

Component leveling:

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

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.

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

6.1.4 Definition of the Family FMT_LIM

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

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

FMT_LIM ***“Limited capabilities and availability”***

Family behavior

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

Component leveling:

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

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

FMT_LIM.1	***“Limited capabilities”***
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.

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

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2 ***"Limited availability"***

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

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

6.1.5 Definition of the Family FPT_EMS

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

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS.1 TOE emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 ***"TOE Emanation"***

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

7 SECURITY REQUIREMENTS

7.1 Security functional requirements

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

SFR in ST	SFR in [PP_EAC]	Descr.	Step			
			Before 5	5	6	7
FAU_SAS.1.1	FAU_SAS.1.1	7.1.1.1	✓	×	×	×
FCS_CKM.1.1/CA	FCS_CKM.1.1	7.1.2.1				
FCS_CKM.1.1/MSK_DIV	Additional SFR		×	✓	×	×
FCS_CKM.1.1/GP			×	✓	✓	×
FCS_CKM.1.1/LSK_DIV			×	✓	×	×
FCS_CKM.1.1/KEY_GEN			×	✓	✓	×
FCS_CKM.4.1	FCS_CKM.4.1	7.1.2.2	×	✓	✓	✓
FCS_COP.1.1/CA_SHA	FCS_COP.1.1/SHA	7.1.2.3	×	×	×	✓
FCS_COP.1.1/CA_ENC	FCS_COP.1.1/SYM		×	×	×	✓
FCS_COP.1.1/CA_MAC	FCS_COP.1.1/MAC		×	×	×	✓
FCS_COP.1.1/SIG_VER	FCS_COP.1.1/SIG_VER		×	×	×	✓
FCS_COP.1.1/MSK_SHA	Additional SFR		×	✓	×	×
FCS_COP.1.1/GP_ENC			×	✓	✓	×
FCS_COP.1.1/GP_AUTH			×	✓	✓	×
FCS_COP.1.1/GP_MAC			×	✓	✓	×
FCS_COP.1.1/GP_SDT_DEC			×	✓	✓	×
FCS_COP.1.1/ADDCODE_DEC			×	✓	×	×
FCS_COP.1.1/ADDCODE_MAC			×	✓	×	×
FCS_COP.1.1/ADDCODE_SHA			×	✓	×	×
FCS_COP.1.1/SIG_GEN			×	×	×	✓
FCS_RND.1.1	FCS_RND.1.1	7.1.2.4	×	✓	✓	✓
FIA_UID.1.1	FIA_UID.1.1	7.1.3.1	×	✓	✓	✓
FIA_UID.1.2	FIA_UID.1.2		×	✓	✓	✓
FIA_UAU.1.1	FIA_UAU.1.1	7.1.3.2	×	✓	✓	✓
FIA_UAU.1.2	FIA_UAU.1.2		×	✓	✓	✓
FIA_UAU.4.1	FIA_UAU.4.1	7.1.3.3	×	✓	✓	✓
FIA_UAU.5.1/EAC	FIA_UAU.5.1	7.1.3.4	×	×	✓	✓
FIA_UAU.5.2/EAC	FIA_UAU.5.2		×	×	✓	✓
FIA_UAU.5.1/MP	Additional SFR		×	✓	×	×
FIA_UAU.5.2/MP			×	✓	×	×
FIA_UAU.6.1/EAC	FIA_UAU.6.1	7.1.3.5	×	×	×	✓
FIA_UAU.6.1/MP	Additional SFR		×	✓	✓	×
FIA_UAU.6.1/ADD_CODE			×	✓	×	×
FIA_AFL.1.1/MP	Additional SFR		×	✓	✓	×
FIA_AFL.1.2/MP			×	✓	✓	×
FIA_API.1.1/CA	FIA_API.1.1	7.1.3.7	×	×	×	✓
FIA_API.1.1/AA	Additional SFR		×	×	×	✓
FDP_ACC.1.1/EAC	FDP_ACC.1.1	7.1.4.1	×	×	✓	✓
FDP_ACC.1.1/MP	Additional SFR		×	✓	✓	×
FDP_ACC.1.1/ID	Additional SFR		×	✓	✓	✓
FDP_ACC.1.1/UPD_FILE	Additional SFR		×	×	×	✓

SFR in ST	SFR in [PP_EAC]	Descr.	Step			
			Before 5	5	6	7
FDP_ACF.1.1/EAC	FDP_ACF.1.1	7.1.4.2	×	×	✓	✓
FDP_ACF.1.2/EAC	FDP_ACF.1.2		×	×	✓	✓
FDP_ACF.1.3/EAC	FDP_ACF.1.3		×	×	✓	✓
FDP_ACF.1.4/EAC	FDP_ACF.1.4		×	×	✓	✓
FDP_ACF.1.1/MP	Additional SFR		×	✓	✓	×
FDP_ACF.1.2/MP			×	✓	✓	×
FDP_ACF.1.3/MP			×	✓	✓	×
FDP_ACF.1.4/MP			×	✓	✓	×
FDP_ACF.1.1/ID	Additional SFR		×	✓	✓	✓
FDP_ACF.1.2/ID			×	✓	✓	✓
FDP_ACF.1.3/ID			×	✓	✓	✓
FDP_ACF.1.4/ID			×	✓	✓	✓
FDP_ACF.1.1/UPD_FILE	Additional SFR		×	×	✓	✓
FDP_ACF.1.2/UPD_FILE			×	×	✓	✓
FDP_ACF.1.3/UPD_FILE			×	×	✓	✓
FDP_ACF.1.4/UPD_FILE			×	×	✓	✓
FDP_UCT.1.1/EAC	FDP_UCT.1.1	7.1.4.3	×	×	×	✓
FDP_UCT.1.1/MP	Additional SFR		×	✓	✓	×
FDP_UCT.1.1/ADD_CODE			×	✓	×	×
FDP_UIT.1.1/EAC	FDP_UIT.1.1	7.1.4.4	×	×	×	✓
FDP_UIT.1.2/EAC	FDP_UIT.1.2		×	×	×	✓
FDP_UIT.1.1/MP	Additional SFR		×	✓	✓	×
FDP_UIT.1.2/MP			×	✓	✓	×
FDP_UIT.1.1/ADD_CODE			×	✓	×	×
FDP_UIT.1.2/ADD_CODE			×	✓	×	×
FDP_ITC.1.1/MP	Additional SFR	7.1.4.5	×	✓	✓	×
FDP_ITC.1.2/MP			×	✓	✓	×
FDP_ITC.1.3/MP			×	✓	✓	×
FMT_MOF.1.1/PROT	Additional SFR	7.1.5.1	×	✓	✓	×
FMT_MOF.1.1/GP			×	✓	✓	×
FMT_MOF.1.1/BAC_EXP			×	✓	✓	✓
FMT_MOF.1.1/DES_SM_EXP			×	✓	✓	✓
FMT_SMF.1.1	FMT_SMF.1.1	7.1.5.2	✓	✓	✓	×
FMT_SMR.1.1	FMT_SMR.1.1	7.1.5.3	×	✓	✓	✓
FMT_SMR.1.2	FMT_SMR.1.2		×	✓	✓	✓
FMT_LIM.1.1	FMT_LIM.1.1	7.1.5.4	×	✓	✓	✓
FMT_LIM.2.1	FMT_LIM.2.1		×	✓	✓	✓
FMT_MTD.1.1/INI_ENA	FMT_MTD.1.1/INI_ENA	7.1.5.6	×	✓	✓	✓
FMT_MTD.1.1/INI_DIS	FMT_MTD.1.1/INI_DIS		×	✓	✓	✓
FMT_MTD.1.1/CVCA_INI	FMT_MTD.1.1/CVCA_INI		×	✓	✓	✓
FMT_MTD.1.1/CVCA_UPD	FMT_MTD.1.1/CVCA_UPD		×	✓	✓	✓
FMT_MTD.1.1/DATE	FMT_MTD.1.1/DATE		×	✓	✓	✓
FMT_MTD.1.1/KEY_WRITE	FMT_MTD.1.1/KEY_WRITE		×	×	✓	×
FMT_MTD.1.1/CAPK	FMT_MTD.1.1/CAPK		×	✓	✓	✓
FMT_MTD.1.1/KEY_READ	FMT_MTD.1.1/KEY_READ		×	✓	✓	✓
FMT_MTD.1.1/MP_KEY_WRITE	Additional SFR		✓	✓	✓	✓
FMT_MTD.1.1/MP_KEY_READ			✓	✓	✓	✓
FMT_MTD.1.1/AA_KEY_WRITE			×	✓	✓	✓
FMT_MTD.1.1/AA_KEY_READ			×	✓	✓	✓
FMT_MTD.1.1/LCS_PREP			×	✓	✓	✓
FMT_MTD.1.1/LCS_PERS			×	✓	✓	✓
FMT_MTD.1.1/LSK_READ			✓	✓	✓	✓

