IDEMIA

Document Title: ID-One ePass IDL Full EACv2 in BAC MRTD configuration - Security Target Lite

FQR No:110-8334

FQR Issue:3

Legal Notice

© IDEMIA. All rights reserved.

Specifications and information are subject to change without notice.

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

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

*** Printed versions of this document are uncontrolled ***

Document Management

A. Identification

Business Unit - Department	CAI R&D
Document type:	FQR
Document Title:	ID-One ePass IDL Full EACv2 in BAC MRTD configuration – Security Target Lite
FQR No:	110 8334
FQR Issue:	3

B. Document revision

Date	Revision-Issue	Modification	Modified by
01/2017	1	Creation	Muresianu, Philippe
02/2017	2	Update references for Infineon documents	Metzier, Michele
27/08/2021	3	Surveillance 2021: • Update development site location • TOE reference with OPErational user Guide • Update [IC_CERT] and [IC_ST] references • logo IDEMIA	IDEMIA

Table of contents

1 INTRODUCTION 10

1.1 Purpose 10

1.2 Product Overview 10

2 ST LITE INTRODUCTION 11

2.1 ST reference and TOE reference 11

2.1.1 ST reference 11

2.1.2 TOE reference 11

2.1.3 IC Identification 11

2.2 TOE overview 11

2.2.1 Usage and major security features of the TOE 11

2.2.2 TOE type 14

2.2.3 TOE life cycle 14

2.2.3.1 Life cycle overview 14

2.2.3.2 Life cycle phases 15

2.2.4 Required non-TOE hardware/Software/firmware 18

2.3 TOE description 19

2.3.1 TOE Architecture 19

2.3.2 Integrated Circuit 21

2.3.3 Low layer 22

2.3.3.1 OT Basic Input/Output System (BIOS) 22

2.3.3.2 OT Cryptographic library (Crypto) 22

2.3.4 Platform layer 22

2.3.4.1 Services 22

2.3.5 Authentication Protocols 23

2.3.5.1 Terminal Authentication (TA) 23

2.3.5.2 Chip Authentication (**CA**) 23

2.3.5.3 Password Authenticated Connection Establishment (**PACE v2**) 24

2.3.5.4 Basic Access Control (**BAC**) 24

2.3.5.5 Active Authentication (**AA**) 24

2.3.6 Application layer 24

2.3.6.1 Start-Up and Applications Manager (Boot) 24

2.3.6.2 Application Creation Engine (ACRE) 24

2.3.6.3 Resident Application (RA) 24

2.3.6.4 Machine Readable Travel Document (MRTD) 24

3 CONFORMANCE CLAIMS 25
3.1 Common Criteria conformance 25
3.2 Protection Profile conformance 27
3.2.1 Overview 27
3.2.2 Assumptions 27
3.2.3 Threats 28
3.2.4 Organizational Security Policies 28
3.2.5 Security Objectives 28

4 SECURITY PROBLEM DEFINITION 30
4.1 Assets 30
4.1.1 Logical MRTD data 30
4.1.1.1 Personal Data 30
4.1.1.2 Biometric Data 30
4.1.1.3 EF.COM 30
4.1.1.4 EF.SOD 30
4.1.1.5 Chip Authentication Public Key (CA_PK) 31
4.1.1.6 Chip Authentication Private Key (CA_SK) 31
4.1.1.7 Active Authentication Public Key (AA_PK) 31
4.1.1.8 Active Authentication Private Key (AA_SK) 31
4.1.1.9 CPLC 31
4.1.1.10 TOE_ID 31
4.1.1.11 Pre-personalization Agent keys (Pre-perso_K) 31
4.1.1.12 Personalization Agent keys (Perso_K) 31
4.1.1.13 BAC keys (BAC_K) 31
4.1.1.14 Secure Messaging session keys (Session_K) 31
4.1.1.15 TOE Life Cycle State (LCS) 31
4.1.1.16 Configuration Data 32
4.1.2 Authenticity of the MRTD's chip 32
4.2 Subjects 32
4.2.1 Overview 32
4.2.2 IC manufacturer 32
4.2.3 MRTD packaging responsible 33
4.2.4 Embedded software loading responsible 33
4.2.5 Pre-personalization Agent 33
4.2.6 Personalization Agent 33
4.2.7 Terminal 33
4.2.8 Inspection system (IS) 33

4.2.9 MRTD Holder 34
4.2.10 Traveller 34
4.2.11 Attacker 34
4.3 Assumptions 34
4.3.1 A.MRTD_Manufact *"MRTD manufacturing on steps 4 to 6"* 34
4.3.2 A.MRTD_Delivery *"MRTD delivery during steps 4 to 6"* 34
4.3.3 A.Pers_Agent *"Personalization of the MRTD's chip"* 34
4.3.4 A.Insp_Sys *"Inspection Systems for global interoperability"* 34
4.3.5 A.BAC-Keys "Cryptographic quality of Basic Access Control Keys" 35
4.3.6 A.Insp_Sys_Chip_Auth *"Inspection Systems for global interoperability on chip authenticity"* 35
4.3.7 A.Signature_PKI *"PKI for Passive Authentication"* 35
4.4 Threats 35
4.4.1 T.Chip_ID *"Identification of MRTD's chip"* 35
4.4.2 T.Skimming *"Skimming the logical MRTD"* 36
4.4.3 T.Eavesdropping *"Eavesdropping to the communication between TOE and inspection system"* 36
4.4.4 T.Forgery *"Forgery of data on MRTD's chip"* 36
4.4.5 T.Abuse-Func *"Abuse of Functionality"* 37
4.4.6 T.Information_Leakage *"Information Leakage from MRTD's chip"* 37
4.4.7 T.Phys-Tamper *"Physical Tampering"* 37
4.4.8 T.Malfunction *"Malfunction due to Environmental Stress"* 39
4.4.9 T.Configuration *"Tampering attempt of the TOE during preparation"* 39
4.4.10 T.Counterfeit *"MRTD's chip"* 39
4.5 Organisational Security Policies 40
4.5.1 P.Manufact *"Manufacturing of the MRTD's chip"* 40
4.5.2 P.Personalization *"Personalization of the MRTD by issuing State or Organization only"* 40
4.5.3 P.Personal_Data *"Personal data protection policy"* 40

