Security Target Lite
eTravel Next 1.0
BAC and AA activated

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

CONTENT

1. SECURITY TARGET INTRODUCTION 4
1.1 SECURITY TARGET REFERENCE 4
1.2 TOE REFERENCE 4
1.3 SECURITY TARGET OVERVIEW 5
1.4 REFERENCES 6
1.4.1 External References 6
1.4.2 Internal References 8
2. TOE OVERVIEW 9
2.1 TOE DESCRIPTION 9
2.2 TOE BOUNDARIES 9
2.3 TOE USAGE AND SECURITY FEATURES FOR OPERATIONAL USE 10
2.4 TOE LIFE-CYCLE 12
2.4.1 Four phases 12
2.4.2 Actors 13
2.4.2.1 Initialization on module at Gemalto site 14
2.4.3 Non-TOE hardware/software/firmware required by the TOE 15
3. CONFORMANCE CLAIMS 16
3.1 CC CONFORMANCE CLAIM 16
3.2 PP CLAIM, ... 16
3.3 PACKAGE CLAIM 16
3.4 CONFORMANCE STATEMENT 16
4. SECURITY PROBLEM DEFINITION 17
4.1 INTRODUCTION 17
4.1.1 Assets 17
4.1.2 Subjects 17
4.2 ASSUMPTIONS 18
4.3 THREATS 19
4.4 ORGANIZATIONAL SECURITY POLICIES 22
4.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-BAC] AND [ST-IC] 23
4.5.1 Compatibility between threats of [ST-BAC] and [ST-IC] 23
4.5.2 Compatibility between OSP of [ST-BAC] and [ST-IC] 23
4.5.3 Compatibility between assumptions of [ST-BAC] and [ST-IC] 23
5. SECURITY OBJECTIVES 24
5.1 SECURITY OBJECTIVES FOR THE TOE 24
5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 26
5.3 SECURITY OBJECTIVE RATIONALE 28
5.3.1 Rationale between objectives and threats, assumptions, OSP 28
5.3.2 Compatibility between objectives of [ST-BAC] and [ST-IC] 30
5.3.2.1 Compatibility between objectives for the TOE 30
5.3.2.2 Compatibility between objectives for the environment 30
5.3.3 Justifications for adding objectives on the environment 30
5.3.3.1 Additions to [PP-MRTD-BAC] 30
6. EXTENDED COMPONENTS DEFINITION 31
6.1 DEFINITION OF THE FAMILY FAU_SAS 31
6.2 DEFINITION OF THE FAMILY FCS_RND 31
6.3 DEFINITION OF THE FAMILY FIA_API 32
6.4 DEFINITION OF THE FAMILY FMT_LIM 33
6.5 DEFINITION OF THE FAMILY FPT_EMS 35
7. SECURITY REQUIREMENTS 36
7.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE 36
7.1.1 Class FAU Security Audit 36
7.1.2 Class Cryptographic Support (FCS) 37
7.1.3 Class FIA Identification and Authentication 41
7.1.4 Class FDP User Data Protection 44

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7.1.5 Class FMT Security Management *46*
7.1.6 Class FPT Protection of the Security Functions *49*
7.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE 51
7.3 SECURITY REQUIREMENTS RATIONALE 51
7.3.1 Security Functional Requirements Rationale *51*
7.3.2 Dependency Rationale *54*
7.3.3 Security Assurance Requirements Rationale *56*
7.3.4 Security Requirements – Mutual support and internal consistency *56*
7.3.5 Compatibility between SFR of [ST-BAC] and [ST-IC] *56*
8. TOE SUMMARY SPECIFICATION 56
8.1 TOE SECURITY FUNCTIONS 56
8.1.1 TSFs provided by the eTravel Next 1.0 Software *56*
8.1.2 TSFs provided by the Infineon M7892 chip *57*
9. RATIONALES 58
9.1 TOE SUMMARY SPECIFICATION RATIONALE 58
9.1.1 TOE security functions rationale *58*
10. ACRONYMS AND GLOSSARY 59

FIGURES

Figure 1: TOE Boundaries 10
Figure 2: LC1: Initialization on module at Gemalto site 14

TABLES

Table 1: Identification of the actors 13
Table 2: Security objective rationale 28
Table 3: FCS_CKM.1/AA iteration explanation 37
Table 4: FCS_COP.1/AA iteration explanation 40
Table 5: Overview on authentication SFR 41
Table 6: FIA_AFL.1 iteration explanation 43
Table 7: Security functional requirement rationale 52
Table 8: Security functional requirement dependencies 55
Table 9: Security Functions provided by the eTravel Next 1.0 Software 56
Table 10: Security Functions provided by the Infineon M7892 chip 57
Table 11: Rationale table of functional requirements and security functions 58

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

1. SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title:	eTravel Next 1.0 – BAC and AA activated Security Target
Version:	1.5p
ST reference:	D1449178
Origin:	Gemalto
IT Security Evaluation scheme:	Serma Safety & Security
IT Security Certification scheme:	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 TOE REFERENCE

Product Name:	eTravel Next 1.0
Security Controller	M7892 G12
TOE Name	eTravel Next 1.0 BAC+AA
TOE Version	1.29.00
TOE documentation:	Guidance [AGD]

The TOE identification is provided by the Card Production Life Cycle Data (CPLCD). These data are available by executing a dedicated command.
Identification data and dedicated command are described in the TOE guidance documentation.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

1.3 SECURITY TARGET OVERVIEW

Gemalto has developed an eTravel application with all the mandatory features for ePassport specified by ICAO and EU.

The Security Target (ST) is based on Protection Profile *Machine Readable Travel Document with "ICAO Application", Basic Access Control* [PP-MRTD-BAC].

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) based on the requirements of the International Civil Aviation Organization (ICAO). More specifically the TOE consists of operating system of MRTD's chip with ICAO application. The TOE is programmed according to Logical Data Structure as defined in [ICAO-9303].

This ST defines the security requirements for the TOE. The main security objective is to provide the secure enforcing functions and mechanisms to maintain the integrity and confidentiality of the MRTD application and data during its life cycle.

The main objectives of this ST are:

- To introduce TOE and the MRTD application,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

1.4 REFERENCES

1.4.1 External References

[BIO]	*BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS*, Technical Report, Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 2.0, ICAO TAG MRTD/NTWG, 21 May 2004
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, version 3.1 rev 5, April 2017
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2012-09-002, version 3.1 rev 5, April 2017
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2012-09-003, version 3.1 rev 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2012-09-004, version 3.1 rev 5, April 2017
[RGS-B1]	Référentiel général de sécurité version 2.0 Annexe B1 Mécanismes cryptographiques…version 2.03 du 21 février 2014
[SP 800-90]	NIST Special Publication 800-90A, Revision 1, Recommendation for the Random Number Generation Using Deterministic Random Bit Generators, June 2015
[ST-IC]	Security Target Common Criteria EAL6 augmented / EAL6+ M7892 Design Steps D11 and G12 Revision 1.2 as of 2017-11-21
[CR-IC]	Certification Report, M7892 D11 & G12 BSI-DSZ-CC-0891-V3-2018
[FIPS180-2]	*Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+Change Notice to include SHA-224),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[FIPS46-3]	*Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, Reaffirmed 1999 October 25
[FIPS197]	*Federal Information Processing Standards Publication 197 ADVANCED ENCRYPTION STANDARD (AES),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2001 November 26
[ISO15946-1]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General,* 2002
[ISO15946-2]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures,* 2002
[ISO15946-3]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment,* 2002
[ISO7816]	*ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange*, FDIS2004