SFR in ST	SFR in [PP_EAC]	Descr.	Step			
			Before 5	5	6	7
FMT_MTD.1.1/ADDCODE_LOAD			×	✓	✓	✓
FMT_MTD.1.1/ADDCODE_ACT			×	✓	✓	✓
FMT_MTD.1.1/AA_KEY_GEN			×	✓	✓	✓
FMT_MTD.1.1/CA_KEY_GEN			×	✓	✓	✓
FMT_MTD.1.1/BAC_EXP			×	✓	✓	✓
FMT_MTD.1.1/DES_SM_EXP			×	✓	✓	✓
FMT_MTD.1.1/UPD_FILE			×	✓	✓	✓
FMT_MTD.1.1/SM_LVL			×	×	✓	×
FMT_MTD.1.1/DBI			×	✓	✓	✓
FMT_MTD.3.1	FMT_MTD.3.1	7.1.5.7	×	×	×	✓
FPT_EMS.1.1	FPT_EMS.1.1	7.1.6.1	×	✓	✓	✓
FPT_EMS.1.2	FPT_EMS.1.2		×	✓	✓	✓
FPT_FLS.1.1	FPT_FLS.1.1	7.1.6.2	×	✓	✓	✓
FPT_TST.1.1	FPT_TST.1.1	7.1.6.3	×	✓	✓	✓
FPT_TST.1.2	FPT_TST.1.2		×	✓	✓	✓
FPT_TST.1.3	FPT_TST.1.3		×	✓	✓	✓
FPT_PHP.3.1	FPT_PHP.3.1	7.1.6.4	×	✓	✓	✓
FTP_ITC.1.1/MP	Additional SFR	7.1.7.1	×	✓	✓	×
FTP_ITC.1.2/MP			×	✓	✓	×
FTP_ITC.1.3/MP			×	✓	✓	×

Table 16 – SFR of the TOE

7.1.1 Class FAU *"Security Audit"*

7.1.1.1 FAU_SAS.1 *"Audit Storage"*

Hierarchical to: No other components.

Dependencies: No dependencies

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

7.1.2 Class FCS *"Cryptographic Support"*

7.1.2.1 FCS_CKM.1 *"Cryptographic key generation"*

Hierarchical to: No other components.

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

FCS_CKM.1.1/ CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Algorithm]** and specified cryptographic key sizes **[Key size(s)]** that meet the following: **[Standard].**

Algorithm	Key size(s)	Standard

DH compliant to PKCS#3	**1024 to 2048 bit by steps of 256 bits**	**[TR_03110]**
ECDH compliant to [ISO_15946]	**192 to 521 bit**	

FCS_CKM.1.1/ MSK_DIV — The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **MSK derivation from initial MSK, using SHA-256** and specified cryptographic key sizes **256 bit** that meet the following: **none.**

Application note: In Step 5, (Master) MSK is diversified during the first command, and then replaced by the derived MSK generated by FCS_CKM.1/MSK. The secure erasing of the keys is ensured by FCS_CKM.4.

FCS_CKM.1.1/ GP — The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Algorithm]** and specified cryptographic key sizes **[Key size(s)]** that meet the following: **[Standard].**

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

FCS_CKM.1.1/ LSK_DIV — The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **LSK derivation from Initial LSK and Derivation Data, using AES 128 ECB** and specified cryptographic key sizes **128 bit** that meet the following: **None.**

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

Algorithm	Key size(s)	Standard
RSA key generation	**1024 to 2048 in steps of 256 bits**	**[GPC_SPE_034]; appendix E.4.1**
Key pair over Elliptic curve	**192 to 521 bit with prime field p**	

7.1.2.2 FCS_CKM.4 *"Cryptographic key destruction"*

Hierarchical to: No other components.

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

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

Application note: This SFR addresses the destruction of the MSK, ISK, and SM sessions keys.

7.1.2.3 FCS_COP.1 *"Cryptographic operation"*

Hierarchical to: No other components.

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

FCS_COP.1.1/ CA_SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1 and SHA-256** and cryptographic key sizes **none** that meets the following **[FIPS_180_2].**

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

Algorithm	Key size(s)	Standard
Triple-DES in CBC mode	**112 bit**	**[TR_03110]**
AES in CBC mode	**128, 192 and 256 bit**	

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

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

FCS_COP.1.1/ SIG_VER The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following **[FIPS_186_3]**.

Algorithm	Key size(s)	Standard
RSA CRT with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	**1024 to 2048 bit by steps of 256 bits**	**[FIPS_186_3]**
ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	**192 to 521 bit**	**[FIPS_186_3]**

FCS_COP.1.1/ MSK_SHA

The TSF shall perform **hashing for MSK diversification** in accordance with a specified cryptographic algorithm **SHA-256** and cryptographic key sizes **none** that meets the following **[FIPS_180_2].**

FCS_COP.1.1/ GP_ENC

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

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

FCS_COP.1.1/ GP_AUTH

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

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

FCS_COP.1.1/ GP_MAC

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

Algorithm	Key size(s)	Standard
MAC Algorithm 1 with Padding M2	**112 bit**	**[ISO_9797_1]**
AES CMAC	**128, 192 and 256 bit**	**[NIST_800_38B]**

FCS_COP.1.1/ GP_SDT_DEC

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

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

FCS_COP.1.1/ ADDCODE_DEC — The TSF shall perform **secure messaging – decryption** in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **128 bit** that meets the following **[FIPS_197]**

FCS_COP.1.1/ ADDCODE_MAC — The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **AES CMAC** and cryptographic key sizes **128 bit** that meets the following **[NIST_800_38B].**

FCS_COP.1.1/ ADDCODE_SHA — The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-256** and cryptographic key sizes **none** that meets the following **[FIPS_180_2].**

FCS_COP.1.1/ SIG_GEN — The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meet the following **[Standard].**

Algorithm	Key size(s)	Standard
RSA CRT with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	**1024 to 2048 bit by steps of 256 bits**	**[ISO_9796_2]**
ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	**192 to 521 bit**	**[TR_03111]**

7.1.2.4 FCS_RND.1 *"Quality metric for random numbers"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet:

1. The requirement for random number generation following [ANSSI-PG-083].

7.1.3 Class FIA *"Identification and Authentication"*

7.1.3.1 FIA_UID.1 *"Timing of identification"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to establish the communication channel,
2. to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS
3. 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.

7.1.3.2 FIA_UAU.1 *"Timing of authentication"*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification .

FIA_UAU.1.1 The TSF shall allow

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

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

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

7.1.3.3 FIA_UAU.4 *"Single-use authentication mechanisms"*

Hierarchical to: No other components

Dependencies: No dependencies.

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

1. Terminal Authentication Protocol,
2. Authentication Mechanisms based on:
- **Triple-DES,**
- **AES**

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

7.1.3.4 FIA_UAU.5 *"Multiple authentication mechanisms"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/ EAC The TSF shall provide

1. Terminal Authentication Protocol,
2. Secure messaging in MAC-ENC mode,

3. Symmetric Authentication Mechanisms based on:
- **Triple-DES,**
- **AES**

to support user authentication.

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

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

FIA_UAU.5.1/ MP — The TSF shall provide

1. Authentication Mechanism based on:
- **Triple-DES,**
- **AES.**

to support user authentication.

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

1. The TOE accepts the authentication attempt as Manufacturer by the Symmetric Authentication Mechanism with Pre-personalization Agent Key.

7.1.3.5 FIA_UAU.6 *"Re-authenticating"*

Hierarchical to: No other components.

Dependencies: No dependencies.

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.6.1/ 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.**
Application note	This requirement applies to the authentication protocol used by (1) the Manufacturer and (2) the Personalization Agent
FIA_UAU.6.1/ ADD_CODE	The TSF shall re-authenticate the user under the conditions **each command sent to the TOE shall be verified as being prepared by the TOE Developer.**
Application note	This requirement applies to the Additional Code loading

7.1.3.6 FIA_AFL.1 *"Authentication failure handling"*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1/ MP	The TSF shall detect when **3** 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 or surpassed**, the TSF shall **wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the Authentication Mechanisms (based on Triple-DES or AES) attempts.**

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/ CA	The TSF shall provide a **Chip Authentication protocol according to [TR_03110]** to prove the identity of the **TOE**.
FIA_API.1.1/ AA	The TSF shall provide an **Active Authentication protocol according to [ICAO_9303]** to prove the identity of the **TOE**.