5 SECURITY OBJECTIVES 41
5.1 Security objectives for the TOE 41
5.1.1 OT.AC_Pers *"Access Control for Personalization of logical MRTD"* 41
5.1.2 OT.Data_Int *"Integrity of personal data"* 41
5.1.3 OT.Data_Conf *"Confidentiality of personal data"* 41
5.1.4 OT.Identification *"Identification and Authentication of the TOE"* 41
5.1.5 OT.Prot_Abuse-Func *"Protection against Abuse of Functionality"* 42
5.1.6 OT.Prot_Inf_Leak *"Protection against Information Leakage"* 42

5.1.7 OT.Prot_Phys-Tamper *"Protection against Physical Tampering"* 42
5.1.8 OT.Prot_Malfunction *"Protection against Malfunctions"* 42
5.1.9 OT.Chip_Auth_Proof *"Proof of MRTD's chip authenticity"* 42
5.1.10 OT.Configuration *"Protection of the TOE preparation"* 43
5.2 Security objectives for the operational environment 43
5.2.1 Issuing State or Organization 43
5.2.1.1 OE.MRTD_Manufact "Protection of the MRTD Manufacturing" 43
5.2.1.2 OE.MRTD_Delivery "Protection of the MRTD delivery" 43
5.2.1.3 OE.Personalization "Personalization of logical MRTD" 44
5.2.1.4 OE.Pass_Auth_Sign "Authentication of logical MRTD by Signature" 44
5.2.1.5 OE.BAC-Keys "Cryptographic quality of Basic Access Control Keys" 44
5.2.1.6 OE.Auth_MRTD "MRTD Authentication Key" 44
5.2.2 Receiving State or Organization 44
5.2.2.1 OE.Exam_MRTD "Examination of the MRTD passport book" 45
5.2.2.2 OE.Exam_Chip_Auth "Examination of the chip authenticity" 45
5.2.2.3 OE.Passive_Auth_Verif "Verification by Passive Authentication" 45
5.2.2.4 OE.Prot_Logical_MRTD "Protection of data from the logical MRTD" 45
5.3 Security objectives rationale 45

6 EXTENDED COMPONENTS DEFINITION 46
6.1 Extended components definition 46
6.1.1 Definition of the Family FAU_SAS 46
6.1.2 Definition of the Family FCS_RND 47
6.1.3 Definition of the Family FMT_LIM 48
6.1.4 Definition of the Family FPT_EMS 49
6.1.5 Definition of the Family FIA_API 50

7 SECURITY REQUIREMENTS 52
7.1 Security functional requirements 52
7.1.1 Class FAU *"Security Audit"* 54
7.1.1.1 FAU_SAS.1 "Audit Storage" 54
7.1.2 Class FCS *"Cryptographic Support"* 55
7.1.2.1 FCS_CKM.1 "Cryptographic key generation" 55
7.1.2.2 FCS_CKM.4 "Cryptographic key destruction" 55
7.1.2.3 FCS_COP.1 "Cryptographic operation" 56
7.1.2.4 FCS_RND.1 "Quality metric for random numbers" 58
7.1.3 Class FIA "Identification and Authentication" 58
7.1.3.1 FIA_UID.1 "Timing of identification" 58
7.1.3.2 FIA_UAU.1 "Timing of authentication" 58

7.1.3.3 FIA_UAU.4 "Single-use authentication mechanisms" 59
7.1.3.4 FIA_UAU.5 "Multiple authentication mechanisms" 59
7.1.3.5 FIA_UAU.6 "Re-authenticating" 60
7.1.3.6 FIA_AFL.1 "Authentication failure handling" 60
7.1.3.7 FIA_API.1 "Authentication Proof of Identity" 61
7.1.4 Class FDP *"User Data Protection"* 61
7.1.4.1 FDP_ACC.1 "Subset access control" 61
7.1.4.2 FDP_ACF.1 "Basic Security attribute based access control" 62
7.1.4.3 FDP_UCT.1 "Basic data exchange confidentiality" 64
7.1.4.4 FDP_UIT.1 "Data exchange integrity" 65
7.1.4.5 FDP_ITC.1 "Import of user data without security attributes" 65
7.1.5 Class FMT *"Security Management"* 66
7.1.5.1 FMT_MOF "Management of functions in TSF" 66
7.1.5.2 FMT_SMF.1 "Specification of Management Functions" 67
7.1.5.3 FMT_SMR.1 "Security roles" 67
7.1.5.4 FMT_LIM.1 "Limited capabilities" 67
7.1.5.5 FMT_LIM.2 "Limited availability" 68
7.1.5.6 FMT_MTD.1 "Management of TSF data" 68
7.1.6 Class FPT *"Protection of the Security Functions"* 69
7.1.6.1 FPT_EMS.1 "TOE Emanation" 69
7.1.6.2 FPT_FLS.1 "Failure with preservation of secure state" 70
7.1.6.3 FPT_TST.1 "TSF testing" 70
7.1.6.4 FPT_PHP.3 "Resistance to physical attack" 71
7.1.7 Class FTP "Trusted path/channels" 71
7.1.7.1 FTP_ITC.1 "Inter-TSF trusted channel" 71
7.2 Security assurance requirements 72
7.2.1 EAL rationale 72
7.2.2 EAL augmentation rationale 72
7.2.2.1 ALC_DVS.2 "Sufficiency of security measures" 72
7.2.2.2 ADV_FSP.5 "Complete semi-formal functional specification with additional error information" 72
7.2.2.3 ADV_INT.2 "Well-structured internals" 72
7.2.2.4 ADV_TDS.4 "Semiformal modular design" 72
7.2.2.5 ALC_CMS.5 "Development tools CM coverage" 73
7.2.2.6 ALC_TAT.2 "Compliance with implementation standards" 73
7.2.2.7 ATE_DPT.3 "Testing: modular design" 73
7.2.1 Dependencies 73
7.3 Security requirements rationale 74

8 TOE SUMMARY SPECIFICATION 75

8.1 TOE summary specification 75

8.1.1 Overview 75

8.1.2 Access Control in Reading 75

8.1.3 Access Control in Writing 76

8.1.4 Active Authentication 76

8.1.5 Basic Access Control 76

8.1.6 Chip Authentication 77

8.1.7 MRTD Personalization 77

8.1.8 Physical Protection 77

8.1.9 MRTD Pre-personalization 77

8.1.10 Safe State Management 77

8.1.11 Secure Messaging 78

8.1.12 Self Tests 78

8.2 SFR and TSF 79

9 COMPOSITION WITH IC SECURITY TARGET 82

APPENDIX A: GLOSSARY 83

9.1 Acronyms 88

APPENDIX B: LITERATURE 89

1 INTRODUCTION

1.1 Purpose

This security target Lite describes the security needs induced by the ePass ICAO essential product in BAC configuration with CA and AA on Infineon SLE77 components.