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

[ISO9796-2]	*ISO/IEC 9797: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms,* 2002
[ISO9797-1]	*ISO/IEC 9797: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,* 1999
[ICAO-9303]	9303 ICAO Machine Readable Travel Document 7th edition, 2015 Part 1-12
[PKCS#3]	*PKCS #3: Diffie-Hellman Key-Agreement Standard,* An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PKI]	*MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access* International Civil Aviation Organization Version 1.1, October 01 2004
[PP-IC-0084]	*Smartcard IC Platform protection Profile* BSI-CC-PP-0084-2014
[PP-MRTD-EACv2]	Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012 (Version 1.3.2, 05th December 2012)
[PP-MRTD-SAC]	Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22th July 2014
[PP-MRTD-BAC]	Protection Profile, Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10, 25 mars 2009. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-PP-0055-2009
[SS]	*ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS*, *Excerpts from ICAO Doc 9303, Part 1* Machine Readable Passports, Fifth Edition – 2003
[TR-ECC]	*Elliptic Curve Cryptography according to ISO 15946,* Technical Guideline, TR-ECC, BSI, 2006
[TR-EAC-1]	TR-03110 Technical Guideline – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Version 2.2 February 2015
[TR-SAC]	ICAO TR – Supplemental Access Control for Machine Readable Travel Document, Version 1.1, April 15, 2014.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

1.4.2 Internal References

[ST-BAC]	eTravel Next 1.0 BAC and AA activated Security Target Ref: D1449178
[AGD]	Guidance Documentation
[PRE_MRTD]	eTravel Next 1.0 AGD - PRE Document Ref. D1449281 Rev 1.1
[OPE_MRTD]	eTravel Next 1.0 AGD - OPE Document Ref. D1449282 Rev 1.2
[AGD_USR]	Ref D1404349 eTravel Next 1.x Administrator Reference Manual April 12,2018 eTravel Next 1.x Personalization Reference Manual April 12,2018 eTravel Next 1.0 Administrator Reference Manual addendum for configuration settings April 12,2018

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

2. TOE OVERVIEW

This Security Target defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control and the Active Authentication specified in the Technical reports of 'ICAO Doc 9303' [ICAO-9303].

2.1 TOE DESCRIPTION

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [ICAO-9303] and providing the Basic Access Control according (BAC) to the 'ICAO Doc 9303' [ICAO-9303]

In addition to [PP-MRTD-BAC], the TOE supports the active authentication as defined in [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
- a cryptographic library developed by Gemalto (the cryptographic library proposed by the chip supplier is not used)

2.2 TOE BOUNDARIES

Application note: The TOE is the module designed to be the core of an MRTD passport. The TOE is an integrated circuit. The TOE is connected to an antenna and capacitors and is mounted on a plastic film. This inlay is then embedded in the coversheet or datapage of the MRTD passport and provides a contactless interface for the passport holder identification.

The TOE is programmed according to the Logical Data Structure [ICAO-9303] and providing:

- the Basic Access Control (BAC) according to the ICAO document [ICAO-9303]
- the Active Authentication (AA) mechanism according to the ICAO document [ICAO-9303]

Application note: Additionally to the [PP-MRTD-BAC], the TOE has a set of administrative commands for the management of the product during the product life.

Application note: Components within the TOE boundary are defined in the following manner:

- *the Integrated Circuit (IC),*
- *the IC Dedicated Test Software,*
- *the IC Dedicated Support Software (Boot Rom Software),*
- *the eTravel Next 1.0 Embedded Software (ES),*
- *part of the MRTD Logical Data Structure,*
- *the guidance documentation of the eTravel Next 1.0 product*
    - *the preparation guide (assurance family AGD-PRE),*
    - *the operational guide (assurance family AGD-OPE)*

The TOE provides only contactless interface, contact mode is irreversibly deactivated.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

The eTravel Next 1.0 Embedded Software (ES) is implemented in the NVM memory (flash technology) of the chip.

The TOE is delivered to the Administration Authority with data and guidance documentation in order to perform the initialization of the product. In addition, the Administration Key is delivered from the MRTD Manufacturer to the Administration Authority.

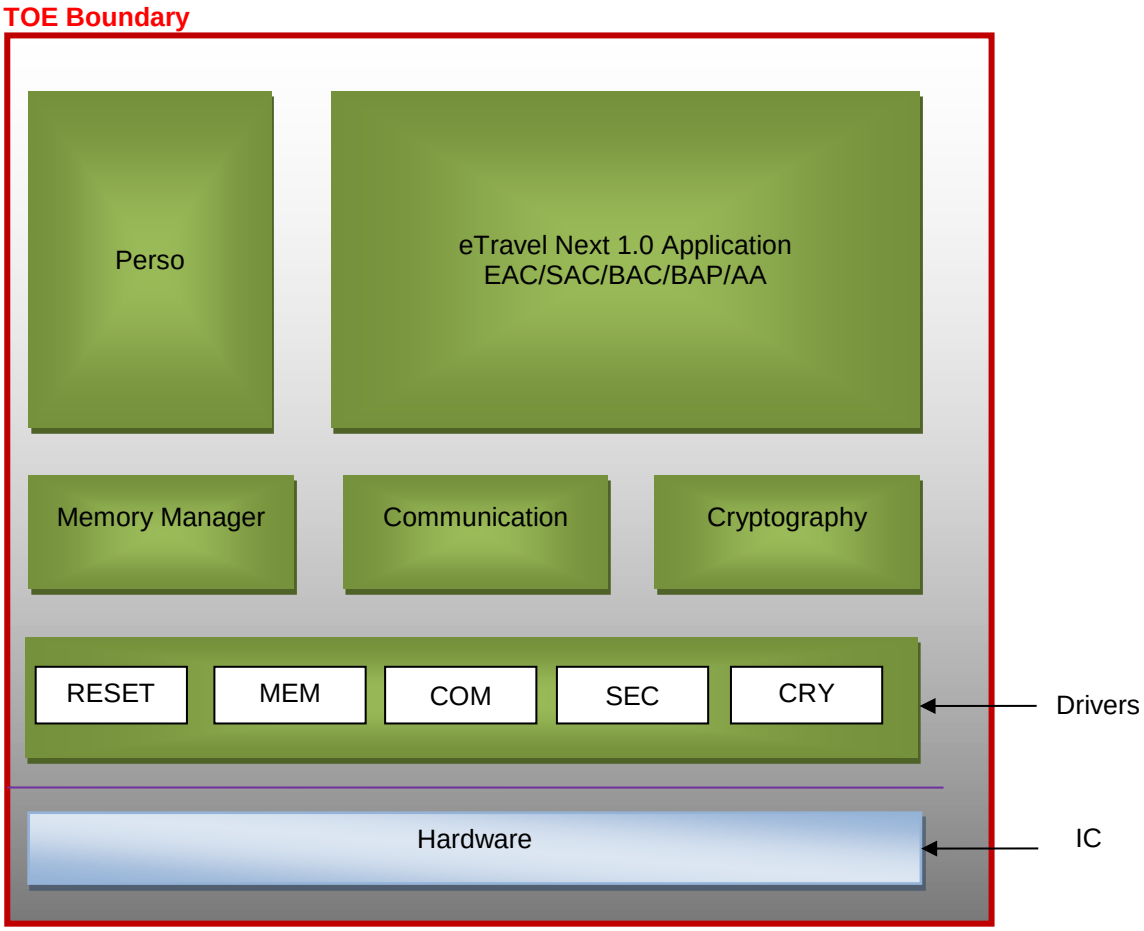


Figure 1: TOE Boundaries

2.3 TOE USAGE AND SECURITY FEATURES FOR OPERATIONAL USE

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

For this security target the MRTD is viewed as unit of

(a) the **physical MRTD** as travel document in form of paper, plastic and chip. It presents 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

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

(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[1]
(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 of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism. This security target addresses the Active Authentication but does not address the Extended Access Control, both optional security mechanisms.

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], normative appendix 5.

[1] These additional biometric reference data are optional

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

2.4 TOE LIFE-CYCLE

As a summary description of how the parts of the TOE are delivered to the final customer, the eTravel Next 1.0 application is delivered mainly in form of an inlay. The form factor is packaged on Gemalto's manufacturing facility and sent to final customer premises.