7.1.4 Class FDP *"User Data Protection"*

7.1.4.1 FDP_ACC.1 *"Subset access control"*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ EAC: 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_ACC.1.1/ MP: The TSF shall enforce the **GP Access Control SFP** on **terminals gaining write, read and modification access to the CPLC, the Pre-Perso_K, the Perso_K, the LCS, the Configuration Data, the Additional Code, the Active Authentication Keys (AA_PK and AA_SK) and the Chip Authentication Keys (CA_PK and CA_SK).**

FDP_ACC.1.1/ ID: The TSF shall enforce the **ID Access Control** on **terminals gaining write, read and modification access to the CPLC and the TOE_ID.**

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.**

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

Hierarchical to: No other components.

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

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

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

2. Objects:
- **a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,**
- **b. data EF.DG3 and EF.DG4 of the logical MRTD**
- **c. data in EF.COM,**
- **d. data in EF.SOD,**

3. Security attributes
- **a. authentication status of terminals,**
- **b. Terminal Authorization.**

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

1. the successfully authenticated Personalization Agent is allowed to write and read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative

certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD.
3. the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD
4. Moreover, the successfully authenticated Inspection System shall communicate with the TOE using a secure messaging level at least equal to the one defined at the creation of the DG 3 and DG 4.

Application Note: Possible secure messaging levels are: DES, AES 128, AES 192 or AES 256.

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

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

1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,
5. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
6. Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD.

FDP_ACF.1.1/ MP — The TSF shall enforce the **GP Access Control SFP** to objects based on the following

1. Subjects:
a. Manufacturer,
b. Personalization Agent,
2. Objects:
a. the Pre-Perso_K,
b. the Perso_K,
c. the LCS,
d the Configuration Data,
e the Additional Code,
f. the Active Authentication Private Key,
g. the Active Authentication Public Key,
h. the Chip Authentication Private Key,
i. the Chip Authentication Public Key.
3. Security attributes
a. authentication status of the Manufacturer,
b. authentication status of the Personalization Agent.

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

1. the Manufacturer is allowed to write the Pre-Perso_K, the Perso_K, the LCS and the Configuration Data,

2. **the Manufacturer is allowed to read the Configuration Data and the LCS,**
3. **the Personalization Agent is allowed to write the Perso_K, the LCS and the Configuration Data,**
4. **the Personalization Agent is allowed to read the Configuration Data and the LCS,**
5. **the Manufacturer is allowed to load and activate the Additional Code,**
6. **the Personalization Agent is allowed to import the Active Authentication Private Key,**
7. **the Personalization Agent is allowed to generate the Active Authentication Private Key and the Active Authentication Public Key**
8. **the Personalization Agent is allowed to import the Chip Authentication Private Key,**
9. **the Personalization Agent is allowed to generate the Chip Authentication Private Key and the Chip Authentication Public Key.**

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

FDP_ACF.1.4/ MP — The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

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

1. **Subjects:**
   a. **Manufacturer,**
   b. **Personalization Agent,**
   c. **Extended Inspection System,**
   d. **Terminal,**
2. **Objects:**
   a. **the TOE_ID,**
   b. **the CPLC,**
3. **Security attributes**
   a. **authentication status of the Manufacturer,**
   b. **authentication status of the Personalization Agent,**
   c. **authentication status of the Basic Inspection System.**

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

1. **the Manufacturer is allowed to write and read the CPLC,**
2. **the Personalization Agent is allowed to write and read the CPLC,**
3. **the Extended Inspection System is allowed to read the CPLC,**

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

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

1. **Any Terminal is not allowed to read the CPLC and the TOE_ID,**
2. **Any Terminal is not allowed to modify the CPLC.**

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

1. Subjects:
a. Personalization Agent,
b. Extended Inspection System,
c. Terminal,
2. Objects:
a. data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD
3. Security attributes
a. 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:

1. 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,
2. 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:

1. 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.

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

Hierarchical to: No other components.

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

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

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

Application Note: Additional SFR FDP_UCT.1/MP enforces confidentiality of data import and export in steps 5 and 6.

FDP_UCT.1.1/ ADD_CODE — The TSF shall enforce the **GP Access Control SFP** to **receive** user data in a manner protected from unauthorised disclosure.

Application Note: Additional SFR FDP_UCT.1/ADD_CODE enforces confidentiality of data import in step 5.

7.1.4.4 FDP_UIT.1 *"Data exchange integrity"*

Hierarchical to: No other components.

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

FDP_UIT.1.1/ EAC: 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 protocol**

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

FDP_UIT.1.1/ MP: The TSF shall enforce the **GP Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay errors.**

FDP_UIT.1.2/ MP: The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred**.**

Application Note: Additional SFR FDP_UIT.1/MP enforces integrity of data import and export in steps 5 and 6.

FDP_UIT.1.1/ ADD_CODE: The TSF shall enforce the **GP Access Control SFP** to **receive** user data in a manner protected from **modification, deletion, insertion and replay errors.**

FDP_UIT.1.2/ ADD_CODE: The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred**.**

Application Note: Additional SFR FDP_UIT.1/ADD_CODE enforces integrity of data import in step 5.

7.1.4.5 FDP_ITC.1 *"Import of user data without security attributes"*

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1/ MP: The TSF shall enforce the **GP Access Control SFP** when importing user data, controlled under the SFP, from outside the TOE.

FDP_ITC.1.2/ MP: The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/ MP: The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **sensitive data (Pre-Perso_K, Perso_K, BAC_K, CA_SK and AA_SK) shall be encrypted.**

Application Note: Additional SFR FDP_ITC.1/MP enforces confidentiality of sensitive data import in steps 5 and 6.

7.1.5 Class FMT *"Security Management"*

7.1.5.1 FMT_MOF *"Management of functions in TSF"*

Hierarchical to: No other components.

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

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

- **Active Authentication,**
- **Chip Authentication v1 through MSE: SET KAT**

to **the Manufacturer**.

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_MOF.1.1/ BAC_EXP: The TSF shall restrict the ability to **enable** the functions

- **deactivation of the BAC protocol**

to **Country Verifying Certification Authority and Domestic document Verifier once the current date has reached or passed the value set by FMT_MTD.1/BAC_EXP**

Application Note: The BAC is automatically deactivated by the TOE once the authenticated subject (Country Verifying Certification Authority or domestic Document Verifier) has updated the current date of the TOE with a date that reaches or passes the reference date configured by FMT_MTD.1/BAC_EXP

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

- **deactivation of secure channel algorithms based on DES**

to **Country Verifying Certification Authority and Domestic document Verifier once the current date has reached or passed the value set by FMT_MTD.1/DES_SM_EXP**

Application Note: Secure channel algorithms based on DES are automatically deactivated by the TOE once the authenticated subject (Country Verifying Certification Authority or domestic Document Verifier) has updated the current date of the TOE with a date that reaches or passes the reference date configured by FMT_MTD.1/DES_SM_EXP

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

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

1. **Initialization**
2. **Pre-personalization**
3. **Personalization**
4. **Active Authentication protocol,**
5. **Protection of incoming user data,**
6. **Protection of outgoing user data**
7. **Basic Access Control expiration**

7.1.5.3 FMT_SMR.1 *"Security roles"*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles:

1. **Manufacturer**
2. **Personalization Agent**
3. **Country Verifying Certification Authority,**
4. **Document Verifier,**
5. **domestic Extended Inspection System**
6. **foreign Extended Inspection System**

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

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

7.1.5.4 FMT_LIM.1 *"Limited capabilities"*

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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

Deploying Test Features after TOE Delivery does not allow

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

7.1.5.5 FMT_LIM.2 *"Limited availability"*

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

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

Deploying Test Features after TOE Delivery does not allow
1. **User Data to be disclosed or manipulated,**
2. **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,**
3. **TSF data to be disclosed or manipulated,**
4. **software to be reconstructed and,**
5. **substantial information about construction of TSF to be gathered which may enable other attacks**.

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

Hierarchical to: No other components.