The objectives of this Security Target Lite are:

- To describe the Target of Evaluation (TOE), its life cycle and to position it in the smart card life cycle,
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the platform active phases,
- To describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the product active phases,
- To specify the security requirements which include the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment,
- To describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements,
- To present evidence that this ST Lite is a complete and cohesive set of requirements that the TOE provides on an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements.

1.2 Product Overview

The ePass ICAO essential is a multi configuration MRTD product. It provides four configurations, which are:

- the ePass ICAO essential product in BAC configuration with CA and AA,
- the ePass ICAO essential product in EAC configuration with AA,
- the ePass ICAO essential product in EAC with PACE configuration with AA,
- the ePass ICAO essential product in PACE configuration with CA, AA.

The ePass ICAO essential Operating System is embedded on two different components:

- SLE77CLFX2400P,
- SLE77CLFX2407P,

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

2 ST LITE INTRODUCTION

2.1 ST reference and TOE reference

2.1.1 ST reference

Title	ID-One ePass IDL Full EACv2 in BAC MRTD configuration – Security Target
Version	6
Author	IDEMIA
Publication Date	27/08/2021
CC version	3.1 revision 4
EAL	EAL4 augmented with: • ADV_FSP.5, ADV_INT.2, ADV_TDS.4, • ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, • ATE_DPT.3
PP	See [PP_BAC]

Table 1 – ST Reference

2.1.2 TOE reference

Developer Name	IDEMIA
Product Name	ID-One ePass ICAO essential configuration SAC and EAC
TOE Name	ID-One ePass IDL Full EACv2 in BAC MRTD configuration
TOE Identification	SAAAAR code: 084194
Guidance documents	FQR 110 7226 Ed6 – ePass ICAO Essential – Perso Guide FQR 110 8250, version 2 - ePass ICAO essential OPErational user Guide

Table 2 – TOE Reference

2.1.3 IC Identification

IC Certificate	See [IC_CERT]
IC Public Security Target	See [IC_ST]

Table 3 – IC Identification

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 traveller presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this Security Target Lite contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid MRTD personalized for a holder with

the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

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.

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

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

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

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

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

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

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, the Active Authentication and the Chip Authentication according to [ICAO_9303].

The TOE comprises at least:

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

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

2.2.3 TOE life cycle

2.2.3.1 *Life cycle overview*

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

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

Table 4 - Roles identification on the life cycle

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

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
	TOE delivery point				
	4	MRTD packaging responsible	×		
	5	Pre-personalization agent	×	AGD_PRE	
3 - Personalization	6	Personalization agent	×	AGD_PRE	
4 - Operational Use	7	End user	×	AGD_OPE	

Table 5 - Subjects identification following life cycle steps – Scheme 1

Scheme 2, MRTD chip Embedded Software loaded by the OS loader 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	×	ALC packaging centre	Vitré and/or Shenzhen
		Embedded software loading responsible	✓	ALC Embedded software loading centre	Vitré and/or Shenzhen
	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 6 - Subjects identification following life cycle steps – Scheme 2

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 Lite. The table below indicates how terms shall be read:

Term in [PP_BAC]	Meaning in this ST Lite
Software developer	TOE developer
non-volatile non-programmable	Part of the Flash memory where the Flash Loader and the

memory(ies)	**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 is 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 is 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 is 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 1: 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 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [CC_1] §92) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Basic Authentication Control Key.

Application note 3: This security target lite distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [ICAO_9303]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

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

Application note 5: The intention of this security target lite 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 Lite 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 - TOE architecture. Each part of the TOE is presented in the following chapters.