The different guides accompanying the TOE and parts of the TOE are the ones specified in [AGD] section. They are delivered in form of electronic documents (*.pdf) by Gemalto's Technical representative.

2.4.1 Four phases

The TOE life cycle is described in terms of the four life cycle phases With respect to [PP-BSI-0084], the TOE life cycle is additionally subdivided into 7 steps.

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 ePassport application and the guidance documentation associated with these TOE components.

Phase 2 "Manufacturing":

(Step3)
The TOE integrated circuit is produced by the IC manufacturer conforming to Gemalto requirements. The IC manufacturer writes the IC Identification Data onto the chip to control the IC 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 or to the Inlay Manufacturer.

(Step4)
The MRTD manufacturer initializes the IC/inlay by loading the MRTD application in the IC flash memory

(Step5)
The MRTD manufacturer (i) initializes the MRTD application and (ii) equips MRTD's chips with pre-personalization Data (**mainly diversified administration key**). The pre-personalized MRTD together with the IC Identifier are securely delivered from the MRTD manufacturer to the **Administration Authority**. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the **Administration Authority**.

Phase 3 "Personalization of the MRTD":

(Step6)
The Administration Authority:

- Set the final configuration of the MRTD
- Complete the pre-personalization (Creates MRTD file structure)
- Load the Personalization key

(Step6 bis)
The personalization of the MRTD includes:

- the survey of the MRTD holder biographical data,
- the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- the printing of the visual readable data onto the physical MRTD,
- the writing the TOE User Data and TSF Data into the logical MRTD,

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

- the writing the TSF Data into the logical MRTD and configuration of the TSF if necessary.

The step "writing the TOE User Data" is performed by the Personalization Agent and includes but is not limited to the creation of:

- the digital MRZ data (EF.DG1),
- the digitized portrait (EF.DG2),
- the Document security object (SOD).

The signing of the Document security object by the Document signer [PKI] 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.

Phase 4 "Operational Use"

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

Application note: In this ST, the role of the Personalization Agents is strictly limited to the phase 3 Personalization. In the phase 4 Operational Use updating and addition of the data groups of the MRTD application is forbidden.

2.4.2 Actors

Actors	Identification
Integrated Circuit (IC) Developer	Infineon
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	Infineon
Module manufacturer	Gemalto
Inlay manufacturer	Gemalto or another Inlay manufacturer
Book manufacturer	Gemalto or another printer
Administration Authority	The agent who is acting on the behalf of the issuing State or Organization and set final configuration of the product and complete pre-personalisation of the MRTD before issuing the product to the Personalization Agent.
Personalization Agent	The agent who is acting on the behalf of the issuing State or Organization and personalize the MRTD for the holder by activities establishing the identity of the holder with biographic data.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.

Table 1: Identification of the actors

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

2.4.2.1 Initialization on module at Gemalto site

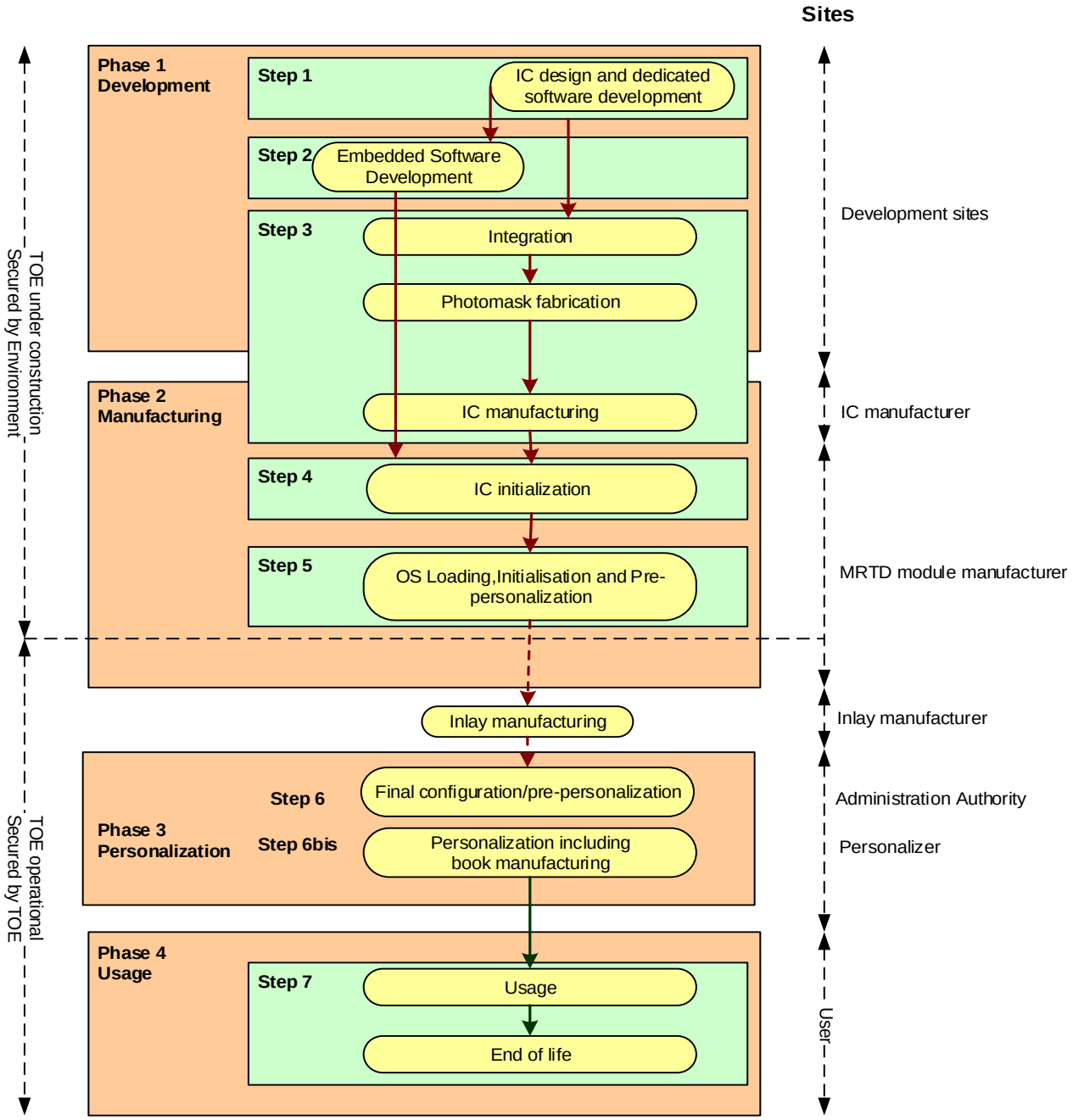


Figure 2: LC1: Initialization on module at Gemalto site

LC1 describes the standard Life Cycle. The IC is manufactured at the founder site. It is then shipped to Gemalto site where it is initialized (OS loading, default configuration and pre-personalization). The transformation of wafers into modules can be performed either at the founder site or at Gemalto site. The modules/inlay are then shipped to the Administration Authority for final configuration and pre-personalisation. During the shipment from Gemalto to the Administration Authority the module/inlay is protected by a diversified key.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

2.4.3 Non-TOE hardware/software/firmware required by the TOE

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

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

3. CONFORMANCE CLAIMS

3.1 CC CONFORMANCE CLAIM

Common criteria Version:

This ST conforms to CC Version 3.1 [CC-1] [CC-2] [CC-3]

Conformance to CC part 2 and 3:

CC Part 2 extended,

- CC Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; [CEM] has to be taken into account.

3.2 PP CLAIM,

The **eTravel Next 1.0 – BAC and AA activated Security Target** claims strict conformance to the Protection Profile “Machine Readable Travel Document with ICAO Application, Basic Access Control ([PP-MRTD-BAC]).