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

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

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

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

1. **initial Country Verifying Certification Authority Public Key,**
2. **initial Country Verifying Certification Authority Certificate,**
3. **initial Current Date**

to **the Personalization Agent.**

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

1. **Country Verifying Certification Authority Public Key,**
2. **Country Verifying Certification Authority Certificate,**

to **Country Verifying Certification Authority.**

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

1. **Country Verifying Certification Authority,**
2. **Document Verifier**
3. **domestic Extended Inspection System.**

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

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

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to **read** the **1. Document Basic Access Keys,** **2. Chip Authentication Private Key,** **3. Personalization Agent Keys** to **none**
FMT_MTD.1.1/ MP_KEY_WRITE	The TSF shall restrict the ability to **write** the **Pre-personalization Agent Keys and the Personalization Agent Keys** to **the Manufacturer.**
FMT_MTD.1.1/ MP_KEY_READ	The TSF shall restrict the ability to **read** the **Pre-personalization Agent Keys and the Personalization Agent Keys** to **none.**
FMT_MTD.1.1/ AA_KEY_WRITE	The TSF shall restrict the ability to **write** the **Active Authentication Keys** to **the Personalization Agent.**
FMT_MTD.1.1/ AA_KEY_READ	The TSF shall restrict the ability to **read** the **Active Authentication Keys** to **none.**
FMT_MTD.1.1/ LCS_PREP	The TSF shall restrict the ability **to switch** the **LCS from phase 5 to phase 6** to **the Manufacturer.**
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.1.1/ LSK_READ	The TSF shall restrict the ability to **read** the **Load Secure Key** to **none.**
FMT_MTD.1.1/ ADDCODE_LOAD	The TSF shall restrict the ability to **write** the **Additional Code** to **the Manufacturer.**
FMT_MTD.1.1/ ADDCODE_ACT	The TSF shall restrict the ability to **activate** the **Additional Code** to **the Manufacturer.**
FMT_MTD.1.1/ AA_KEY_GEN	The TSF shall restrict the ability to **generate** the **Active Authentication Keys (AA_PK and AA_SK)** to **the Personalization Agent.**
FMT_MTD.1.1/ CA_KEY_GEN	The TSF shall restrict the ability to **generate** the **Chip Authentication Keys (CA_PK and CA_SK)** to **the Personalization Agent.**
FMT_MTD.1.1/ BAC_EXP	The TSF shall restrict the ability **to set** the **BAC expiry date** to **the Personalization Agent.**
Application note:	By default, BAC expiration feature is not activated.
FMT_MTD.1.1/ DES_SM_EXP	The TSF shall restrict the ability **to set** the **DES secure messaging expiry date** to **the Personalization Agent.**
Application note:	By default, DES secure messaging expiration is not activated.
FMT_MTD.1.1/ UPD_FILE	The TSF shall restrict the ability **to set** the **name (or beginning of the name) of the terminal allowed to modify files in phase 7, and identifiers of these files (different from EF.COM, EF.SOD, EF.DG1 to EF.DG16)** to **the Personalization Agent.**

Application note:	Name of the terminal is the Card Holder Reference (CHR) of the EIS. Beginning of the name is a string of the left most significant bytes of the CHR of the EIS.
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.**
Application Note:	Possible secure messaging levels are: DES, AES 128, AES 192 or AES 256.
FMT_MTD.1.1/ DBI	The TSF shall restrict the ability **to set** the **name (or beginning of the name) of the terminal allowed to remove the watermarking on files in phase 7, and identifiers of these files** to **the Personalization Agent.**
Application note:	Name of the terminal is the Card Holder Reference (CHR) of the EIS. Beginning of the name is a string of the left most significant bytes of the CHR of the EIS.

7.1.5.7 FMT_MTD.3 *"Secure TSF data"*

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

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

Refinement: The certificate chain is valid if and only if

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

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

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

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

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

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

7.1.6.1 FPT_EMS.1 *"TOE Emanation"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMS.1.1 The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to **Personalization Agent Key(s) and Chip Authentication Private Key** and:

- **Personal Data including Biometric Data,**
- **EF.COM,**
- **EF.SOD,**
- **Active Authentication Private Key,**
- **Active Authentication Public Key,**
- **CPLC,**
- **TOE_ID,**
- **Pre-personalization Agent Keys,**
- **Secure Messaging Session Keys,**
- **TOE Life Cycle State,**
- **Configuration Data,**
- **Updatable Data.**

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

- **Personal Data including Biometric Data,**
- **EF.COM,**
- **EF.SOD,**
- **Active Authentication Private Key,**
- **Active Authentication Public Key,**
- **CPLC,**
- **TOE_ID,**
- **Pre-personalization Agent Keys,**
- **Secure Messaging Session Keys,**
- **TOE Life Cycle State,**
- **Configuration Data,**
- **Updatable Data.**

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

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

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

7.1.6.3 FPT_TST.1 *"TSF testing"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

- **At reset,**
- **Before any cryptographic operation,**
- **When accessing a DG or any EF,**
- **Prior to any use of TSF data,**
- **Before execution of any command,**
- **When performing the EAC Authentication,**
- **When performing the Active Authentication.**

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**.

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

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

7.1.7 Class FTP "Trusted path/channels"

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

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

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

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

7.2 Security assurance requirements

The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 5 (EAL5) and augmented by taking the following component: ALC_DVS.2 and AVA_VAN.5.

7.2.1 EAL rationale

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.

7.2.2 EAL augmentation rationale

7.2.2.1 ALC_DVS.2 "Sufficiency of security measures"

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

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

7.2.2.2 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

7.2.3 Dependencies

SAR	Dependencies	Support of the Dependencies
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	ADV_FSP.5 ADV_TDS.4
ADV_FSP.5	ADV_TDS.1 ADV_IMP.1	ADV_TDS.4 ADV_IMP.1
ADV_IMP.1	ADV_TDS.3 ALC_TAT.1	ADV_TDS.4 ALC_TAT.2
ADV_INT.2	ADV_IMP.1 ADV_TDS.3 ALC_TAT.1	ADV_IMP.1 ADV_TDS.4 ALC_TAT.2
ADV_TDS.4	ADV_FSP.5	ADV_FSP.5

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

Table 17 - SARs dependencies

7.3 Security requirements rationale

7.3.1 Security Functional Requirements Rationale

7.3.1.1 Overview

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

SFR \ SO	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Configuration	OT.Update_File	OT.BAC_Expiration	OT.AC_SM_Level	OT.Secure_Load_ACode	OT.Secure_AC_Activation	OT.TOE_Identification	OT.DES_SM_Expiration
FAU_SAS.1				X													
FCS_CKM.1/CA	X	X	X		X												
FCS_CKM.1/MSK_DIV										X							
FCS_CKM.1/GP										X							
FCS_CKM.1/LSK_DIV										X				X	X		
FCS_CKM.1/KEY_GEN	X																
FCS_CKM.4	X	X	X														
FCS_COP.1/MSK_SHA	X	X	X							X							
FCS_COP.1/CA_SHA	X	X	X		X												
FCS_COP.1/CA_ENC	X	X	X		X												
FCS_COP.1/CA_MAC	X	X	X		X												
FCS_COP.1/SIG_VER	X		X														
FCS_COP.1/GP_ENC	X	X	X							X							
FCS_COP.1/GP_AUTH										X							
FCS_COP.1/GP_MAC	X	X	X							X							
FCS_COP.1/GP_SDT_DEC			X							X							
FCS_COP.1/ADDCODE_DEC										X				X			
FCS_COP.1/ADDCODE_MAC										X				X	X		
FCS_COP.1/ADDCODE_SHA										X					X		
FCS_COP.1/SIG_GEN					X												
FCS_RND.1	X		X														
FIA_UID.1	X	X	X														
FIA_UAU.1	X	X	X														
FIA_UAU.4	X	X	X														
FIA_UAU.5/EAC	X	X	X														
FIA_UAU.5/MP										X							
FIA_UAU.6/EAC	X	X	X														
FIA_UAU.6/MP	X	X	X							X							
FIA_UAU.6/ADD_CODE										X				X	X		
FIA_AFL.1/MP	X									X							
FIA_API.1/CA					X												
FIA_API.1/AA					X												
FDP_ACC.1/EAC	X	X	X														
FDP_ACC.1/MP										X							
FDP_ACC.1/ID	X			X						X							
FDP_ACC.1/UPD_FILE	X	X	X								X						
FDP_ACF.1/EAC	X	X	X														