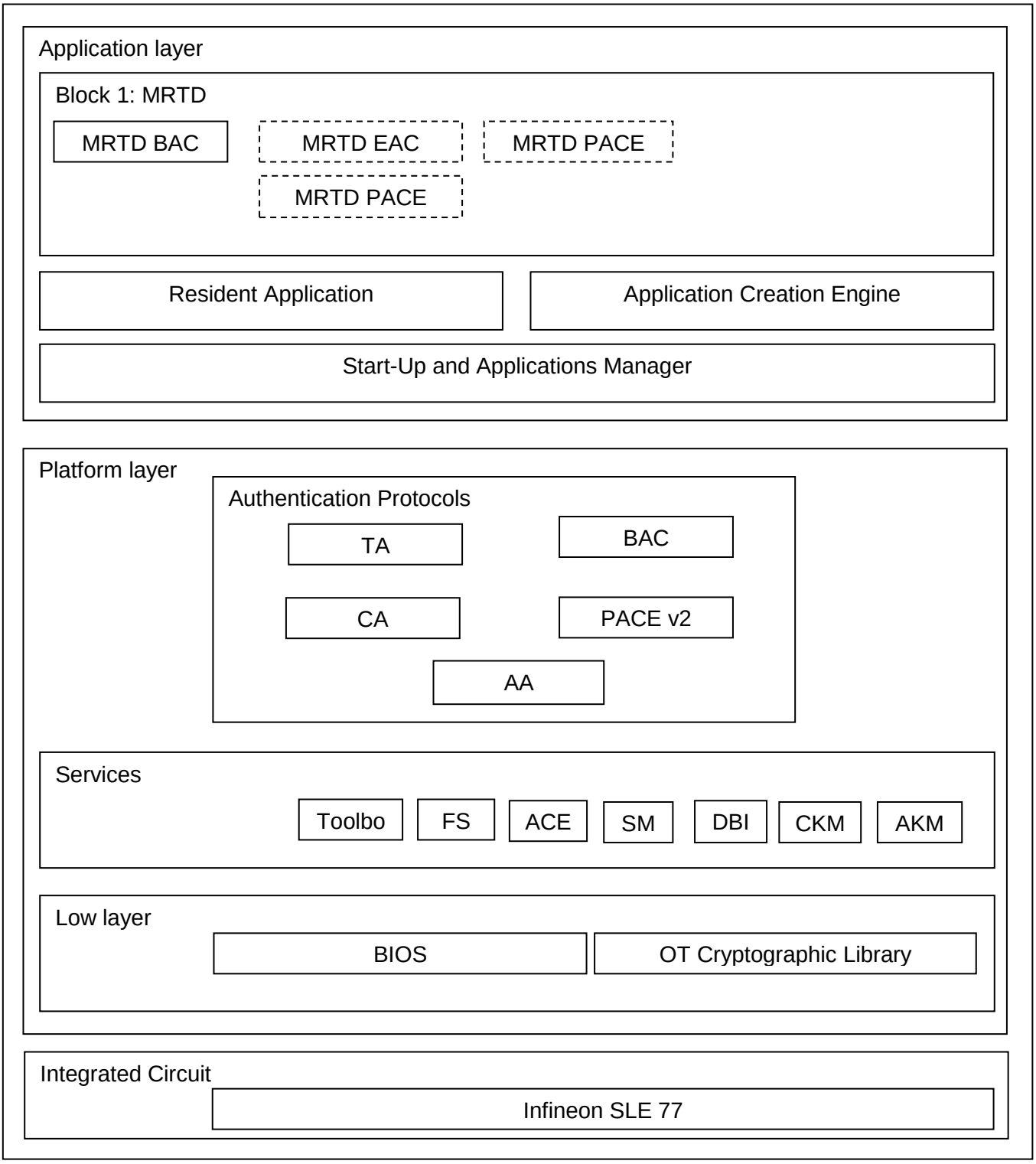

Figure 1 - TOE architecture

2.3.2 Integrated Circuit

The TOE is embedded on Infineon chips SLE77CLFX2400P and SLE77CLFX2407P. The IC part of the TOE comprises the following:

Core System:

- CPU
- Memory Encryption/Decryption Unit (MED)
- Memory Management Unit (MMU)

Memories:

- Read-Only Memory (ROM)
- Random Access Memory (RAM)
- SOLID FLASH™ NVM

Peripherals:

- True Random Number Generator (TRNG)
- Pseudo Random Number Generator (PRNG)
- Watchdog and timers
- Universal Asynchronous Receiver/Transmitter (UART)
- Checksum module (CRC)
- Radio Frequency Interface (RFI)

Control:

- Dynamic Power Management
- Internal Clock Oscillator (ICO)
- Interrupt and Peripheral Event Channel Controller (ITP and PEC)
- Interface Management Module (IMM)
- User mode Security Life Control (UmSLC)
- Voltage regulator

Coprocessors:

- Crypto2304T for asymmetric algorithms like RSA and EC
- Symmetric Crypto Coprocessor for AES and 3DES Standard

Security Peripherals:

- Filters
- Sensors

Buses:

- Memory Bus
- Peripheral Bus

And associated Firmware and Software, it comprises:

- RMS and SAM routines for Solid Flash NVM programming; security functions test, random number online testing. STS consisting of test and initialization routines. All stored in the ROM part.
- The Flash Loader that allows the loading of TOE software.
- And cryptographic libraries.

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 *OT 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 *OT 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. This specific 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

2.3.4.1.7 Digitally Blurred Image (**DBI**)

The Digital Blurred Image (DBI) is ensured by Watermarking Module. It allows the blurring of a JPG or JPEG2000 file stored in a transparent file.
This feature is the implementation of patents owned by IDEMIA.

*The DBI module is part of the TOE but is **NOT** 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 but is **NOT** 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 *Basic Access Control (**BAC**)*

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

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

2.3.5.5 *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:

- Creation of application
- Storage of the Active Authentication key (ECC and RSA keys)
- Storage of multiple Chip Authentication keys under the ADF (supporting ECC and RSA Keys)
- Storage of CVCA Keys under each ADF

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).

3 CONFORMANCE CLAIMS

3.1 Common Criteria conformance

This Security Target Lite (ST Lite) claims conformance to the Common Criteria (CC) version 3.1 revision 4. 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",** • **FMT_LIM.1 "Limited capabilities",** • **FMT_LIM.2 "Limited availability",** • **FPT_EMS.1 "TOE Emanation",** • **FIA_API.1[1] "Authentication Proof of Identity",**
Part 3	**Conformance with package EAL4 augmented[2] with:** • **ALC_DVS.2 "Sufficiency of security measures" defined in [CC_3],** • **ADV_FSP.5 "Complete semi-formal functional specification with additional error information" defined in [CC_3],** • **ADV_INT.2 "Well-structured internals" defined in [CC_3],** • **ADV_TDS.4 "Semiformal modular design" defined in [CC_3],** • **ALC_CMS.5 "Development tools CM coverage" defined in [CC_3],** • **ALC_TAT.2 "Compliance with implementation standards" defined in [CC_3],** • **ATE_DPT.3 "Testing: modular design" defined in [CC_3].**

Table 7 - Common Criteria conformance claim

Remark

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

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

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.

---

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

[2] *This EAL and its augmentations correspond to an EAL5 + ALC_DVS.2 where AVA_VAN level is downgraded to AVA_VAN.3 following constraint of MRZ entropy described in [ICAO_9303].*

3.2 Protection Profile conformance

3.2.1 Overview

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

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

Table 8 - Protection Profile conformance

This ST Lite also addresses the Manufacturing and Personalization phases at TOE level (cf. §2.2.3 TOE life cycle), as well as the Chip Authentication (CA) and 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_BAC] that covers the advanced security methods BAC in operational use phase.

The following parts list assumptions, threats, OSP, OT and OE for this TOE (i.e. from [PP_BAC] 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_BAC],
- **A.MRTD_Delivery** *"MRTD delivery during steps 4 to 6"* defined in [PP_BAC],
- **A.Pers_Agent** *"Personalization of the MRTD's chip"* defined in [PP_BAC],
- **A.Insp_Sys** *"Inspection Systems for global interoperability"* defined in [PP_BAC],
- **A.BAC-Keys** *"Cryptographic quality of Basic Access Control Keys"* defined in [PP_BAC],
- **A.Insp_Sys_Chip_Auth** *"Inspection Systems for global interoperability on chip authenticity"* defined in this ST Lite,
- **A.Signature_PKI** *"PKI for Passive Authentication"* defined in [PP_EAC].

A.Insp_Sys_Chip_Auth and A.Signature_PKI are additional for the Chip Authentication protocol and Active Authentication protocol which are not in the original scope of the [PP_BAC]. These assumptions are only linked to threats for the Chip Authentication protocol and 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_BAC], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_BAC].

3.2.3 Threats

The following threats are averted by this TOE:

- **T.Chip_ID** *"Identification of MRTD's chip"* defined in [PP_BAC],
- **T.Skimming** *"Skimming the logical MRTD"* defined in [PP_BAC],
- **T.Eavesdropping** *"Eavesdropping to the communication between TOE and inspection system"* defined in [PP_BAC],
- **T.Forgery** *"Forgery of data on MRTD's chip"* defined in [PP_BAC],
- **T.Abuse-Func** *"Abuse of Functionality"* defined in [PP_BAC],
- **T.Information_Leakage** *"Information Leakage from MRTD's chip"* defined in [PP_BAC],
- **T.Phys-Tamper** *"Physical Tampering"* defined in [PP_BAC],
- **T.Malfunction** *"Malfunction due to Environmental Stress"* defined in [PP_BAC],
- **T.Configuration** *"Tampering attempt of the TOE during preparation"* defined in this ST Lite,
- **T.Counterfeit** *"MRTD's chip"* defined in [PP_EAC].