The TOE also claims conformance to other Protection Profiles. This is described in other Security Targets:

- The **eTravel Next 1.0 – PACE, EAC and AA activated Security Target** claims strict conformance to Profile [PP-MRTD-EACv2] and [PP-MRTD-SAC].

3.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2, ATE_DPT.3, ALC_DVS.2 defined in CC part 3 [CC-3].

3.4 CONFORMANCE STATEMENT

This ST strictly conforms to [PP-MRTD-BAC].

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

4. SECURITY PROBLEM DEFINITION

4.1 INTRODUCTION

4.1.1 Assets

The assets to be protected by the TOE include the User Data on the MRTD's chip.

Logical MRTD Data
The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [ICAO-9303]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons as the 'ICAO Doc 9303' [9303] the TOE described in this security target specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to:

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

The TOE prevents read access to sensitive User Data

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

A sensitive asset is the following more general one.

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.

4.1.2 Subjects

This security target considers the following subjects:

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

Administration Authority
The Administration Authority (acting in step 6) is the agent acting on behalf of the issuing State or Organization who is responsible to configure and to initialize the MRTD before Personalization. Administration Authority loads the personalization key.

Personalization Agent
The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [ICAO-9303].

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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

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

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

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

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

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

4.2 ASSUMPTIONS

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

A.MRTD_Manufact MRTD manufacturing on steps 4 to 6
It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery MRTD delivery during steps 4 to 6
Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:
- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent 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.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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.

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

4.3 THREATS

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

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

T.Chip_ID **Identification of MRTD's chip**
Adverse action: An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.
Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance
Asset: Anonymity of user,

T.Skimming **Skimming the logical MRTD**
Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.
Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance
Asset: confidentiality of logical MRTD data

T.Eavesdropping **Eavesdropping to the communication between TOE and inspection system**
Adverse action: An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.
Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance
Asset: confidentiality of logical MRTD data

T.Forgery **Forgery of data on MRTD's chip**
Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.
This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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,

The TOE shall avert the threats as specified below.

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

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

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

T.Malfunction Malfunction due to Environmental Stress

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

4.4 ORGANIZATIONAL SECURITY POLICIES

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

P.Manufact Manufacturing of the MRTD's chip
The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

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

P.Personal_Data Personal data protection policy
The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)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].

P.Active_Auth Active Authentication

The TOE implements the active authentication protocol as described in [ICAO-9303].

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

4.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-BAC] AND [ST-IC]

4.5.1 Compatibility between threats of [ST-BAC] and [ST-IC]

T.Chip_ID, T.Skimming, T.Eavesdropping are specific to [ST-BAC] and they do no conflict with the threats of [ST-IC].
T.Forgery is included in T.Phys-Manipulation.
T.Abuse-Func of [ST-BAC] is included in T.Abuse-Func of [ST-IC].
T.Information_Leakage is included in T.Leak-Inherent and T.Leak-Forced.
T.Phys-Tamper is included in T.Phys-Manipulation
T.Malfunction of [ST-BAC] is included in T.Malfunction of [ST-IC].

We can therefore conclude that the threats of [ST-BAC] and [ST-IC] are consistent.

4.5.2 Compatibility between OSP of [ST-BAC] and [ST-IC]

P.Manufact, P.Personalization and P.PersonalData are specific to the MRTD and they do no conflict with the OSP of [ST-IC].

We can therefore conclude that the OSP of [ST-BAC] and [ST-IC] are consistent.

4.5.3 Compatibility between assumptions of [ST-BAC] and [ST-IC]

A.MRTD_Manufact and A.MRTD_Delivery are included in A.Process-Sec-IC

A.Pers_Agent, A.Insp_Sys, and A.BAC-Keys are assumptions specific to [ST-BAC] and they do no conflict with the assumptions of [ST-IC].

We can therefore conclude that the assumptions for the environment of [ST-BAC] and [ST-IC] are consistent.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

5. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the security objectives for the TOE 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.

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.

Application note: The OT.AC_Pers implies that
(1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) cannot be changed by write access after personalization,
(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

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

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

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

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

The following TOE security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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

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

OT.Prot_Inf_Leak Protection against Information Leakage
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.

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.

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.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

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

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

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

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

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

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

OE.Active_Auth_Sign Active Authentication of logical MRTD by Signature
The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) ensure the secrecy of the MRTD's Active Authentication Private Key, sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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

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

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

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

OE.Active_Auth_Verif Verification by Active Authentication
In addition to the verification by passive authentication, the inspection systems may use the verification by active authentication, which offers a stronger guaranty of the authenticity of the MRTD.

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).

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

5.3 SECURITY OBJECTIVE RATIONALE

5.3.1 Rationale between objectives and threats, assumptions, OSP

The rationale in this paragraph comes from [PP-MRTD-BAC] §4.3. Additions due to Active Authentication are shaded.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Activ_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.Active_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Active_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip_ID				X											X				
T.Skimming			X												X				
T.Eavesdropping			X												X				
T.Forgery	X	X						X					X	X		X	X	X	
T.Abuse-Func						X						X							
T.Information_Leakage							X												
T.Phys-Tamper								X											
T.Malfunction									X										
P.Manufact				X															
P.Personalization	X			X								X							
P.Personal_Data		X	X																
P.Active_Auth					X									X				X	
A.MRTD_Manufact										X									
A.MRTD_Delivery											X								
A.Pers_Agent												X							
A.Insp_Sys																X			X
A.BAC-Keys															X				

Table 2: Security objective rationale

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

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

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

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

The OSP **P.Active_Auth** “Active Authentication” addresses the active authentication protocol as described in [ICAO-9303]. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Active_Auth_Sign “**Active Authentication of logical MRTD by Signature” and verified by the inspection system according to **OE.Active_Auth_Verif** “Verification by Active Authentication”. This is possible only because genuine TOE enforce AA as specified in **OT.Active_Auth_Proof**.

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

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

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

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

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

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

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

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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

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

The assumption **A.BAC-Keys** “Cryptographic quality of Basic Access Control Keys” is directly covered by the security objective for the TOE environment **OE.BAC-Keys** “Cryptographic quality of Basic Access Control Keys” ensuring the sufficient key quality to be provided by the issuing State or Organization.

5.3.2 Compatibility between objectives of [ST-BAC] and [ST-IC]

5.3.2.1 Compatibility between objectives for the TOE

OT.AC_Pers, OT.Activ_Auth_Proof are specific to [ST-BAC] and they do not conflict with the objectives of [ST-IC].
OT.Data_Conf is included in O.RND,O.TDES and O.AES
OT.Data_Int is included in O.RND,O.TDES and O.AES
OT.Identification is included in O.Identification.
OT.Prot_Abuse-Func is included in O.Abuse-Func.
OT.Prot_Inf_Leak is included in O.Leak-Inherent and O.Leak-Forced
OT.Prot_Phys-Tamper is included in O.Phys-Manipulation and O.Phys-Probing.
OT.Prot_Malfunction is included in O.Malfunction.

We can therefore conclude that the objectives for the TOE of [ST-BAC] and [ST-IC] are consistent.

5.3.2.2 Compatibility between objectives for the environment

OE.MRTD_Manufact is included in OE.Process-TOE and OE.Process-Card.
OE.MRTD_ Delivery is included in OE.Process-Card.
OE.Personalization is partly included in OE.Process-Card.
OE.Pass_Auth_Sign, OE.Active_Auth_Sign, OE.Auth_Key_MRTD, OE.Authoriz_Sens_Data, OE.BAC_PP, OE.Exam_MRTD, OE.Passive_Auth_Verif, OE.Active_Auth_Verif, OE.Prot_Logical_MRTD, OE.Ext_Insp_Systems are specific to [ST-BAC] and they do no conflict with the objectives of [ST-IC].