SFR \ SO	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Configuration	OT.Update_File	OT.BAC_Expiration	OT.AC_SM_Level	OT.Secure_Load_ACode	OT.Secure_AC_Activation	OT.TOE_Identification	OT.DES_SM_Expiration
FDP_ACF.1/MP										X							
FDP_ACF.1/ID	X			X													
FDP_ACF.1/UPD_FILE	X	X	X								X						
FDP_UCT.1/EAC			X														
FDP_UCT.1/MP	X	X	X							X							
FDP_UCT.1/ADD_CODE										X				X	X		
FDP_UIT.1/EAC		X	X														
FDP_UIT.1/MP	X	X	X							X							
FDP_UIT.1/ADD_CODE										X				X	X		
FDP_ITC.1/MP			x							x							
FMT_MOF.1/PROT					x					x							
FMT_MOF.1/GP		x	x		x												
FMT_MOF.1/BAC_EXP												x					
FMT_MOF.1/DES_SM_EXP																	x
FMT_SMF.1	X	x										x					
FMT_SMR.1	X	x															
FMT_LIM.1						x											
FMT_LIM.2						x											
FMT_MTD.1/INI_ENA				x													
FMT_MTD.1/INI_DIS				x													
FMT_MTD.1/CVCA_INI			x														
FMT_MTD.1/CVCA_UPD			x														
FMT_MTD.1/DATE			x														
FMT_MTD.1/KEY_WRITE	X																
FMT_MTD.1/CAPK		x	x		x												
FMT_MTD.1/KEY_READ	X	x	x		x												
FMT_MTD.1/MP_KEY_WRITE		x	x							x							
FMT_MTD.1/MP_KEY_READ		x	x							x							
FMT_MTD.1/AA_KEY_WRITE	X				x												
FMT_MTD.1/AA_KEY_READ	X				x												
FMT_MTD.1/LCS_PREP	X									X							
FMT_MTD.1/LCS_PERS	X																
FMT_MTD.1/LSK_READ														X	X		
FMT_MTD.1/ADDCODE_LOAD														X	X		
FMT_MTD.1/ADDCODE_ACT														X		X	
FMT_MTD.1/AA_KEY_GEN	X																
FMT_MTD.1/CA_KEY_GEN	X																
FMT_MTD.1/BAC_EXP												x					
FMT_MTD.1/DES_SM_EXP																	x
FMT_MTD.1/UPD_FILE											x						
FMT_MTD.1/SM_LVL													x				
FMT_MTD.1/DBI										X							
FMT_MTD.3			x														
FPT_EMS.1	X						x										
FPT_FLS.1							x		x								

SFR \ SO	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Configuration	OT.Update_File	OT.BAC_Expiration	OT.AC_SM_Level	OT.Secure_Load_ACode	OT.Secure_AC_Activation	OT.TOE_Identification	OT.DES_SM_Expiration
FPT_TST.1							x		x								
FPT_PHP.3							x	x									
FTP_ITC.1/MP										x							

Table 18 - SFRs and Security Objectives

7.3.1.2 OT.AC_Pers

The security objective **OT.AC_Pers** *"Access Control for Personalization of logical MRTD"* addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR **FIA_UID.1**, **FIA_UAU.1**, **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. 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**, **FCS_COP.1/CA_SHA** (for the derivation of the new session keys after Chip Authentication), and **FCS_COP.1/CA_ENC** 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/CA_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 and **FDP_UCT.1/MP** and **FDP_UIT.1/MP** 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 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.

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

SFR **FDP_ACC.1/ID** and **FDP_ACF.1/ID** define rules to access TOE_ID and CPLC which allow the TOE identification.

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**.

Only the Personalization Agent is allowed to generate Chip Authentication Key pair and Active Authentication Key pair according to respectively ***FMT_MTD.1/CA_KEY_GEN*** and ***FMT_MTD.1/AA_KEY_GEN,*** following rules define in ***FDP_ACC.1/MP*** and ***FDP_ACF.1/MP.*** The generation of these key pairs is ensured by ***FCS_CKM.1/KEY_GEN***.

The Personalization Agent can set the name (or beginning of the name) of the terminal allowed to remove the watermarking on files in phase 7, according to ***FMT_MTD.1/DBI.***

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

7.3.1.3 OT.Data_Int

The security objective **OT.Data_Int** *"Integrity of personal data"* requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the 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** and **FIA_UAU.1** 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** (for the generation of shared secret), **FCS_COP.1/CA_SHA** (for the derivation of the new session keys), and **FCS_COP.1/CA_ENC** and **FCS_COP.1/CA_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***, ***FDP_UCT.1/MP*** and ***FDP_UIT.1/MP*** 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. The SFR

FMT_MTD.1/MP_KEY_WRITE requires the Manufacturer to establish the Symmetric Authentication Private Key in a way that it cannot be read by anyone in accordance to ***FMT_MTD.1/MP_KEY_READ***. ***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**.

7.3.1.4 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** (for the generation of shared secret), **FCS_COP.1/SHA** (for the derivation of the new session keys), and **FCS_COP.1/CA_ENC** and **FCS_COP.1/CA_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.Data_Conf.

Manufacturer and Personalization Agent are also able to detect any modification of the transmitted logical MRTD data by means of the Symmetric Authentication mechanism. The SFR ***FIA_UAU.6/MP***, ***FDP_UCT.1/MP*** and ***FDP_UIT.1/MP*** 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. The SFR ***FMT_MTD.1/MP_KEY_WRITE*** requires the Manufacturer to establish the Symmetric Authentication Private Key in a way that it cannot be read by anyone in accordance to ***FMT_MTD.1/MP_KEY_READ***. ***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**.

7.3.1.5 OT.Identification

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

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"*.

SFR FDP_ACF.1/ID and ***FDP_ACC.1/ID*** define rules to read and write TOE_ID and CPLC which allow the TOE identification.

7.3.1.6 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 Protocol [TR_03110] requires additional TSF according to **FCS_COP.1/CA_SHA** (for the derivation of the session keys), **FCS_COP.1/CA_ENC** and **FCS_COP.1/CA_MAC** (for the ENC_MAC_Mode secure messaging).

7.3.1.7 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.

7.3.1.8 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**.

7.3.1.9 OT.Prot_Phys-Tamper

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

7.3.1.10 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.

7.3.1.11 OT.Configuration

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

The Manufacturer Secret Key (MSK) loaded by Embedded software loading responsible (scheme 2 and scheme 3) or IC manufacturer (scheme 1) is diversified at first command according to SFR **FCS_CKM.1/MSK_DIV** and **FCS_CKM.1/MSK_SHA**. This secures the transport of the chip between IC manufacturing centre and MRTD manufacturing centre.

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

Once step 4 is done, the MRTD packaging responsible is allowed to set the Pre-personalization Agent keys according to the SFR **FMT_MTD.1/MP_KEY_WRITE, FDP_ITC.1/MP** and **FCS_COP.1/GP_SDT_DEC**. The SFR **FMT_MTD.1/MP_KEY_READ** prevents read access to the Pre-personalization keys and ensure together with the SFR **FPT_EMS.1**, **FPT_FLS.1** and **FPT_PHP.3** the confidentially of these keys. This operation destroys the MSK (**FCS_CKM.4**).

The write access to these data is defined by the SFR **FDP_ACC.1/MP** and **FDP_ACF.1/MP** as follows: only the successfully authenticated Pre-personalization Agent and Personalization Agent are allowed to write these data.

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/MP**. The Manufacturer shall be authenticated by using the symmetric authentication mechanism (**FCS_COP.1/GP_AUTH**).

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

The SFR **FIA_UAU.6/MP** describes the re-authentication and **FDP_UCT.1/MP** and **FDP_UIT.1/MP** 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 Manufacturer is also able to detect any modification of the transmitted logical Additional Code data by means of the Symmetric Authentication mechanism. The SFR ***FIA_UAU.6/ADD_CODE***, ***FDP_UCT.1/ADD_CODE*** and ***FDP_UIT.1/ADD_CODE*** requires the protection of the received data by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/LSK_DIV***, and ***FCS_COP.1/ADDCODE_DEC*** and ***FCS_COP.1/ ADDCODE_MAC*** for the ENC_MAC_Mode. The LSK used as a seed for DIV_LSK cannot be read by anyone in accordance to ***FMT_MTD.1/LSK_READ***. ***FCS_CKM.4*** enforces the destruction of Secure Messaging session keys. ***FCS_CKM.4*** also enforces the destruction of the LSK once the TOE is in Step 6.

The Manufacturer is the only one who can load and activate Additional Codes according to SFR ***FMT_MTD.1.1/ADDCODE_LOAD*** and ***FMT_MTD.1.1/ADDCODE_ACT.*** The Additional Code activation is enforced by the cryptographic function ***FCS_COP.1/ADDCODE_SHA.***

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

The Manufacturer and the Personalization Agent can select the protection mode of user data following **FMT_MOF.1.1/GP**.

The Manufacturer can enable the BAC deactivation according to **FMT_MTD.1/BAC_EXP**. In operational use phase Country Verifying Certification Authority and Domestic document Verifier can then deactivate BAC according to **FMT_MOF.1/BAC_EXP**.

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 according to the SFR **FMT_MTD.1/MP_KEY_WRITE** as authentication reference data. The SFR **FMT_MTD.1/MP_KEY_READ** prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR **FCS_CKM.4**, **FPT_EMS.1**, **FPT_FLS.1** and **FPT_PHP.3** the confidentially of these keys.

SFR **FDP_ACF.1/ID** and **FDP_ACC.1/ID** define rules to access TOE_ID and CPLC which allow the TOE identification.

The Manufacturer is the only subject allowed to ends Pre-personalization of logical MRTD, setting the TOE Life Cycle State in Personalization state according to **FMT_MTD.1.1/LCS_PREP**. 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.

7.3.1.12 OT.Secure_Load_ACode

The security objective **OT.Secure_Load_ACode** *"Secure loading of the Additional Code"* addresses the loading of the Additional Code.

The Manufacturer is also able to detect any modification of the transmitted logical Additional Code data by means of the Symmetric Authentication mechanism. The SFR ***FIA_UAU.6/ADD_CODE***, ***FDP_UCT.1/ADD_CODE*** and ***FDP_UIT.1/ADD_CODE*** requires the protection of the received data by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/LSK_DIV***, and ***FCS_COP.1/ADDCODE_DEC*** and ***FCS_COP.1/ ADDCODE_MAC*** for the ENC_MAC_Mode. The LSK used as a seed for DIV_LSK cannot be read by anyone in accordance to ***FMT_MTD.1/LSK_READ***. ***FCS_CKM.4*** enforces the destruction of Secure Messaging session keys. ***FCS_CKM.4*** also enforces the destruction of the LSK once the TOE is in Step 6.

The Manufacturer is the only one who can load and activate Additional Codes according to SFR ***FMT_MTD.1.1/ADDCODE_LOAD*** and ***FMT_MTD.1.1/ADDCODE_ACT.*** The Additional Code activation is enforced by the cryptographic function ***FCS_COP.1/ADDCODE_SHA.***

7.3.1.13 OT.Secure_AC_Activation

The security objective **OT.Secure_AC_Activation** *"Secure activation of the Additional Code"* addresses the activation of the Additional Code.

The Manufacturer is also able to detect any modification of the transmitted logical Additional Code data by means of the Symmetric Authentication mechanism. The SFR ***FIA_UAU.6/ADD_CODE***, ***FDP_UCT.1/ADD_CODE*** and ***FDP_UIT.1/ADD_CODE*** requires the protection of the received data by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/LSK_DIV***, and ***FCS_COP.1/ADDCODE_DEC*** and ***FCS_COP.1/ ADDCODE_MAC*** for the ENC_MAC_Mode. The LSK used as a seed for DIV_LSK cannot be read by anyone in accordance to ***FMT_MTD.1/LSK_READ***. ***FCS_CKM.4*** enforces the destruction of Secure Messaging session keys. ***FCS_CKM.4*** also enforces the destruction of the LSK once the TOE is in Step 6.

The Manufacturer is the only one who can load and activate Additional Codes according to SFR ***FMT_MTD.1.1/ADDCODE_LOAD*** and ***FMT_MTD.1.1/ADDCODE_ACT.*** The Additional Code activation is enforced by the cryptographic function ***FCS_COP.1/ADDCODE_SHA.***

7.3.1.14 OT.TOE_Identification

The security objective **OT.TOE_Identification** "Secure identification 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***.

SFR FDP_ACF.1/ID and ***FDP_ACC.1/ID*** define rules to read and write TOE_ID and CPLC which allow the TOE identification.

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

7.3.1.15 OT.DES_SM_Expiration

SFRs FMT_MOF.1/DES_SM_EXP and FMT_MTD.1/DES_SM_EXP cover the security objective **OT.DES_SM_Expiration** *"*Automatic deactivation of DES-based secure messaging*"*. FMT_MOF.1/DES_SM_EXP permits to the Country Verifying Certification Authority and Domestic Document Verifier to proceed with the deactivation of the function when it expires whereas FMT_MTD.1/DES_SM_EXP restricts the ability to set the expiry date of the function to the Personalization Agent.

7.3.2 Dependency Rationale

7.3.2.1 Overview

The Table 19 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1/CA	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC FCS_CKM.4
FCS_CKM.1/MSK_DIV		FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC FCS_CKM.4
FCS_CKM.1/GP		FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC FCS_CKM.4
FCS_CKM.1/LSK_DIV		FCS_COP.1/ ADDCODE_DEC and FCS_COP.1/ ADDCODE_MAC FCS_CKM.4
FCS_CKM.1/KEY_GEN		FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC and FCS_COP.1/SIG_GEN FCS_CKM.4
FCS_CKM.4	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/BAC and FCS_CKM.1/ MSK and FCS_CKM.1/GP and FCS_CKM.1/CA_ECDH
FCS_COP.1/CA_SHA	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	See § 7.3.2.2.1 FCS_CKM.4
FCS_COP.1/CA_ENC		FCS_CKM.1/BAC FCS_CKM.4
FCS_COP.1/CA_MAC		FCS_CKM.1/BAC FCS_CKM.4
FCS_COP.1/SIG_VER		
FCS_COP.1/MSK_SHA		See § 7.3.2.2.1 FCS_CKM.4
FCS_COP.1/GP_ENC		FCS_CKM.1/GP FCS_CKM.4
FCS_COP.1/GP_AUTH		FCS_CKM.1/GP FCS_CKM.4
FCS_COP.1/GP_MAC		FCS_CKM.1/GP FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/GP_SDT_DEC		FCS_CKM.1/GP FCS_CKM.4
FCS_COP.1/ADDCODE_DEC		FCS_CKM.1/LSK_DIV FCS_CKM.4
FCS_COP.1/ADDCODE_MAC		FCS_CKM.1/LSK_DIV FCS_CKM.4
FCS_COP.1/ADDCODE_SHA		FCS_CKM.1/LSK_DIV FCS_CKM.4
FCS_COP.1/SIG_GEN		FDP_ITC.1/MP FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5/EAC	No dependencies	n.a.
FIA_UAU.5/MP		
FIA_UAU.6/EAC	No dependencies	n.a.
FIA_UAU.6/MP		
FIA_UAU.6/ADD_CODE		
FIA_AFL.1/MP	FIA_UAU.1	FIA_UAU.1
FIA_API.1/CA	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1/EAC	FDP_ACF.1	FDP_ACF.1/EAC
FDP_ACC.1/MP		FDP_ACF.1/MP
FDP_ACC.1/ID		FDP_ACF.1/ID
FDP_ACC.1/UPD_FILE		FDP_ACF.1/UPD_FILE
FDP_ACF.1/EAC	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/EAC See § 7.3.2.2.2
FDP_ACF.1/MP		FDP_ACC.1/MP See § 7.3.2.2.3
FDP_ACF.1/ID		FDP_ACC.1/ID See § 7.3.2.2.3
FDP_ACF.1/UPD_FILE		FDP_ACC.1/UPD_FILE See § 7.3.2.2.2
FDP_UCT.1/MP		FTP_ITC.1 FDP_ACC.1/MP
FDP_UCT.1/ADD_CODE		FTP_ITC.1 FDP_ACC.1/MP
FDP_UCT.1/EAC		See § 7.3.2.2.4 FDP_ACC.1/EAC
FDP_UIT.1/MP		FTP_ITC.1 FDP_ACC.1/MP

SFR	Dependencies	Support of the Dependencies
FDP_UIT.1/ADD_CODE		FTP_ITC.1/MP FDP_ACC.1/MP
FDP_UIT.1/EAC		See § 7.3.2.2.4 FDP_ACC.1/EAC
FDP_ITC.1/MP	[FDP_ACC.1, or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/MP See § 7.3.2.2.5
FMT_MOF.1/PROT	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MOF.1/GP		
FMT_MOF.1/BAC_EXP		
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS		
FMT_MTD.1/CVCA_INI		
FMT_MTD.1/CVCA_UPD		
FMT_MTD.1/DATE		
FMT_MTD.1/KEY_WRITE		
FMT_MTD.1/CAPK		
FMT_MTD.1/KEY_READ		
FMT_MTD.1/MP_KEY_WRITE		
FMT_MTD.1/MP_KEY_READ		
FMT_MTD.1/AA_KEY_WRITE		
FMT_MTD.1/AA_KEY_READ		
FMT_MTD.1/LCS_PREP		
FMT_MTD.1/LCS_PERS		
FMT_MTD.1/LSK_READ		
FMT_MTD.1/ADDCODE_LOAD		
FMT_MTD.1/ADDCODE_ACT		
FMT_MTD.1/AA_KEY_GEN		
FMT_MTD.1/CA_KEY_GEN		
FMT_MTD.1/BAC_EXP		
FMT_MTD.1/UPD_FILE		
FMT_MTD.1/SM_LVL		
FMT_MTD.1/DBI		
FMT_MTD.3	FMT_MTD.1	FMT_MTD.1.1/CVCA_INI and FMT_MTD.1.1/CVCA_UPD
FPT_EMS.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FTP_ITC.1/MP	No dependencies	n.a.

Table 19 - Dependencies between the SFR for the TOE

7.3.2.2 Rationale for the exclusion of dependencies

7.3.2.2.1 FCS_COP.1/CA_SHA and FCS_COP.1/MSK_SHA

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

7.3.2.2.2 FDP_ACF.1/EAC and FDP_ACF.1/UPD_FILE

The access control TSF according to **FDP_ACF.1/EAC** and **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.

7.3.2.2.3 FDP_ACF.1/MP and FDP_ACF.1/ID

The access control TSF according to **FDP_ACF.1/MP** and **FDP_ACF.1/ID** uses security attributes which are fixed during the development of the OS 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.

7.3.2.2.4 FDP_UCT.1/EAC and FDP_UIT.1/EAC

The SFR **FDP_UCT.1/EAC** and **FDP_UIT.1/EAC** require 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.

7.3.2.2.5 FDP_ITC.1/MP

The SFR FDP_ITC.1/MP requires the verification of security attributes when Manufacturer and Personalization Agent imports user data. There is no need for FMT_MSA.3, e.g. to initialize these security attributes, as they are fixed during the development of the OS.

8 TOE SUMMARY SPECIFICATION

8.1 TOE summary specification

8.1.1 Overview

The TOE provides the following Security Functions (TSF):

TSF	Acronym	Descr.	Step		
			5	6	7
Access Control in Reading	F.ACR	§ 8.1.2	✓	✓	✓
Access Control in Writing	F.ACW	§ 8.1.3	✓	✓	✓
Active Authentication	F.AA	§ 8.1.4	✓	×	✓
Extended Access Control	F.EAC	§ 8.1.5	×	×	✓
MRTD Personalization	F.PERS	§ 8.1.6	×	✓	×
Physical Protection	F.PHY	§ 8.1.7	✓	✓	✓
MRTD Pre-personalization	F.PREP	§ 8.1.8	✓	×	×
Safe State Management	F.SS	§ 8.1.9	✓	✓	✓
Secure Messaging	F.SM	§ 8.1.10	✓	✓	✓
Self Tests	F.STST	§ 8.1.11	✓	✓	✓

Table 20 - TSF of the TOE

8.1.2 Access Control in Reading

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

- MSK,
- Pre-personalization Agent keys,
- Personalization Agent keys,
- BAC keys,
- AA private key,
- CA private key,
- LSK.

It controls access to the CPLC data as follow:

- It ensures the CPLC data can be read during the personalization phase,
- It ensures it cannot be readable without authentication at the end of the personalization step.

It controls access to the TOE_ID as follow:

- It ensures the TOE_ID data can be read during the manufacturing and personalization phases,
- It ensures it cannot be readable without authentication in operational use phase.

Regarding the file structure:

In the Operational Use phase:

- The terminal can read user data, the Document Security Object, EF.COM only after BAC authentication and through a valid secure channel.

In the Manufacturing and Personalization phases:

- The Manufacturer and the Personalization Agent can read all the data stored in the TOE after it is authenticated by the TOE (using its authentication keys).

It ensures as well that no other part of the memory can be accessed at anytime

8.1.3 Access Control in Writing

This function controls access to write functions (in EEPROM) 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.

It also ensures the CPLC data cannot be written anymore once the TOE is in Operational Use phase.

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.

In the Manufacturing and Personalization phases:

The Manufacturing and Personalization Agent can create and write through a valid secure channel all the data files it needs after it is authenticated by the TOE (using its authentication keys).

8.1.4 Active Authentication

This TSF provides the Active Authentication as described in [ICAO_9303]. It also provides management of this function in phase 5.

8.1.5 Extended Access Control

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

8.1.6 MRTD Personalization

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

- Manage symmetric authentication using Personalization Agent keys,
- Compute session keys to be used by F.SM,
- Load and activate Additional Code,
- Load user data,
- Configure SM level for biometrical data access,
- Load Chip Authentication keys and Active Authentication keys,
- Set Personalization Agent CPLC Data,
- Configure BAC deactivation mechanism
- Set the name of the terminal allowed to modify files in phase 7, and identifiers of these files
- Set TOE life cycle in Operational Use phase.

8.1.7 Physical Protection

This Security Function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data, CPLC data, configuration data and TOE life cycle. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE.

8.1.8 MRTD Pre-personalization

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

- Manage symmetric authentication using Pre-personalization Agent keys,
- Compute session keys to be used by F.SM,
- Load data,
- Create the MRTD application
- Load Personalization Agent keys,
- Load the Pre-personalization Agent CPLC Data,
- ,Set TOE life cycle in Personalization phase.

This security function ensures the destruction of the MSK, once ISK is loaded. This security function ensures the destruction of the ISK, once Personalization Agent keys are loaded.

8.1.9 Safe State Management

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

- an integrity error is detected by F.STST described in § 8.1.11,
- a tearing occurs (during a copy of data in EEPROM).

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

8.1.10 Secure Messaging

This security functionality ensures the confidentiality, authenticity and integrity of the communication between the TOE and the interface device. In the operational phase, after a successful Authentication Procedure (i.e. BAC or CA), a secure channel is established. This security functionality also provides a Secure Messaging (SCP02) for the Pre-personalization and Personalization phases. The protocols can be configured to protect the exchanges integrity and/or confidentiality. If an error occurs in the secure messaging layer, the session keys are destroyed.

8.1.11 Self Tests

The TOE performs self-tests to verify the integrity of the TSF data:

- At Reset,
- Before using the TSF data,
- Before using Chip Authentication key and Active Authentication key.