3.2.4 Organizational Security Policies

This TOE complies with the following OSP:

- **P.Manufact** *"Manufacturing of the MRTD's chip"* defined in [PP_BAC],
- **P.Personalization** *"Personalization of the MRTD by issuing State or Organization only"* defined in [PP_BAC],
- **P.Personal_Data** *"Personal data protection policy"* defined in [PP_BAC].

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_BAC],
- **OT.Data_Int** *"Integrity of personal data"* defined in [PP_BAC],
- **OT.Data_Conf** *"Confidentiality of personal data"* defined in [PP_BAC],
- **OT.Identification** *"Identification and Authentication of the TOE"* defined in [PP_BAC],
- **OT.Prot_Abuse-Func** *"Protection against Abuse of Functionality"* defined in [PP_BAC],
- **OT.Prot_Inf_Leak** *"Protection against Information Leakage"* defined in [PP_BAC],
- **OT.Prot_Phys-Tamper** *"Protection against Physical Tampering"* defined in [PP_BAC],
- **OT.Prot_Malfunction** *"Protection against Malfunctions"* defined in [PP_BAC],
- **OT.Chip_Auth_Proof** *"Proof of MRTD's chip authenticity"* defined in this ST Lite,
- **OT.Configuration** *"Protection of the TOE preparation"* defined in this ST Lite.

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

- **OE.MRTD_Manufact** *"Protection of the MRTD Manufacturing"* defined in [PP_BAC],
- **OE.MRTD_Delivery** *"Protection of the MRTD delivery"* defined in [PP_BAC],
- **OE.Personalization** *"Personalization of logical MRTD"* defined in [PP_BAC],
- **OE.Pass_Auth_Sign** *"Authentication of logical MRTD by Signature"* defined in [PP_BAC],
- **OE.BAC-Keys** *"Cryptographic quality of Basic Access Control Keys"* defined in [PP_BAC],
- **OE.Exam_MRTD** *"Examination of the MRTD passport book"* defined in [PP_BAC],
- **OE.Passive_Auth_Verif** *"Verification by Passive Authentication"* defined in [PP_BAC],
- **OE.Prot_Logical_MRTD** *"Protection of data from the logical MRTD"* defined in [PP_BAC],
- **OE.Auth_MRTD** *"MRTD Authentication Key"* defined in this ST Lite,
- **OE.Exam_Chip_Auth** *"Examination of the chip authenticity"* defined in this ST Lite.

OE.Auth_MRTD and OE.Exam_Chip_Auth are additional objectives for the operational environment for the Chip Authentication protocol and Active Authentication protocol which are not in the original scope of the [PP_BAC]. These objectives are only linked to threats for the Chip Authentication protocol and 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_BAC], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_BAC].

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	✗	✓	✗
BAC_K	✗	✓	✓
Session_K	✓	✓	✓
LCS	✓	✓	✓
Configuration data	✓	✓	✓

Table 9 - 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*

This data allows the identification of the TOE. This data are part of the IC Embedded Software in the non-volatile non-programmable memory.

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 *BAC keys (BAC_K)*

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

4.1.1.14 *Secure Messaging session keys (Session_K)*

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

4.1.1.15 *TOE Life Cycle State (LCS)*

This is the Life Cycle State of the TOE.

4.1.1.16 *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.

4.1.2 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 §2.2.3TOE 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	✗	✗	✗	✓	✗
Terminal	4.2.7	✗	✗	✓	✓	✓
Inspection System	4.2.8	✗	✗	✗	✗	✓
MRTD Holder	4.2.9	✗	✗	✗	✗	✓
Traveller	4.2.10	✗	✗	✗	✗	✓
Attacker	4.2.11	✓	✓	✓	✓	✓

Table 10 - 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_BAC]. 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_BAC]. 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_BAC]. 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 used 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_BAC]. This subject is responsible for the preparation of the card, i.e. creation of the MF and MRTD ADF. He also sets Personalization Agent keys 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 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.

4.2.8 Inspection system (IS)

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

Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

4.2.9 MRTD Holder

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

4.2.10 Traveller

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

4.2.11 Attacker

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

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).

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.

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 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.

4.3.5 A.BAC-Keys **"Cryptographic quality of Basic Access Control Keys"**

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the [ICAO_9303], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

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

The Inspection System implements at least one of the following protocols to authenticate the MRTD's chip: Chip Authentication and Active Authentication. The Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism, or uses the signature returned by the TOE during Active Authentication as proof of authenticity.

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

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

4.4 Threats

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

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

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data

printed on the MRTD data page in advance

Asset: Anonymity of user

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

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

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

Asset: confidentiality of logical MRTD data.

4.4.3 T.Eavesdropping *"Eavesdropping to the communication between TOE and inspection system"*

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

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

Asset: confidentiality of logical MRTD data.

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

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

another contactless chip.

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

Asset: authenticity of logical MRTD data.

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

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

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

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

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

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

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

Asset: confidentiality of logical MRTD and TSF data.

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

Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker

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

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

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

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

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

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

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

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

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

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

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

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

Asset: authenticity of logical MRTD data

4.5 Organisational Security Policies

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

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

4.5.2 P.Personalization *"Personalization of the MRTD by issuing State or Organization only"*

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

4.5.3 P.Personal_Data *"Personal data protection policy"*

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)[3] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO_9303].

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

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.Data_Conf *"Confidentiality of personal data"*

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

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). In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

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

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

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

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

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

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

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

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

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

with a prior

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

5.1.8 OT.Prot_Malfunction *"Protection against Malfunctions"*

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

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

The TOE must support the Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [TR_03110], or Active Authentication as defined in in combination with the Document Security Object (SOD) verification to verify the SOD belongs to the data page, the chip is genuine and chip and data page

belong to each other as defined in [ICAO_9303].The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

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.

5.2 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.

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.

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.BAC-Keys* "Cryptographic quality of Basic Access Control Keys"

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the [ICAO_9303] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

5.2.1.6 *OE.Auth_MRTD* "MRTD Authentication Key"

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

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

5.2.2 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 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].

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

Additionally to the OE.Exam_MRTD, inspection system performs the Chip Authentication Protocol or 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 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 receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

5.3 Security objectives rationale

Removed from ST

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 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].*

6.1.4 Definition of the Family FPT_EMS

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

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS.1 TOE emanation has two constituents:

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

data or user data.