We can therefore conclude that the objectives for the environment of [ST-BAC] and [ST-IC] are consistent
.

5.3.3 Justifications for adding objectives on the environment

*5.3.3.1 Additions to [PP-MRTD-*BAC]

The only additional objectives on the environment are OE.Active_Auth_Sign and OE.Active_Auth_Verif. These objectives request the environment to support Active Authentication. AA is an operation outside [PP-MRTD-BAC]. Therefore the added objectives on the environment do not weaken the TOE

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

6. EXTENDED COMPONENTS DEFINITION

This ST uses components defined as extensions to CC part 2. Some of these components are defined in protection profile [PP-IC-0084], other components are defined in the protection profile [PP-MRTD-BAC].

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

Component levelling

FAU_SAS Audit data storage	1

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1
There are no management activities foreseen.

Audit: FAU_SAS.1
There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components
Dependencies: No dependencies

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

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

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

Component levelling:

FCS_RND Generation of random numbers	1

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*].

6.3 Definition of the Family FIA_API

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

FIA_API Authentication Proof of Identity

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

Component levelling:

FIA_API Authentication Proof of Identity	1

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*].

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

6.4 DEFINITION OF THE FAMILY FMT_LIM

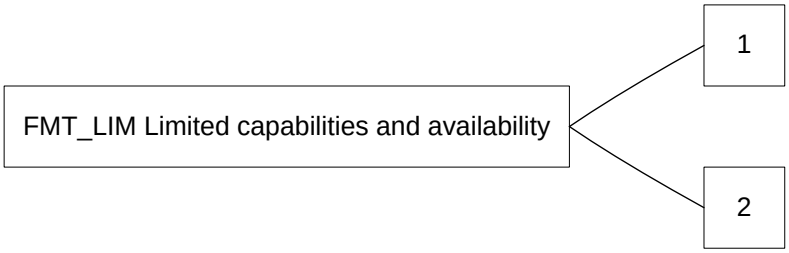
The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class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

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

FMT_LIM Limited capabilities and availability

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

Component leveling:



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

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.

Management: FMT_LIM.1, FMT_LIM.2
There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2
There are no actions defined to be auditable.

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

The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components
Dependencies: FMT_LIM.2 Limited availability.

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

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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*].

Application note: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

6.5 DEFINITION OF THE FAMILY FPT_EMS

Rationale

This family is defined in [PP-MRTD-BAC] as FPT_EMSEC and is renamed as FTP_EMS in this ST.

Family FPT_EMS (TOE Emanation) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. This requirement is not covered by CC Part 2 [CC-2].

Family behavior:

This family defines requirements to prevent attacks against TSF data and user 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.

Component leveling:

FPT_EMS TOE emanation	1

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*].

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7. SECURITY REQUIREMENTS

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Basic Inspection System”, and “Terminal” used in the following chapter is given in section 4.1. Note that all these subjects are acting for homonymous external entities. All used objects are defined either in section 10 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [CC-2]. The operation “load” is synonymous to “import” used in [CC-2].

Definition of security attributes:

security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalization Agent	Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

7.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.
Refinements in this section are in underline font when the SFR’s refinement is already present in [PP-MRTD-BAC], and in bold font when the refinement is done in this ST. When the SFR is refined in the [PP-MRTD-BAC] and additionally refined in this ST then the font is bold and underline.

For this section, a presentation choice has been selected. Each SFR presents a table with different type of algorithms treated. For each case, there is no distinction regarding the technical objectives fulfilled by each row on the table (thus algorithm family). The technical objectives are the same disregarding this differentiation.

7.1.1 Class FAU Security Audit

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

FAU_SAS.1 Audit storage

Hierarchical to: No other components
Dependencies: No dependencies

FAU_SAS.1.1 The TSF shall provide the Manufacturer[2] with the capability to store the IC Identification Data[3] in the audit records.

[2] [assignment: authorized users]
[3] [assignment: list of audit information]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7.1.2 Class Cryptographic Support (FCS)

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

FCS_CKM.1 /AA Cryptographic key generation for AA

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 /AA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Refer to Table 3 column "Algorithm"*[4] and specified cryptographic key sizes *Refer to Table 3 column "key size"*[5] that meet the following: *Refer to Table 3 column "Standard"*[6]

Algorithm Type	Algorithm	Key size	Standard
RSA	**RSA CRT Key generation**	**1024, 1280, 1536 and 2048 bits**	**none (generation of random numbers and Miller-Rabin primality testing)**
ECC	**ECC Key generation**	**160, 192, 224, 256, 320, 384, 512 and 521 bits**	**None**

Table 3: FCS_CKM.1/AA iteration explanation

FCS_CKM.1 /Session Cryptographic key generation – Generation of Document Basic Access Keys by the TOE

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 /Session The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[7] and specified cryptographic key sizes 112 bits[8] that meet the following: [ICAO-9303], normative appendix 5[9]

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2).

[4] [assignment: cryptographic key generation algorithm]
[5] [assignment: cryptographic key sizes]
[6] [assignment: list of standards]
[7] [assignment: cryptographic key generation algorithm]
[8] [assignment: cryptographic key sizes]
[9] [assignment: list of standards]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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 *Secure erasing by overwriting session keys by random value*[10] that meets the following: *none*[11].

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation by MRTD

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/ SHA The TSF shall perform hashing[12] in accordance with a specified cryptographic algorithm SHA-1, *SHA-224, SHA-256, SHA-384 and SHA-512*[13] and cryptographic key sizes none[14] that meet the following: *FIPS 180-2*[15].

FCS_COP.1/ENC Cryptographic operation – Encryption / Decryption TDES

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/ ENC The TSF shall perform secure messaging (BAC) – encryption and decryption[16] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[17] and cryptographic key sizes 112 bits[18] that meet the following: FIPS 46-3 [FIPS46-3] and [ICAO-9303]; normative appendix 5, A5.3[19].

[10] [assignment: list of cryptographic key destruction method]
[11] [assignment: list of standards]
[12] [assignment: list of cryptographic operations]
[13] [assignment: cryptographic algorithm]
[14][assignment: cryptographic key sizes]
[15] [assignment: list of standards]
[16] [assignment: list of cryptographic operations]
[17] [assignment: cryptographic algorithm]
[18] [assignment: cryptographic key sizes]
[19] [assignment: list of standards]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

FCS_COP.1/AUTH Cryptographic operation – Authentication

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/ AUTH	The TSF shall perform symmetric authentication – encryption and decryption[20] in accordance with a specified cryptographic algorithm *Triple-DES, AES*[21] and cryptographic key sizes *112 bits for TDES / 128, 192 and 256 bits for AES* [22] that meet the following: *FIPS 46-3 [FIPS46-3], FIPS 197 [FIPS197]*[23].

FCS_COP.1/MAC Cryptographic operation – Retail MAC

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/ MAC	The TSF shall perform secure messaging – message authentication code[24] in accordance with a specified cryptographic algorithm Retail MAC[25] and cryptographic key sizes 112 bits[26] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[27].

[20] [assignment: list of cryptographic operations]
[21] [assignment: cryptographic algorithm]
[22] [assignment: cryptographic key sizes]
[23] [assignment: list of standards]
[24] [assignment: list of cryptographic operations]
[25] [assignment: cryptographic algorithm]
[26] [assignment: cryptographic key sizes]
[27] [assignment: list of standards]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

FCS_COP.1/AA Cryptographic operation – Active Authentication

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]: fulfilled by FCS_CKM.1/AA
FCS_CKM.4 Cryptographic key destruction: not fulfilled, see application note.

FCS_COP.1.1 /AA The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm *Refer to Table 4 column "Algorithm"*[28] and cryptographic key sizes *Refer to Table 4 column "Key size"*[29] that meet the following: *Refer to Table 4 column "Standard"*[30] .