8.2 SFR and TSF

SFR \ TSF	F.ACR	F.ACW	F.AA	F.EAC	F.PERS	F.PHY	F.PREP	F.SS	F.SM	F.STST
FAU_SAS.1	×	×	×	×	×	✓	×	✓	×	×
FCS_CKM.1/CA	×	×	×	✓	×	×	×	×	×	✓
FCS_CKM.1/MSK_DIV	×	×	×	×	×	×	✓	×	×	✓
FCS_CKM.1/GP	×	×	×	×	✓	×	✓	×	×	✓
FCS_CKM.1/LSK_DIV	×	×	×	×	×	×	✓	×	×	✓
FCS_CKM.1/KEY_GEN	×	×	×	×	✓	×	✓	×	×	✓
FCS_CKM.4	×	×	×	×	✓	×	✓	×	✓	×
FCS_COP.1/CA_SHA	×	×	×	✓	×	×	×	×	×	×
FCS_COP.1/CA_ENC	×	×	×	×	×	×	×	×	✓	✓
FCS_COP.1/CA_MAC	×	×	×	×	×	×	×	×	✓	✓
FCS_COP.1.1/SIG_VER	×	×	×	✓	×	×	×	×	×	✓
FCS_COP.1/MSK_SHA	×	×	×	×	×	×	✓	×	×	×
FCS_COP.1/GP_ENC	×	×	×	×	×	×	×	×	✓	✓
FCS_COP.1/GP_AUTH	×	×	×	×	✓	×	✓	×	×	✓
FCS_COP.1/GP_MAC	×	×	×	×	×	×	×	×	✓	✓
FCS_COP.1/GP_SDT_DEC	×	×	×	×	✓	×	✓	×	×	✓
FCS_COP.1/SIG_GEN	×	×	✓	×	×	×	×	×	×	✓
FCS_COP.1/ADDCODE_DEC	×	×	×	×	×	×	✓	×	×	✓
FCS_COP.1/ADDCODE_MAC	×	×	×	×	×	×	✓	×	×	✓
FCS_COP.1/ADDCODE_SHA	×	×	×	×	×	×	✓	×	×	✓
FCS_RND.1	×	×	✓	✓	✓	×	✓	×	×	✓
FIA_UID.1	✓	✓	×	×	×	×	×	×	×	×
FIA_UAU.1	✓	✓	×	×	×	×	×	×	×	×
FIA_UAU.4	×	×	×	✓	✓	×	✓	×	×	✓
FIA_UAU.5/EAC	×	×	×	✓	✓	×	×	×	✓	✓
FIA_UAU.5/MP	×	×	×	×	×	×	✓	×	×	✓
FIA_UAU.6/EAC	×	×	×	×	×	×	×	×	✓	✓
FIA_UAU.6/MP	×	×	×	×	×	×	×	×	✓	✓
FIA_UAU.6/ADD_CODE	×	×	×	×	×	×	✓	×	×	✓
FIA_AFL.1/MP	×	×	×	×	✓	×	✓	×	×	✓
FIA_API.1/CA	×	×	×	✓	×	×	×	×	×	×
FIA_API.1/AA	×	×	✓	×	×	×	×	×	×	×
FDP_ACC.1/EAC	✓	✓	×	✓	✓	×	×	×	×	×
FDP_ACC.1/MP	✓	✓	×	×	✓	×	✓	×	×	×
FDP_ACC.1/ID	✓	✓	×	✓	✓	×	✓	×	×	×
FDP_ACC.1/UPD_FILE	✓	✓	×	✓	✓	×	×	×	×	×
FDP_ACF.1/EAC	✓	✓	×	✓	✓	×	×	×	×	×
FDP_ACF.1/MP	✓	✓	×	✓	✓	×	✓	×	×	×
FDP_ACF.1/ID	✓	✓	×	✓	✓	×	×	×	×	×
FDP_ACF.1/UPD_FILE	✓	✓	×	✓	✓	×	×	×	×	×
FDP_UCT.1/EAC	×	×	×	×	×	×	×	×	✓	✓
FDP_UCT.1/MP	×	×	×	×	×	×	×	×	✓	✓
FDP_UCT.1/ADD_CODE	×	×	×	×	×	×	✓	×	×	✓
FDP_UIT.1/EAC	×	×	×	×	×	×	×	×	✓	✓
FDP_UIT.1/MP	×	×	×	×	×	×	×	×	✓	✓
FDP_UIT.1/ADD_CODE	×	×	×	×	×	×	✓	×	×	✓
FDP_ITC.1/MP	×	×	×	×	✓	×	✓	×	×	✓

FMT_MOF.1/PROT	×	×	✓	×	×	×	✓	×	×	×
FMT_MOF.1/GP	×	×	×	×	✓	×	✓	×	×	×
FMT_MOF.1/BAC_EXP	×	×	×	✓	×	×	×	×	×	×
FMT_MOF.1/DES_SM_EXP	×	×	×	✓	×	×	×	×	×	×
FMT_SMF.1	×	✓	✓	×	✓	×	✓	×	✓	×
FMT_SMR.1	×	×	×	✓	✓	×	✓	×	×	×
FMT_LIM.1	×	×	×	×	×	✓	×	✓	×	×
FMT_LIM.2	×	×	×	×	×	✓	×	✓	×	×
FMT_MTD.1/INI_ENA	✓	✓	×	×	×	×	✓	×	×	×
FMT_MTD.1/INI_DIS	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1/CVCA_INI	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1/CVCA_UPD	✓	✓	×	✓	×	×	×	×	×	×
FMT_MTD.1/DATE	✓	✓	×	✓	×	×	×	×	×	×
FMT_MTD.1.1/KEY_WRITE	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1.1/CAPK	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1/KEY_READ	✓	✓	×	×	×	×	×	×	×	×
FMT_MTD.1/MP_KEY_WRITE	✓	✓	×	×	×	×	✓	×	×	×
FMT_MTD.1/MP_KEY_READ	✓	✓	×	×	×	×	×	×	×	×
FMT_MTD.1/AA_KEY_WRITE	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1/AA_KEY_READ	✓	✓	×	×	×	×	×	×	×	×
FMT_MTD.1/LCS_PREP	✓	✓	×	×	×	×	✓	×	×	×
FMT_MTD.1/LCS_PERS	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1/LSK_READ	✓	✓	×	×	×	×	×	×	×	×
FMT_MTD.1/ADDCODE_LOAD	✓	✓	×	×	×	×	✓	×	×	×
FMT_MTD.1/ADDCODE_ACT	✓	✓	×	×	×	×	✓	×	×	×
FMT_MTD.1/AA_KEY_GEN	×	×	×	×	✓	×	✓	×	×	×
FMT_MTD.1/CA_KEY_GEN	×	×	×	×	✓	×	✓	×	×	×
FMT_MTD.1/BAC_EXP	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1/DES_SM_EXP	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1/UPD_FILE	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.1.1/SM_LVL	✓	✓	×	×	✓	×	×	×	×	×
FMT_MTD.3	✓	✓	×	✓	×	×	×	×	×	×
FMT_MTD.1/DBI	×	×	×	×	✓	×	×	×	×	×
FPT_EMS.1	×	×	✓	✓	✓	✓	✓	×	✓	✓
FPT_FLS.1	×	×	×	×	×	✓	×	✓	×	×
FPT_TST.1	×	×	×	×	×	×	×	×	×	✓
FPT_PHP.3	×	×	×	×	×	✓	×	✓	×	×
FTP_ITC.1/MP	×	×	×	×	✓	×	✓	×	×	✓

Table 21 - SFR and TSF

9 GLOSSARY AND ACRONYMS

9.1 Glossary

Term	Definition
Active Authentication	Security mechanism defined in [6] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined in [6] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO_9303]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self- signed certificate).
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.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing State or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [ICAO_9303], describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

Term	Definition
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]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations.
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]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO_9303]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer (i.e MRTD packaging responsible).
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_9303]
Improperly document person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_9303]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (cf.2.2.3.2.2).

Term	Definition
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO_9303]
Inspection System (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]
Issuing State	The Country issuing the MRTD. [ICAO_9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder, (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16). (6) EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
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]

Term	Definition
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [ICAO_9303], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14, EF.DG 16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [ICAOT], p. 14.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. 2.2.3.2.3, Step 6).
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-Personalisation	9.1.1 Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the MRTD Application (cf. 2.2.3.2.3, Step 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 Active Authentication Key Pair and the Personalization Agent Key Pair.

Term	Definition
Pre-personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
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.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or Organization, which may be used by the rightful holder for international travel. [ICAO_9303]
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE ([CC_1]).
Unpersonalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalisation Agent from the Manufacturer.
User data	Data created by and for the user, that does not affect the operation of the TSF ([CC_1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee'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
EIS	Extended Inspection System
GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number
ISK	Issuer Secret Key
MF	Master File
MSK	Manufacturer Secret Key
n.a.	Not applicable
OSP	Organizational Security Policy
PT	Personalization Terminal
SAR	Security Assurance Requirements
SFR	Security Functional Requirement
TOE	Target Of Evaluation
TSF	TOE Security Functions

10 LITERATURE

Common Criteria

[CC_1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017

[CC_2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 5, April 2017

[CC_3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 5, April 2017

[CC_EM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017

Protection Profiles

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

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

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

[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-MA-02, Version 1.3.2, 5th December 2012

ANSSI

[JIL_SRCL] Joint Interpretation Library – Security requirements for post-delivery code loading – Version 1.0, February 2016

IC

[IC_CERT] BSI-DSZ-CC-1110-V5-2022 Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, 29 April 2022

[IC_ST] Public Security Target BSI-DSZ-CC-1110-V5-2022, Version 2.0, 2022-03-28, “Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”, Infineon Technologies AG (sanitised public document)

[IC_PPM] Production and Personalization – 16-bit Security Controller Rev. 3.6, 2019-06-24

ICAO

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

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

ISO

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

[ISO_15946] Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves

[ISO_9796_2] ISO/IEC 9796-2:2010 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms

IDEMIA

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

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

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

Other

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

[TR_03111] BSI: Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 2012

[FIPS_180_2] FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002

[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

[ANSSI-PG-083] ANSSI-PG-083 v2.04 – 2020-01-01

RÈGLES ET RECOMMANDATIONS CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MÉCANISMES CRYPTOGRAPHIQUES