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6.1.5 Definition of the Family FIA_API

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

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

Family behavior

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

Component leveling:

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: There are no actions defined to be auditable.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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_BAC]	Descr.	Step			
			Before 5	5	6	7
Class FAU "Security Audit"						
FAU_SAS.1.1	FAU_SAS.1.1	7.1.1.1	✓	✗	✗	✗
Class FCS "Cryptographic Support"						
FCS_CKM.1.1/BAC	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/CA	Additional SFR		✗	✗	✗	✓
FCS_CKM.4.1	FCS_CKM.4.1	7.1.2.2	✗	✓	✓	✓
FCS_COP.1.1/BAC_SHA	FCS_COP.1.1/SHA	7.1.2.3	✗	✗	✗	✓
FCS_COP.1.1/BAC_ENC	FCS_COP.1.1/ENC		✗	✗	✗	✓
FCS_COP.1.1/AUTH	FCS_COP.1.1/AUTH		✗	✗	✓	✗
FCS_COP.1.1/BAC_MAC	FCS_COP.1.1/MAC		✗	✗	✗	✓
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_KEY_DEC			✗	✓	✓	✗
FCS_COP.1.1/CA_SHA	Additional SFR		✗	✗	✗	✓
FCS_COP.1.1/CA_ENC			✗	✗	✗	✓
FCS_COP.1.1/CA_MAC			✗	✗	✗	✓
FCS_COP.1.1/AA_DSA	Additional SFR		✗	✗	✗	✓
FCS_RND.1.1	FCS_RND.1.1	7.1.2.4	✗	✓	✓	✓
Class FIA "Identification and Authentication"						
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/BAC	FIA_UAU.5.1	7.1.3.4	✗	✗	✓	✓
FIA_UAU.5.2/BAC	FIA_UAU.5.2		✗	✗	✓	✓

SFR in ST	SFR in [PP_BAC]	Descr.	Step			
			Before 5	5	6	7
FIA_UAU.5.1/MP	Additional SFR		✗	✓	✗	✗
FIA_UAU.5.2/MP			✗	✓	✗	✗
FIA_UAU.5.1/CA	Additional SFR		✗	✗	✓	✓
FIA_UAU.5.2/CA			✗	✗	✓	✓
FIA_UAU.6.1/BAC	FIA_UAU.6.1	7.1.3.5	✗	✗	✗	✓
FIA_UAU.6.1/MP	Additional SFR		✗	✓	✓	✗
FIA_UAU.6.1/CA	Additional SFR		✗	✗	✗	✓
FIA_AFL.1.1/BAC	FIA_AFL.1.1	7.1.3.6	✗	✗	✗	✓
FIA_AFL.1.2/BAC	FIA_AFL.1.2		✗	✗	✗	✓
FIA_AFL.1.1/MP	Additional SFR		✗	✓	✓	✗
FIA_AFL.1.2/MP	Additional SFR		✗	✓	✓	✗
FIA_API.1.1/CA	Additional SFR	7.1.3.7	✗	✗	✗	✓
FIA_API.1.1/AA	Additional SFR		✗	✗	✗	✓
Class FDP "User Data Protection"						
FDP_ACC.1.1/BAC	FDP_ACC.1.1	7.1.4.1	✗	✗	✓	✓
FDP_ACC.1.1/MP	Additional SFR		✗	✓	✓	✗
FDP_ACC.1.1/ID	Additional SFR		✗	✓	✓	✓
FDP_ACF.1.1/BAC	FDP_ACF.1.1	7.1.4.2	✗	✗	✓	✓
FDP_ACF.1.2/BAC	FDP_ACF.1.2		✗	✗	✓	✓
FDP_ACF.1.3/BAC	FDP_ACF.1.3		✗	✗	✓	✓
FDP_ACF.1.4/BAC	FDP_ACF.1.4		✗	✗	✓	✓
FDP_ACF.1.1/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_UCT.1.1/BAC	FDP_UCT.1.1	7.1.4.3	✗	✗	✗	✓
FDP_UCT.1.1/MP	Additional SFR		✗	✓	✓	✗
FDP_UCT.1.1/CA	Additional SFR		✗	✗	✗	✓
FDP_UIT.1.1/BAC	FDP_UIT.1.1	7.1.4.4	✗	✗	✗	✓
FDP_UIT.1.2/BAC	FDP_UIT.1.2		✗	✗	✗	✓
FDP_UIT.1.1/MP	Additional SFR		✗	✓	✓	✗
FDP_UIT.1.2/MP			✗	✓	✓	✗
FDP_UIT.1.1/CA	Additional SFR		✗	✗	✗	✓
FDP_UIT.1.2/CA			✗	✗	✗	✓

SFR in ST	SFR in [PP_BAC]	Descr.	Step			
			Before 5	5	6	7
FDP_ITC.1.1/MP	Additional SFR	7.1.4.5	✗	✓	✓	✗
FDP_ITC.1.2/MP			✗	✓	✓	✗
FDP_ITC.1.3/MP			✗	✓	✓	✗
Class FMT "Security Management"						
FMT_MOF.1.1/PROT	Additional SFR	7.1.5.1	✗	✓	✓	✗
FMT_MOF.1.1/GP			✗	✓	✓	✗
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	7.1.5.5	✗	✓	✓	✓
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/KEY_WRITE	FMT_MTD.1.1/KEY_WRITE		✗	✓	✓	✓
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/CAPK	Additional SFR		✗	✓	✓	✓
FMT_MTD.1.1/CAPK_READ			✗	✓	✓	✓
FMT_MTD.1.1/AA_KEY_WRITE	Additional SFR		✗	✓	✓	✓
FMT_MTD.1.1/AA_KEY_READ			✗	✓	✓	✓
FMT_MTD.1.1/LCS_PREP	Additional SFR		✗	✓	✓	✓
FMT_MTD.1.1/LCS_PERS			✗	✓	✓	✓
Class FPT "Protection of the Security Functions"						
FPT_EMS.1.1	FPT_EMSEC.1.1	7.1.6.1	✗	✓	✓	✓
FPT_EMS.1.2	FPT_EMSEC.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	✗	✓	✓	✓
Class FTP "Trusted path/channels"						
FTP_ITC.1.1/MP	Additional SFR	7.1.7.1	✗	✓	✓	✗
FTP_ITC.1.2/MP			✗	✓	✓	✗
FTP_ITC.1.3/MP			✗	✓	✓	✗

Table 11 - 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/ BAC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Document Basic Access Key Derivation Algorithm** and specified cryptographic key sizes **112 bit** that meet the following: **[ICAO_9303], normative appendix 5**.