Algorithm type	Algorithm	Key size	Standard
AA_RSA	**RSA (CRT)**	**1024, 1280, 1536, 2048, 3072 and 4096 bits**	**ISO9796-2**
AA_ECDSA	**ECDSA**	**160, 192, 224, 256, 320, 384, 512 and 521**	**[TR-ECC]**

Table 4: FCS_COP.1/AA iteration explanation

Application note:

- The dependency of FCS_COP.1/AA on FCS_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.

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 *RGS [RGS-B1] and [SP 800-90] with seed entropy at least 128 bits*[31].

[28] [assignment: cryptographic key generation algorithm]
[29] [assignment: cryptographic key sizes]
[30] [assignment: list of standards]
[31] [assignment: a defined quality metric]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7.1.3 Class FIA Identification and Authentication

Application note: Table 5 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO-9303] normative appendix 5
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Active Authentication Protocol	FIA_API.1/AA and FIA_UAU.4	ECDSA, 160, 192, 224, 256, 320, 384,512 and 521 bits (cf. FCS_COP.1/AA AA_ECDSA) and RSA CRT, 1024, 1280, 1536, 2048, 3072 and 4096 bits (cf. FCS_COP.1/AA AA_RSA)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	Triple-DES with 112 bit keys and AES with 128, 192 and 256 bit keys (cf. FCS_COP.1/AUTH)

Table 5: Overview on authentication SFR

The TOE shall meet the requirement “Timing of identification (FIA_UID.1)” as specified below (Common Criteria Part 2).

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.

The TOE shall meet the requirement “Timing of authentication (FIA_UAU.1)” as specified below (Common Criteria Part 2).

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow
1. to 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.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4 Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

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 Mechanism based on *Triple-DES, AES*[32][33].

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2).

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide
1. Basic Access Control Authentication Mechanism,
2. Symmetric Authentication Mechanism based on *Triple-DES, AES*[34][35].

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:
1. TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) *the Symmetric Authentication Mechanism with the Personalization Agent Key* ***and Administration Key***.[36]
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.[37]

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

FIA_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism[38].

[32] [selection: Triple-DES, AES or other approved algorithms]
[33] [assignment: identified authentication mechanism(s)]
[34] [selection: Triple-DES, AES]
[35] [assignment: list of multiple authentication mechanisms]
[36] [selection: *the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]*]
[37] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[38] [assignment: *list of conditions under which re-authentication is required*]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1)" as specified below (Common Criteria Part 2).

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *Refer to Table 6 column "Number"* [39]unsuccessful authentication attempts occur related to *Refer to Table 6 column "Authentication events"*[40].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*[41], the TSF shall *Refer to Table 6 column "Actions"*[42].

Number	Authentication events	Actions
3	**Unsuccessful Mutual Authentication command with Administration Key**	**Administration Key blocked**
An administrator configurable positive integer within 1 - 14	**Unsuccessful Mutual Authentication command with Personalization Key**	**Personalization Key blocked**
1	**Unsuccessful Basic Access Control authentication attempt**	**Exponentially increasing time delay before new authentication attempt is possible**

Table 6: FIA_AFL.1 iteration explanation

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended).

FIA_API.1/AA Authentication Proof of Identity – Active Authentication

Hierarchical to: No other components
Dependencies: No dependencies

FIA_API.1.1/AA The TSF shall provide an *Active Authentication Protocol according to [ICAO-9303]*[43] to prove the identity of the *TOE*[44].

Application note: This SFR requires the TOE to implement the Active Authentication Mechanism specified in [ICAO-9303]. The terminal generates a secret then verifies whether the MRTD's chip was able or not to sign it properly using its Active Authentication private key corresponding to the Active Authentication public key (EF.DG15).

[39] [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
[40] [assignment: *list of authentication events*]
[41][selection: *met, surpassed*]
[42] [assignment: *list of actions*]
[43] [assignment: *authentication mechanism*]
[44] [assignment: *authorized user or role*]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7.1.4 Class FDP User Data Protection

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2).

FDP_ACC.1 Subset access control – Basic Access Control

Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the Basic Access Control SFP[45] 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.[46]

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2).

FDP_ACF.1 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 The TSF shall enforce the Basic Access Control SFP[47] to objects based on the following:

1. Subjects:
   a. Personalization Agent**,**
   b. Basic Inspection System
   c. Terminal,
   d. Administration Authority
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[48],

FDP_ACF.1.2 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 **or Administration Authority**,is allowed to write and to 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[49].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[50].

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

[45] [assignment: *access control SFP*]
[46] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[47] [assignment: *access control SFP*]
[48] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[49] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[50] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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.[51]

The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

FDP_UCT.1 Basic data exchange confidentiality - MRTD

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	The TSF shall enforce the Basic Access Control SFP[52] to be able to transmit and receive[53] user data in a manner protected from unauthorised disclosure.

The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2).

FDP_UIT.1 Data exchange integrity - MRTD

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	The TSF shall enforce the Basic Access Control SFP[54] to be able to transmit and receive[55] user data in a manner protected from modification, deletion, insertion and replay[56] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[57] has occurred.

[51] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[52] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[53] [selection*: transmit, receive*]
[54] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[55] [selection*: transmit, receive*]
[56] [selection: *modification, deletion, insertion, replay*]
[57] [selection: *modification, deletion, insertion, replay*]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7.1.5 Class FMT Security Management

Application note: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 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[58].

The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2).

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. **Administration Authority,**
3. Personalization Agent,
4. Basic Inspection System[59].

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

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

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[60]

[58] [assignment: *list of management functions to be provided by the TSF*]
[59] [assignment: *the authorized identified roles*]
[60] [assignment: *Limited capability and availability policy*]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

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.[61]

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization 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[62] the Initialization Data and Pre-personalization Data[63] to the Manufacturer and **the Administration Authority[64].**

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ INI_DIS The TSF shall restrict the ability to disable read access for users[65] to the Initialization Data[66] to the Personalisation Agent **and the Administration Authority**[67].

[61] [assignment: *Limited capability and availability policy*]
[62] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[63] [assignment: *list of TSF data*]
[64] [assignment: *the authorized identified roles*]
[65] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[66] [assignment: *list of TSF data*]
[67] [assignment: the authorized identified roles]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write

Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write[68] the Document Basic Access Keys[69] to the Personalization Agent[70] **and the Administration Authority.**

FMT_MTD.1/AAK Management of TSF data – Active Authentication Private Key

Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ AAK	The TSF shall restrict the ability to **create and load** [71]the **Active Authentication Private Key**[72] to **the Personalization Agent**[73].

FMT_MTD.1/KEY_READ Management of TSF data – Key Read

Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read[74] the 1. Document Basic Access Keys,[75] 2. Personalization Agent Keys, **3. Active Authentication Private Key** **4. Administration Key** to none[76].

[68] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[69] [assignment: list of TSF data]
[70] [assignment: the authorized identified roles]
[71] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[72] [assignment: list of TSF data]
[73] [assignment: the authorized identified roles]
[74] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[75] [assignment: list of TSF data]
[76] [assignment: the authorized identified roles]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7.1.6 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSF testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFRs "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)" together with the SAR "Security architecture description" (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement "TOE Emanation (FPT_EMS.1)" as specified below (Common Criteria Part 2 extended):

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components
Dependencies: Dependencies.

FPT_EMS.1.1 The TOE shall not emit **electromagnetic and current emissions**[77] in excess of **intelligible threshold**[78] enabling access to Personalization Agent Key(s), **Administration Key, Document Basic Access Keys, Active Authenticate Private Keys, EF.COM, EF.SOD, EF.DG1, EF.DG2**[79] and **EF.DG6 to EF.DG16**[80]**.**

FPT_EMS.1.2 The TSF shall ensure any users[81] are unable to use the following interface smart card circuit contacts[82] to gain access to Personalization Agent Key(s), **Administration Key, Document Basic Access Keys, Active Authenticate Private Keys, EF.COM, EF.SOD, EF.DG1, EF.DG2**[83] and **EF.DG6 to EF.DG16**[84]**.**

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components
Dependencies: 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[85].

[77] [assignment: types of emissions]
[78] [assignment: specified limits]
[79] [assignment: list of types of TSF data]
[80] [assignment: list of types of user data]
[81] [assignment: type of users]
[82] [assignment: type of connection]
[83] [assignment: list of types of TSF data]
[84] [assignment: list of types of user data]
[85] [assignment: list of types of failures in the TSF]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

FPT_TST.1 TSF testing

Hierarchical to: No other components
Dependencies: Dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up, periodically during normal operation, after cryptographic computation, before any use or update of TSF data**[86] to demonstrate the correct operation of the TSF[87].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data[88].

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

Application Note: The MRTD's chip uses state-of-the-art smart card technology, therefore it will run the some self tests at the request of an authorized user and some self tests automatically (cf [ST-IC]). E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 is executed during initial start-up by the user Manufacturer in the life phase 'Manufacturing'. Other self tests automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation of a integrity check value as soon as data is accessed, to check calculation with a private RSA CRT key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks, to check the RNG of the chip for failures in accordance to the chip manufacturer guidance.
.

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components
Dependencies: Dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[89] to the TSF[90] by responding automatically such that the SFRs are always enforced.

[86] [selection: during initial start-up,periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]
[87] [selection: [assignment: parts of TSF], the TSF]
[88] [selection: [assignment: parts of TSF], TSF data]
[89] [assignment: physical tampering scenarios]
[90] [assignment: list of TSF devices/elements]

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The SAR 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_TAT.2, ATE_DPT.3 and ALC_DVS.2.

7.3 SECURITY REQUIREMENTS RATIONALE

7.3.1 Security Functional Requirements Rationale

The rationale in this paragraph comes from [PP-MRTD-BAC] §6.3.1. Additions due to Active Authentication are shaded.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Activ_Auth_Proof	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				X					
FCS_CKM.1 /Session	X	X	X						
FCS_CKM.1 /AA					X				
FCS_CKM.4	X		X						
FCS_COP.1/SHA	X	X	X						
FCS_COP.1/ENC	X	X	X						
FCS_COP.1/AUTH	X	X							
FCS_COP.1/MAC	X	X	X						
FCS_COP.1/AA					X				
FCS_RND.1	X	X	X						
FIA_UID.1			X	X					
FIA_AFL.1			X	X					
FIA_UAU.1			X	X					
FIA_UAU.4	X	X	X						
FIA_UAU.5	X	X	X						
FIA_UAU.6	X	X	X						
FIA_API.1/AA					X				
FDP_ACC.1	X	X	X						
FDP_ACF.1	X	X	X						
FDP_UCT.1	X	X	X						
FDP_UIT.1	X	X	X						
FMT_SMF.1	X	X	X						
FMT_SMR.1	X	X	X						
FMT_LIM.1									X
FMT_LIM.2									X
FMT_MTD.1/INI_ENA				X					
FMT_MTD.1/INI_DIS				X					
FMT_MTD.1/KEY_WRITE	X	X	X						
FMT_MTD.1/KEY_READ	X	X	X						
FMT_MTD.1/AAK		X	X		X				
FPT_EMS.1	X					X			
FPT_TST.1						X		X	
FPT_FLS.1	X					X		X	

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Activ_Auth_Proof	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FPT_PHP.3	X					X	X		

Table 7: Security functional requirement rationale

The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent or the Administration Authority is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once (please refer to [AGD_USR] for specific TEST mode used for iterative development of the personalization process).
The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1/Session, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [19] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).
In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/Session, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.
The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.
The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/Session, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode.
The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.
The SFR FMT_MTD.1/AAK and FMT_MTD.1/KEY_READ requires that the Active Authentication Key cannot be written unauthorized or read afterwards.

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).
The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1/Session, FCS_CKM.4, FCS_COP.1/SHA and
FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.
Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.
The SFR FMT_MTD.1/AAK and FMT_MTD.1/KEY_READ requires that the Active Authentication Key cannot be written unauthorized or read afterwards.

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

The security objective **OT.Activ_Auth_Proof “**Proof of MRTD’s chip authenticity through AA” addresses the verification of the chip's authenticity. This done by the SFR FIA_API.1/AA which authenticates the chip, using cryptographic operations covered by the SFR FCS_COP.1/AA.
The Active Authentication Protocol is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAK and FMT_MTD.1/KEY_READ. This confidential private key is generated by the TOE cryptographic operation done by FCS_CKM.1/AA.

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

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

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

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

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

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

7.3.2 Dependency Rationale

The rationale in this paragraph comes from [PP-MRTD-BAC] §6.3.2. Additions due to Active Authentication are shaded.

SFR	Dependencies	Support of the dependencies
FAU_SAS.1	No dependencies	
FCS_CKM.1/Session	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_CKM.4
FCS_CKM.1/AA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/AA justification 5 for non-satisfied dependencies,
FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/Session
FCS_COP.1/SHA	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	justification 1 for non-satisfied dependencies,
FCS_COP.1/ENC	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/Session FCS_CKM.4
FCS_COP.1/AUTH	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	justification 2 for non-satisfied dependencies,
FCS_COP.1/MAC	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/Session FCS_CKM.4
FCS_COP.1/AA	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/AA FCS_CKM.4
FCS_RND.1	No dependencies	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.4	No dependencies	
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_API.1/AA	No dependencies	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, justification 3 for non-satisfied dependencies,
FDP_UCT.1	[FTP_ITC.1, or FTP_TRP.1], [FDP_IFC.1 or FDP_ACC.1]	justification 4 for non-satisfied dependencies, FDP_ACC.1

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

SFR	Dependencies	Support of the dependencies
FDP_UIT.1	[FTP_ITC.1, or FTP_TRP.1], [FDP_IFC.1 or FDP_ACC.1]	justification 4 for non-satisfied dependencies, FDP_ACC.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/AAK	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FPT_EMS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_PHP.3	No dependencies	

Table 8: Security functional requirement dependencies

Justification for non-satisfied dependencies between the SFR for TOE:

1. The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1/Session), nor an import (FDP_ITC.1/2) is necessary.
2. The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1/Session or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.
3. The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.
4. The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.
5. The SFR FCS_COP.1/AA uses the asymmetric Key permanently stored during the Personalization process. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

7.3.3 Security Assurance Requirements Rationale

Cf [PP-MRTD-BAC] §6.3.3 or also explain:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL4)		
ALC_DVS.2	No dependencies	
	Regarding the secure handling of the MRTD's raw materials, it provides higher assurance of the security of the manufacturing and development.	
ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2, ATE_DPT.3	No dependencies	
	Required due to sensitivity of ID documents to reach a higher level of assurance.	

7.3.4 Security Requirements – Mutual support and internal consistency

Cf [PP-MRTD-BAC] §6.3.4

7.3.5 Compatibility between SFR of [ST-BAC] and [ST-IC]

FAU_SAS.1 is included in FAU_SAS.1 of [ST-IC].
FCS_RND.1 is supported by FCS_RNG.1 of [ST-IC].
FCS_COP.1/SHA is supported by FCS_COP.1/SHA of [ST-IC]
FCS_COP.1/ENC, FCS_COP.1/MAC are supported by FCS_COP.1/TDES of [ST-IC].
FCS_COP.1/AUTH is supported by FCS_COP.1/TDES and FCS_COP.1/AES of [ST-IC].
FPT_EMS.1 and FPT_PHP.3 are included in FPT_PHP.3 of [ST-IC].
FPT_FLS.1 is included in FPT_FLS.1 of [ST-IC].

FCS_CKM.1/Session,FCS_CKM.1/AA, FCS_COP.1/AA, FCS_CKM.4, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1/AA, FIA_AFL.1, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FMT_MTD.1/AAK and FPT_TST.1 are specific to [ST-BAC] and they do not conflict with [ST-IC].

We can therefore conclude that the SFR of [ST-BAC] and [ST-IC] are consistent.

8. TOE SUMMARY SPECIFICATION

8.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the eTravel Next 1.0 and by the chip.

8.1.1 TSFs provided by the eTravel Next 1.0 Software

SF	Description
SF.REL	Protection of data
SF.AC	Access control
SF.SYM_AUTH	Symmetric authentication
SF.SM	Secure messaging
SF.AA	Active Authentication

Table 9: Security Functions provided by the eTravel Next 1.0 Software

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

The SF.REL function provides the protection of data on the TOE. It encompasses:

- physical protection of the TOE as defined in **FPT_PHP.3**, **FPT_EMS.1** , **FPT_FLS.1**,
- the test mechanisms as defined in **FPT_TST.1**,
- protection against misuse of tests as defined in **FMT_LIM.1** and **FMT_LIM.2**,

The SF.AC function provides the access control of the TOE. It encompasses:

- the access control by the terminal as defined in **FDP_ACC.1** and **FDP_ACF.1**,
- the access control to specific data as defined in **FAU_SAS.1**, **FMT_MTD.1/INI_ENA**, **FMT_MTD.1/INI_DIS**, **FMT_MTD.1/KEY_WRITE**, **FMT_MTD.1/KEY_READ**,
- the role management as defined in **FMT_SRM.1**,
- the management functions linked to the different states of the TOE as defined in **FMT_SMF.1**

The SF.SYM_AUTH function provides the symmetric authentication functions to the TOE. It encompasses:

- the identification and authentication as defined in **FIA_AFL.1, FIA_UID.1, FIA_UAU.1**, **FIA_UAU.4**, **FIA_UAU.5**, and **FIA_UAU.6**,

The SF.SM function provides the secure messaging of the TOE. It encompasses:

- the secure transfer of data through SM as defined in **FDP_UCT.1** and **FDP_UIT.1**,
- the cryptographic mechanisms used for the authentication and the SM, as defined in **FCS_CKM.1/Session**, **FCS_COP.1/SHA**, **FCS_COP.1/ENC**, **FCS_COP.1/AUTH**, **FCS_COP.1/MAC**, **FIA_AFL.1** and **FCS_RND.1**. Some cryptographic mechanisms are used for both authentication and secure messaging. For convenience, they are grouped in this function.
- the erasure of session keys as defined in **FCS_CKM.4**

The SF.AA function provides the active authentication. It encompasses:

- the AA protocol itself as defined in **FIA_API.1/AA**,
- the AA cryptographic algorithm as defined in **FCS_COP.1/AA**,
- the generation and input of AA keys, as defined in **FCS_CKM.1/AA** and **FMT_MTD.1/AAK**, .

8.1.2 TSFs provided by the Infineon M7892 chip

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR-IC]. The IC and its primary embedded software have been evaluated at level EAL 6+.

SF	Description
SF_DPM	Device phase management
SF_PS	Protection against snooping
SF_PMA	Protection against modifying attacks
SF_PLA	Protection against logical attacks
SF_CS	Cryptographic support

Table 10: Security Functions provided by the Infineon M7892 chip

These SF are described in [ST-IC].

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

9. RATIONALES

9.1 TOE SUMMARY SPECIFICATION RATIONALE

9.1.1 TOE security functions rationale

	SF.REL	SF.AC	SF.SYM_AUT	SF.SM	SF.AA	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FAU_SAS.1		X				X				
FCS_CKM.1/Session				X						X
FCS_CKM.1/AA					X					X
FCS_CKM.4				X						
FCS_COP.1/SHA				X						
FCS_COP.1/ENC				X						X
FCS_COP.1/AUTH				X						X
FCS_COP.1/MAC				X						X
FCS_COP.1/AA					X					X
FCS_RND.1				X						X
FIA_API.1/AA					X					
FIA_AFL.1			X							
FIA_UID.1			X							
FIA_UAU.1			X							
FIA_UAU.4			X							
FIA_UAU.5			X							
FIA_UAU.6			X							
FDP_ACC.1		X								
FDP_ACF.1		X								
FDP_UCT.1				X						
FDP_UIT.1				X						
FMT_LIM.1	X									
FMT_LIM.2	X									
FMT_MTD.1/INI_ENA		X								
FMT_MTD.1/INI_DIS		X								
FMT_MTD.1/KEY_WRITE		X								
FMT_MTD.1/KEY_READ		X								
FMT_MTD.1/AAK					X					
FMT_SMF.1		X								
FMT_SMR.1		X								
FPT_EMS.1	X						X			
FPT_FLS.1	X						X	X	X	
FPT_PHP.3	X						X	X	X	
FPT_TST.1	X							X		

Table 11: Rationale table of functional requirements and security functions

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

10. ACRONYMS AND GLOSSARY

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

Acr.	Term	Definition
AA	Active Authentication	Security mechanism defined in [PKI] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
	Application note [PP-MRTD-EAC]	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
	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
BAC	Basic Access Control	Security mechanism defined in [PKI] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
BIS	Basic Inspection System	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
	Biographical data (biodata)	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [SS]
	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. [SS]
CSCA	Country Signing Certification Authority	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
CPLCD	Card Production Life Cycle Data	The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in EEPROM. These data are available by executing a dedicated command
CVCA	Country Verifying Certification Authority	The Country Verifying Certification Authority enforces the privacy policy of the issuing Country or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems.
DH	Diffie-Hellman Key Agreement Algorithm	Algorithm for Chip Authentication protocol
DV	Document Verifier	The Document Verifier enforces the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The DV manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the Issuing State or Organization in form of the Document Verifier Certificates.
EC-DH	Elliptic Curve Diffie-Hellman Key Agreement Algorithm	Algorithm for Chip Authentication protocol
	Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [PKI]. 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.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

SOD	Document Security Object	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). [PKI]
	Eavesdropper	A threat agent with moderate 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. [BIO]
EAC	Extended Access Control	Security mechanism identified in [PKI] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
EIS	Extended Inspection System	The EIS in addition to the General Inspection System (GIS) (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.
	Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [SS]
GIS	General Inspection System	The GIS is a Basic Inspection System (BIS) which implements additional the Chip Authentication Mechanism.
	Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [BIO]
	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.
	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. [SS]
	Improperly	A person who travels, or attempts to travel with: (a) an expired travel
	Documented person	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. [BIO]
	Initialisation 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. [BIO]
IS	Inspection system	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

IC	Integrated circuit	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]
LDS	Logical Data Structure	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 (LDS) 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 biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (4) the other data according to LDS (EF.DG5 to EF.DG16).
	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).
MRTD	Machine readable travel document	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]
MRV	Machine readable visa	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]
MRZ	Machine Readable Zone	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. [SS]
	MRTD administrator	The Issuing State or Organization which is allowed to perform administrative commands (update data of the MRTD application, invalidation of the application) in the phase 4 Operational Use.
	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 and EF.DG16), - 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.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

	MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and ICAOT, [10], p. 14. programmed according to the Logical Data Structure as specified by ICAOT, [10], 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	verification of the digital signature of the Document Security Object comparison 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. [SS]
	Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
	Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
	Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT 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/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.
	Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to): biographical data, data of the machine-readable zone, photographic image and other data.
	Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
	Pre – personalized MRTD's chip	MRTD's chip equipped with pre-personalization data.
PIS	Primary Inspection System	A 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 MRTD holder 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.

Content of this document shall not be modified or partially reused without prior written consent of Gemalto

	secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [SS]
	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. [BIO]
	traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
	TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
	Unpersonalized MRTD	MRTD material prepared to produce an personalized MRTD containing an initialised and pre-personalized MRTD's chip.
	User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).
	Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. [BIO]
	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.

END OF DOCUMENT

Content of this document shall not be modified or partially reused without prior written consent of Gemalto