FCS_CKM.1.1/ 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_DIV. 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 **Triple-DES in CBC mode** and specified cryptographic key sizes **112 bit** that meet the following: **[GPC_SPE_034]; appendix E.4.1.**

FCS_CKM.1.1/ CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **based on ECDH compliant to [ISO_15946]** and specified cryptographic key sizes **192 to 521 bit** that meet the following: **[TR_03110].**

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

FCS_COP.1.1/ BAC_ENC The TSF shall perform **secure messaging (BAC) – encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bit** that meets the following **[FIPS_46_3] and [ICAO_9303]; normative appendix 5, A5.3 [ICAO_9303].**

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

FCS_COP.1.1/ BAC_MAC The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bit** that meets the following **[ISO_9797_1] (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).**

FCS_COP.1.1/ 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 **Triple-DES in CBC mode** and cryptographic key sizes **112 bit** that meets the following **[FIPS_46_3].**

FCS_COP.1.1/ GP_AUTH

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

FCS_COP.1.1/ GP_MAC

The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **MAC Algorithm 1 with Padding M2** and cryptographic key sizes **112 bit** that meets the following **[ISO_9797_1].**

FCS_COP.1.1/ GP_KEY_DEC

The TSF shall perform **key decryption** in accordance with a specified cryptographic algorithm **Triple-DES in ECB mode** and cryptographic key sizes **112 bit** that meets the following **[FIPS_46_3]**

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	[FIPS_46_3]
AES in CBC mode	128, 192 and 256 bit	[FIPS_197]

FCS_COP.1.1/ CA_MAC

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

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

FCS_COP.1.1/ AA_DSA — The TSF shall perform **Digital Signature Creation** in accordance with a specified cryptographic algorithm **RSA signature CRT with SHA-1, SHA-224 and SHA-256** and cryptographic key sizes **1024 to 2048 in steps of 256 bits** that meet the following **[FIPS_186_3].**

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 [RGS2_B1].**

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 read the Initialization Data in Phase 2 "Manufacturing",**
2. **to read the random identifier in Phase 3 "Personalization of the MRTD",**
3. **to read the random identifier in Phase 4 "Operational Use"**

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

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

7.1.3.2 *FIA_UAU.1* "Timing of authentication"

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.1.1 The TSF shall allow

1. **to read the Initialization Data in Phase 2 "Manufacturing",**
2. **to read the random identifier in Phase 3 "Personalization of the MRTD",**
3. **to read the random identifier in Phase 4 "Operational Use"**

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

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

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

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/ BAC The TSF shall provide

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

To support user authentication.

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

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

FIA_UAU.5.1/ MP The TSF shall provide

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

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.**

FIA_UAU.5.1/ CA — The TSF shall provide

1. **Secure messaging in MAC-ENC mode,**

To support user authentication.

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

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

7.1.3.5 *FIA_UAU.6* "Re-authenticating"

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/ BAC — The TSF shall re-authenticate the user under the conditions **each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism.**

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

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

FIA_UAU.6.1/ CA — The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the Chip Authentication Protocol shall**

be verified as being sent by the inspection system.

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

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

FIA_AFL.1.1/ MP: The TSF shall detect when **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 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/ BAC: The TSF shall enforce the **Basic Access Control SFP** on **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to**

EF.DG16 of the logical MRTD.

FDP_ACC.1/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 and the Configuration Data.**

FDP_ACC.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.**

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

1. **Subjects:**
   a. **Personalization Agent,**
   b. **Basic Inspection System,**
   c. **Terminal,**
2. **Objects:**
   a. **data EF.DG1 to EF.DG16 of the logical MRTD,**
   b. **data in EF.COM,**
   c. **data in EF.SOD,**
3. **Security attributes**
   a. **authentication status of terminals.**

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

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

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

FDP_ACF.1.4/ BAC

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

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

FDP_ACF.1.1/ 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,**
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.**

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/

The TSF shall explicitly deny access of subjects to objects based on the following

MP 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. **Basic 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 Basic 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,**

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

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

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

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 initialisation

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,**

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**.

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. **Chip Authentication protocol,**
6. **Protection of incoming user data,**
7. **Protection of outgoing user data.**

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. **Basic Inspection System**

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

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

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

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

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

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to **read** the **Document Basic Access Keys and Personalization Agent Keys** to **none.**
FMT_MTD.1.1/ 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/ CAPK	The TSF shall restrict the ability to **write** the **Chip Authentication Keys** to **the Personalization Agent.**
FMT_MTD.1.1/ CAPK_READ	The TSF shall restrict the ability to **read** the **Chip Authentication Private Key** to **none.**
FMT_MTD.1.1/ 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 Private 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.**

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 Keys** and :

- **Personal Data including Biometric Data,**
- **EF.COM,**
- **EF.SOD,**
- **Chip Authentication Private Key,**
- **Chip Authentication Public Key,**

- **Active Authentication Private Key,**
- **Active Authentication Public Key,**
- **CPLC,**
- **TOE_ID,**
- **Pre-personalization Agent Keys,**
- **BAC Keys,**
- **Secure Messaging Session Keys,**
- **TOE Life Cycle State,**
- **Configuration Data.**

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

- **Personal Data including Biometric Data,**
- **EF.COM,**
- **EF.SOD,**
- **Chip Authentication Private Key,**
- **Chip Authentication Public Key,**
- **Active Authentication Private Key,**
- **Active Authentication Public Key,**
- **CPLC,**
- **TOE_ID,**
- **Pre-personalization Agent Keys,**
- **BAC Keys,**
- **Secure Messaging Session Keys,**
- **TOE Life Cycle State,**
- **Configuration 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 a BAC authentication,**
- **When performing the Chip 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, BAC_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 4 (EAL4) and augmented by taking the following component: ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, and ATE_DPT.3.

7.2.1 EAL rationale

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

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 EAL4 has no dependencies to other security requirements

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

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

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

7.2.2.3 *ADV_INT.2 "Well-structured internals"*

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

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

7.2.2.4 *ADV_TDS.4 "Semiformal modular design"*

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

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

7.2.2.5 *ALC_CMS.5 "Development tools CM coverage"*

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

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

7.2.2.6 *ALC_TAT.2 "Compliance with implementation standards"*

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

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

7.2.2.7 *ATE_DPT.3 "Testing: modular design"*

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

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

7.2.1 Dependencies

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

SAR	Dependencies	Support of the Dependencies
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.3	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	ADV_ARC.1 ADV_FSP.5 ADV_TDS.4 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.3

Table 12 - SARs dependencies

7.3 Security requirements rationale

Removed from ST

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	✓	×	✓
Basic Access Control	F.BAC	§ 8.1.5	×	×	✓
Chip Authentication	F.CA	§ 8.1.6	✓	×	✓
MRTD Personalization	F.PERS	§ 8.1.7	×	✓	×
Physical Protection	F.PHY	§ 8.1.8	✓	✓	✓
MRTD Pre-personalization	F.PREP	§ 8.1.9	✓	×	×
Safe State Management	F.SS	§ 8.1.10	✓	✓	✓
Secure Messaging	F.SM	§ 8.1.11	✓	✓	✓
Self Tests	F.STST	§ 8.1.12	✓	✓	✓

Table 13 - 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

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 Basic Access Control

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

8.1.6 Chip Authentication

This TSF provides the Chip Authentication, authentication and session keys generation to be used by F.SM, as described in [TR_03110]. It also provides management of this function in phase 5.

8.1.7 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 user data,
- Load Chip Authentication keys and Active Authentication keys,
- Set Personalization Agent CPLC Data,
- Set TOE life cycle in Operational Use phase.

8.1.8 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.

8.1.9 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:

- Diversify the MSK,
- 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.

8.1.10 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 § 8.1.12,
- 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.

8.1.11 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.

8.1.12 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 Private Key and Active Authentication Private Key.

8.2 SFR and TSF

SFR \ TSF	F.ACR	F.ACW	F.AA	F.BAC	F.CA	F.PERS	F.PHY	F.PREP	F.SS	F.SM	F.STST
FAU_SAS.1	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
FCS_CKM.1/BAC	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓
FCS_CKM.1/MSK_DIV	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓
FCS_CKM.1/GP	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓
FCS_CKM.1/CA	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓
FCS_CKM.4	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗
FCS_COP.1/BAC_SHA	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
FCS_COP.1/BAC_ENC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FCS_COP.1/AUTH	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓
FCS_COP.1/BAC_MAC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FCS_COP.1/MSK_SHA	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
FCS_COP.1/GP_ENC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FCS_COP.1/GP_AUTH	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓
FCS_COP.1/GP_MAC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FCS_COP.1/GP_KEY_DEC	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓
FCS_COP.1/CA_SHA	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗
FCS_COP.1/CA_ENC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FCS_COP.1/CA_MAC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FCS_COP.1/AA_DSA	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
FCS_RND.1	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗	✓
FIA_UID.1	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
FIA_UAU.1	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
FIA_UAU.4	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✓
FIA_UAU.5/BAC	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓
FIA_UAU.5/MP	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓
FIA_UAU.5/CA	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓

SFR \ TSF	F.ACR	F.ACW	F.AA	F.BAC	F.CA	F.PERS	F.PHY	F.PREP	F.SS	F.SM	F.STST
FIA_UAU.6/BAC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FIA_UAU.6/MP	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FIA_UAU.6/CA	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FIA_AFL.1/BAC	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓
FIA_AFL.1/MP	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓
FIA_API.1/CA	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗
FIA_API.1/AA	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
FDP_ACC.1/BAC	✓	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗
FDP_ACC.1/MP	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗
FDP_ACC.1/ID	✓	✓	✗	✓	✗	✓	✗	✓	✗	✗	✗
FDP_ACF.1/BAC	✓	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗
FDP_ACF.1/MP	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗
FDP_ACF.1/ID	✓	✓	✗	✓	✗	✓	✗	✓	✗	✗	✗
FDP_UCT.1/BAC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FDP_UCT.1/MP	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FDP_UCT.1/CA	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FDP_UIT.1/BAC	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FDP_UIT.1/MP	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FDP_UIT.1/CA	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
FDP_ITC.1/MP	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓
FMT_MOF.1/PROT	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗
FMT_MOF.1/GP	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗
FMT_SMF.1	✗	✗	✓	✗	✓	✓	✗	✓	✗	✗	✗
FMT_SMR.1	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗
FMT_LIM.1	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
FMT_LIM.2	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
FMT_MTD.1/INI_ENA	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗

SFR \ TSF	F.ACR	F.ACW	F.AA	F.BAC	F.CA	F.PERS	F.PHY	F.PREP	F.SS	F.SM	F.STST
FMT_MTD.1/INI_DIS	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗
FMT_MTD.1/KEY_WRITE	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗
FMT_MTD.1/KEY_READ	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
FMT_MTD.1/MP_KEY_WRITE	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗
FMT_MTD.1/MP_KEY_READ	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
FMT_MTD.1/CAPK	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗
FMT_MTD.1/CAPK_READ	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
FMT_MTD.1/AA_KEY_WRITE	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗
FMT_MTD.1/AA_KEY_READ	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
FMT_MTD.1/LCS_PREP	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗
FMT_MTD.1/LCS_PERS	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗
FPT_EMS.1	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
FPT_FLS.1	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
FPT_TST.1	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
FPT_PHP.3	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
FTP_ITC.1/MP	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓

Table 14 – SFR and TSF

9 COMPOSITION WITH IC SECURITY TARGET

Removed from ST

Appendix A: Glossary

Term	Definition
Active Authentication	Security mechanism defined in [ICAO_9303] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined in [ICAO_9303] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO_9303]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_9303]
Country Signing CA Certificate (Ccsca)	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [ICAO_9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [ICAO_9303]
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]

Extended Access Control (EAC)	Security mechanism identified in [ICAO_9303] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO_9303]
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).
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]
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	TSF data used for authentication proof and verification of the

Authentication Information	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	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.
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.
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]

Traveller	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 89nrolee whose identity is being claimed, to determine whether it matches the 89nrolee'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.

9.1 Acronyms

Acronym	Term
BIS	Basic Inspection System
CC	Common Criteria
EF	Elementary File
GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number
ISK	Issuer Secret Key
MF	Master File
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

Appendix B: 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 4, September 2012

[CC_2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[CC_3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[CC_EM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

Protection Profiles

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

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

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

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

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

IC

[IC_CERT] Certification Report - BSI-DSZ-CC-0964-V5-2021 for Infineon Technologies Security Controller M7794 A12 and G12

[IC_ST] M7794 A12 and G12 – Security Target Lite Version 2.6, 2021-03-18

[IC_PPM] User's manual, SLx 70 Family, Production anad Personalization, 2015-04

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

IDEMIA

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

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

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

Other

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

[FIPS_180_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

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

[AIS_32] Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik