eTravel 3.1 EAC on BAC on MultiApp V5.1

Common Criteria / ISO 15408 Security Target – Public version EAL5+

Version 1.2 – 04th October 2023

CONTENT

FIGURES

TABLES

1. SECURITYTARGET INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title :	MultiApp V5.1 eTravel 3.1 EAC on BAC Security Target
Version :	1.2
ST Reference :	D1569589_LITE
Origin :	THALES
IT Security Evaluation scheme :	LETI CESTI
IT Security Certification scheme :	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 TOE REFERENCE

The product is available in two configurations:

- Configuration 1: TOE based on the IC AQUARIUS_BA_09- AQUARIUS_v1 called "revision B"
- Configuration 2: TOE based on the IC AQUARIUS_CA_09- AQUARIUS_v2 called "revision C"

Product Name :	eTravel 3.1 (MultiApp V5.1)
Security Controllers :	For the configuration 1 (Revision B): AQUARIUS_BA_09 (Thales DIS France SAS) For the configuration 2 (Revision C): AQUARIUS_CA_09 (Thales DIS France SAS)
TOE Name :	eTravel 3.1 EAC/BAC on MultiApp V5.1
TOE version :	For configuration 1 (revision B): eTravel 3.1.0.0(*) For configuration 2 (Revision C): eTravel 3.1.0.1(*)
TOE documentation :	Guidance [AGD]
Composition elements:	
IC TOE identifier:	For the configuration 1 (Revision B): AQUARIUS_BA_09 - AQUARIUS_v1 For the configuration 2 (Revision C): AQUARIUS_CA_09 - AQUARIUS_v2
IC TOE Version:	For the configuration 1 (Revision B): Hardware revision: B For the configuration 2 (Revision C): Hardware revision: C For both configurations: Platform ROM Firmware Revision: A Platform FLASH Firmware Revision: 09 ➢ *BIOS: Version 1.0-911* ➢ *Loader: Version 2.2*

(*) The TOE version format is 3.1.x.y where x.y are the application revision defined in the CPLC for eTravel.

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

The TOE and the product differ, as further explained in §2.1 TOE :

- The TOE is the eTravel 3.1 application on MultiApp V5.1.
- The MultiApp V5.1 product also includes other applets in ROM.

1.3 TOE Identification

The TOE identification is provided by the Card Production Life Cycle Data (CPLC Data) of the TOE. These data are available by executing a dedicated command.

The TOE identification is provided by a dedicated command GET CARD DATA with the next TAG: 9F7F

The response of the GET CARD DATA is described below. In orange the field of the TOE identification

Name	Values	Description
IC Fabricator	'1290'	Chip Manufacturer – (THALES DIS FRANCE SAS)
IC Type	'0013'	Chip Type
Operating System Identifier	'B0856A'	Thales Family Name + Thales OS name + Thales Product Name
Configuration	'01'	Not relevant for identification
Application revision	'0000'	Major & minor version of the revision (0.0)
IC Fabrication Date		Not relevant for identification
IC Serial Number		
IC Batch Identifier		
IC Module Fabricator		
IC Module Packaging Date		
ICC Manufacturer		
IC Embedding Date		
IC Pre-personalizer		
IC Pre-personalization Date		
IC Pre-personalization Equipment		
IC Personalizer		
IC Personalization Date		
IC Personalization Equipment Identifier		

The identification of the IC type is provided by the Platform.
To read this information, it is needed to make a PACE authentication, a Select ISD and to read the tag 010B as describe in the [STs-Platform]. The command GET CARD DATA can be found in the [AGD-Platform].

Index	Description	IC Revision B Value (Previous)	IC Revision C Value	Part of TOE the identification
0	PRODUCT	0x09	0x09	No
1	HW_REV	0x42	0x43	Yes
2	Not relevant for identification			No
…				No
15				No

1.4 Security Target overview

This Security Target defines the security objectives and requirements for the contact/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 Extended Access Control as well as the advanced authentication mechanisms Chip Authentication and Active Authentication.

The Security Target is based on Protection Profile *Machine Readable Travel Document with "ICAO Application", Extended Access Control* [PP-MRTD-EAC].

The Security Target 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.

1.5 REFERENCES

1.5.1 External References

[CC]	**Common Criteria references**
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation Evaluation Methodology CCMB-2017-04-004, version 3.1 rev 5, April 2017
[JIL_CPE]	Joint Interpretation Library: Composite product evaluation for Smart Cards and similar devices, Version 1.5.1 May 2018
[TDFS]	**THALES DIS FRANCE SAS References**
[ST-AQU-IC]	Security Target for AQUARIUS (Microcontroller AQUARIUS_BA_09 & CA_09 - AQUARIUS_v2) Ref: AQUARIUS_ST Revision: 1.0 – 10/03/2023
[CR-IC]	Certification Report, CERTIFICAT ANSSI-CC-2023/01-M01 AQUARIUS_BA_09 & CA_09 - AQUARIUS_v2 EAL6 Augmenté (ASE_TSS.2, ALC_FLR.2) Date : 21/06/2023 conforme au profil de protection : Security IC Platform Protection Profile with Augmentation Packages, version 1.0 certifié BSI-CC-PP-0084-2014 le 19 février 2014
[ISO]	**ISO references**
[ISO7816]	*ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange*, FDIS2004
[ISO9796-2]	*ISO/IEC 9796-2:2010: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms,* Third edition 2010-12-15
[ISO9797-1]	*ISO/IEC 9797-1:2011: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,* Second edition 2011-03-01
[ICAO-9303]	9303 ICAO Machine Readable Travel Document 7th edition, 2015 Part 1-12
[PP]	**Protection profiles**
[PP-IC-0084]	Security IC Platform Protection Profile with augmentation Packages– BSI-CC-PP-0084-2014
[PP-MRTD-EAC]	Protection Profile, Machine Readable Travel Document with “ICAO Application”, Extended Access Control, version 1.10, 25 mars 2009. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-PP-0056-2009.
[PP-MRTD-SAC]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.01, 22 juillet 2014. Certified and maintained by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-CC-PP-0068-V2-2011-MA-01.
[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.
[EXTERNAL]	**Other External references**

[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]	Technical Guideline – TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26.02.2015
[ICAO-TR-SAC]	MRTD Technical report - Supplemental Access Control for Machine Readable Travel Documents Version - 1.01 Date – November 11, 2010
[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
[RGS-B1]	ANSSI, « Référentiel général de sécurité », https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf Annexe B1 Mécanismes cryptographiques, règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques; version 2.0.4, 2020-01-01
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PKI]	9303 ICAO Machine Readable Travel Document 7th edition, 2015 Part 11-12
[RGS-B1]	Référentiel Général de sécurité version 2 Annexe B1 Mécanismes cryptographiques, règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques; version 2.0.3 du 21 février 2014
[AIS20/31]	A proposal for : Functionality classes for random number generators Version 2.0, 18/09/2011
[SP 800-90]	NIST Special Publication 800-90A, Revision 1, Recommendation for the Random Number Generation Using Deterministic Random Bit Generators, June 2015

1.5.2 Internal References

[STs]	Security Targets
[ST-BAC]	D1569591, BAC Security Target - MultiApp V5.1
[ST-EAC]	D1569589, eTravel 3.1 EAC on BAC Security Target
[ST-JCS]	D1572544, MultiApp V5.1: JCS Security Target
[ST-GP]	D1569436, MultiApp V5.1: GP-SE Security Target
[STs-Platform]	[ST-JCS] & [ST-GP]
[AGD]	Guidance Documentation
[AGD-Ref]	D1584821 – D.2 - eTravel 3.x Reference Manual
[AGD-GDP]	D1390286R - Global Dispatcher Personalization Applet
[AGD-OPE]	D1582202 - MultiApp V5.1: AGD OPE document - eTravel v3.1
[AGD-PRE]	D1574817 - MultiApp V5.1: AGD PRE document - eTravel v3.1

2. TOE OVERVIEW

2.1 TOE DESCRIPTION

The TOE is the module designed to be the core of an MRTD passport. The TOE is a contact/contactless 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 Target of Evaluation (TOE) is the contact/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 (BAC) according to the ICAO document [PKI]
- the Active Authentication (AA) mechanism according to the ICAO document [ICAO-9303]
- the Extended Access Control according to the BSI document [TR-EAC]

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

The TOE comprises of 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 eTravel 3.1 application on MultiApp V5.1 Open Platform.
- The GDP Applet (optional)
- the associated guidance documentation.
- A cryptographic library developed by Thales

The MultiApp V5.1 is an open platform. see [STs-Platform].

TOE Delivery:

The TOE can be delivered under 2 configurations:

- ✓ The configuration called "Standalone" meaning the eTravel 3.1 is the only applet selectable on the platform (GP221 "Final application" privilege).
- ✓ The configuration called "Open" meaning eTravel 3.1 is selectable among other applets on the platform.

The TOE is delivered to the Personalization Agent with data and guidance documentation in order to perform the personalization of the product. In addition, the Personalization Key is delivered from the MRTD Manufacturer to the Personalization Agent. The Personalization Key is generated on the Manufacturing Site and transmitted to the Personalization Agent through a secured method (Key Ceremony involving Security Agents on a dedicated secure environment with KMS devices). Depending on customer needs and preferences, the Personalization Key could also be generated on the Personalization Agent side (dedicated secure environment with KMS devices) and transmitted to the Manufacturing site through a secure method (Key Ceremony involving Security Agents) in order to be integrated to the TOE.

2.2 TOE BOUNDARIES

The eTravel 3.1 EAC/BAC on MultiApp V5.1 Embedded Software (ES) is located in the flash code area.

The figure below gives a description of the TOE and its boundaries (red dash line)

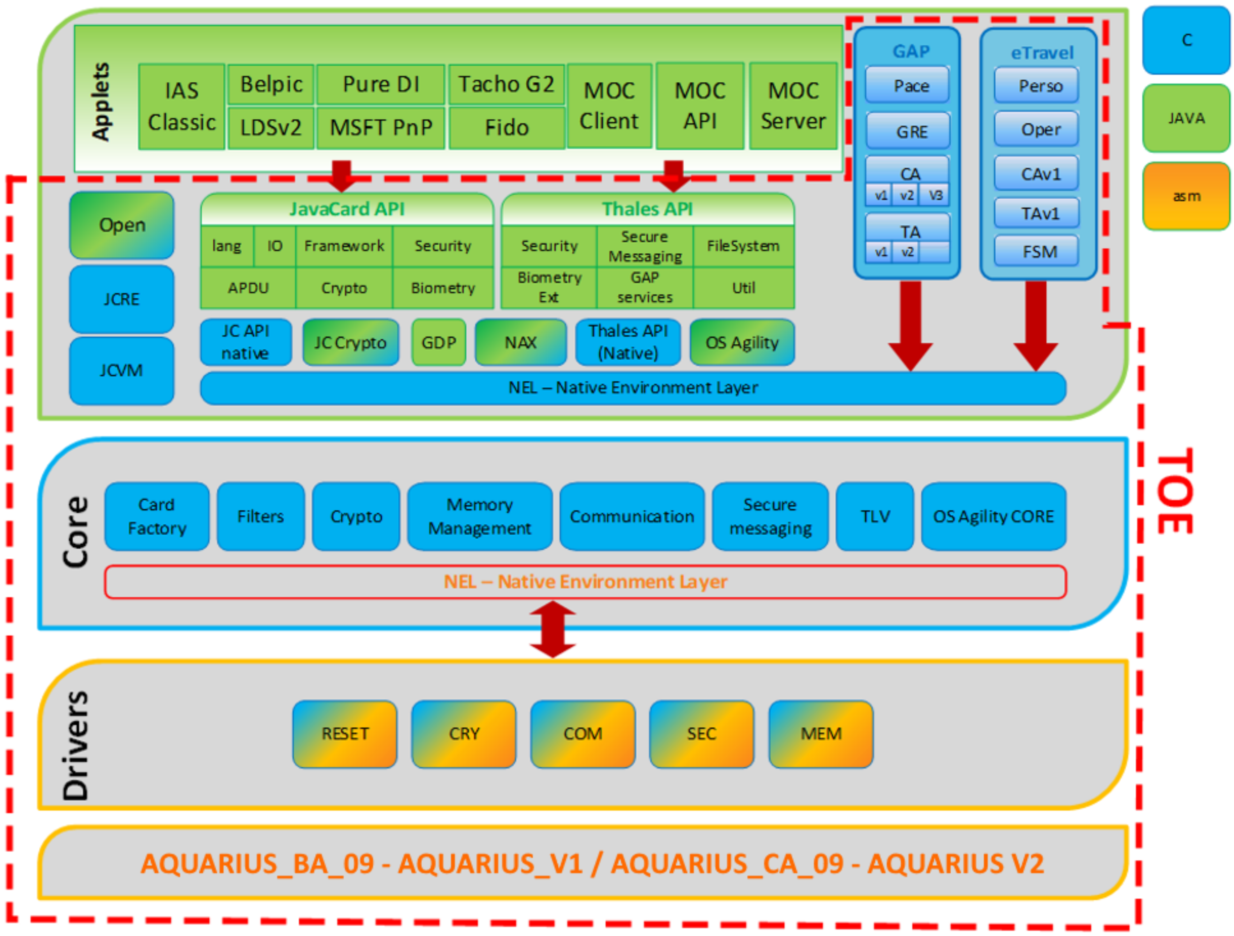


Figure 1: TOE Boundaries

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 traveller presents an 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 traveller is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD.
The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. 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
  (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 biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,
(4) the other data according to LDS (EF.DG5 to EF.DG16) and
(5) the Document security object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO-9303]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of 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 Extended Access Control Mechanism. This security target addresses the Chip Authentication described in [TR-EAC] as an alternative to the Active Authentication stated in [ICAO-9303].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless, this is not explicitly covered by this ST as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfil the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP-BAC-MRTD]. Due to the fact that [PP-BAC-MRTD] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has been evaluated and certified separately according to [ST-BAC], claiming [PP-BAC-MRTD].
For BAC, the inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO-9303], normative appendix 5.

The security target requires the TOE to implement the Chip Authentication defined in [TR-EAC]. The Chip Authentication prevents data traces described in [ICAO-9303], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

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

The security target also requires the TOE to implement Active Authentication as defined in [ICAO-9303].

Keys for Chip authentication and Active Authentication can be generated in the card or loaded into it. These operations take place at personalization time.

2.4 OS Update concept

The eTravel 3.1 product embeds an optional functionality to update the embedded software when it is in operation on the field. This functionality of Embedded Software update is also named OS Agility and it is consistent with [JIL_CPE].

The mechanism will allow to correct product issues or to add a feature requested by issuer when the product is already deployed. The updates are done through a dedicated module (OS-Agility) dealing with a set of update instructions received from trusted environment.
The update instructions are packaged into a block protected in confidentiality and integrity by keys known only by Thales DIS. The block can be transmitted and executed by the TOE only after a successful authentication done with keys only known by the issuer. With such features, Thales DIS is able to load some contents only with the consent of the issuer and the issuer also cannot load a content without the consent of Thales DIS.

Prior to the execution of the instructions of the patch, some prerequisites are verified to confirm ability to perform the correct execution of the instructions. At the end of the execution, the traceability elements are also updated to allow a complete identification of the product (platform version and current patch version). The patch loading mechanism ensures also the atomicity of the updates with change in identification of the TOE.

2.5 TOE Life-cycle

2.5.1 Actors

Actors	Identification
Integrated Circuit (IC) Developer	THALES DIS FRANCE SAS
Embedded Software Developer (Also named OS developer for the phase 1 of the Life cycle)	Thales DIS (See [ALC-DVS] for details)
Integrated Circuit (IC) Manufacturer	THALES DIS FRANCE SAS
Module Manufacturer	THALES (when it is done before the TOE delivery)
Form factor Manufacturer (optional)	THALES (when it is done before the TOE delivery) It can be also an accredited company or the SC Issuer after the TOE delivery
Card manufacturer (Initializer/Pre-personalizer)	THALES (See [ALC-DVS] for details)
Personalization Agent (Personalizer)	The agent who is acting on the behalf of the Issuer (e.g. issuing State or Organization) and personalize the TOE and applicative data (e.g. MRTD for the holder) by activities establishing the identity of the user (e.g. holder with biographic data).
OS Update loader	Agent who is acting on the behalf of the issuer to load the OS patch on the card
Issuer	The Issuer is the actual owner of the SE. As such, no OS Update operation shall be made without his consent. This concept has already been introduced in the SE PP.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.

Table 1: Identification of the actors

2.5.2 TOE Life Cycle

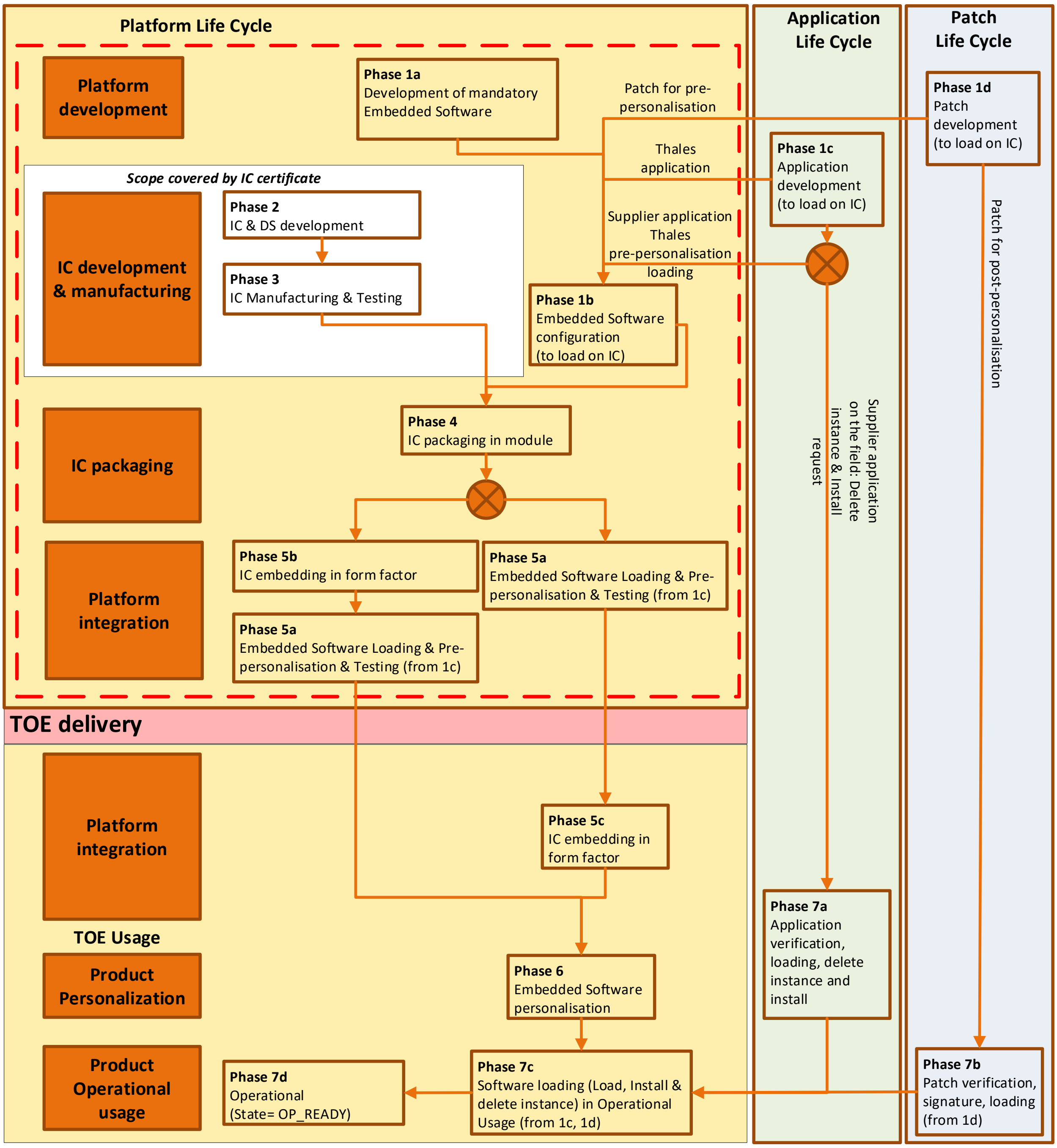


Figure 2: Manufacturing phases description

The Life cycle is described on the figure hereunder:

Phase	Description / comments		Who	Where
1	MAV5.1 platform development	Platform development & tests (1.a)	**Thales** R&D team SL Crypto team - secure environment -	Thales Development site (see §2.5.4)
	Thales MRTD application development	- MRTD Applet Development (1.c) - Generation of principal HEX, mapping description - Script generation for initialization and pre-personalization - Applet tests	**Thales** R&D team - secure environment -	Thales Development site (see §2.5.4)
	Patch development	- Patch Development (1.d) - Patch tests	**Thales** R&D team - secure environment -	Thales Development site (see §2.5.4)
	PSE team	- Platform configuration (1.b) - Script development	**Thales PSE team**	Thales manufacturing site (see §2.5.4)
2	IC development	Integrated circuits development	**Thales DIS FRANCE SAS** - Secure environment -	Thales DIS FRANCE SAS development site(s)
3	IC manufacturing & Testing	Manufacturing of virgin integrated circuits embedding the Thales DIS FRANCE SAS flash loader, and protected by a dedicated transport key.	**Thales DIS FRANCE SAS** - Secure environment -	Thales DIS FRANCE SAS development site(s)
4	SC manufacturing: IC packaging & Embedding, also called “assembly”	- IC packaging & testing	**Thales** Production teams - Secure environment -	Thales manufacturing site (see §2.5.4)
5.a	Initialization / Pre-personalization	Loading of the Thales software (platform and applets on top based on script generated)	**Thales** Production teams - Secure environment -	Thales manufacturing site (see §2.5.4)
5.b	Embedding	Put the module on a dedicated form factor (Card, inlay MFF2, other…)		
5c	Embedding	Put the module on a dedicated form factor (Card, inlay MFF2, other…)	SC Issuer or another accredited company	SC Personalizer or Accredited company site
6	SC Personalization	Creation of files and loading of end-user data	SC Issuer or Another accredited company	SC Personalizer or Accredited company site
7	End-usage	Application verification before loading (7.a)	SC Issuer	Field
		Application Loading (Load, Install and delete instance capabilities) (7.c)	SC Issuer	Field
		Patch verification before loading (Signature) (7.b)	Thales	Field
		Patch update (7.b)	Thales	Field
		End-usage for cardholder (7.d)	Cardholder	Field

Figure 3: Life Cycle description

Remark 1: Initialization & pre-personalization operation could be done on module or on other form factor. The form factor does not affect the TOE security.

Remark 2: For initialization/pre-personalization IC flash loader could be used based on the IC manufacturer recommendation.

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [PP-IC-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 MRTD application and the guidance documentation associated with these TOE components.
As a result a flash mask is generated with initialisation and pre-personalisation scripts.

Phase 2 “Manufacturing”:

Step3) In a first step the IC manufacturer produce virgin chip with IC Identification Data and the flash loader software. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.
(Step4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book
(Step5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD’s chips with pre-personalization Data.
The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 “Personalization of the MRTD”:

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

The signing of the Document security object by the Document signer [5] 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 chip by the traveller and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

The TOE can be updated by agent acting on the behalf of the issuer to load the OS patch on the TOE under control of Thales DIS and issuer.

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.
As a summary description of how the parts of the TOE are delivered to the final customer, the eTravel 3.1 on MultiApp V5.1 application is delivered mainly in form of a smart card or inlay. The form factor is packaged on Thales’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 Thales’s Technical representative.

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

According to [TR-EAC-1], TOE is able to perform its claimed security features when it communicates with a terminal or an Inspection System using a PCD (Proximity Coupling Device) with a RF (Radio Frequency) reading module and an antenna. It is used for the wireless communication with the electronic identity document's chip in order to establish a connection based on the [ISO/IEC 14443] protocol and optionally [ISO/IEC 7816] protocol.

TOE security features of MRTD application are accessible only for devices having privileges to perform MRTD sensitive operations.

TOE security features of personalization application are accessible only for devices having privileges to perform such personalization operations.

TOE security features of OS update are accessible only for devices having privileges to perform loading and activation of additional code.

2.5.4 TOE Delivery

The TOE is delivered as a whole package with the Platform MultiApp V5.1. There is no distinction between the delivery of the platform MultiApp v5.1 and this TOE.

Regarding the documentation to be delivered, a part from the one described on section 2.6.1.4 of the platform Security Target [ST-JCS], and section 2.6.2.2 of the platform Security Target [ST-GP], the documentation found on [AGD] accompanies this TOE.

The documentation is delivered in form of electronic documents (*.pdf) by Thales's Technical representative via a secure file sharing platform download action.

Item type	Item	Reference/Version	Form of delivery
Document	eTravel 3.x Reference Manual	D1584821 – D.2 May 9th, 2023	Electronic document via secure file download
Document	AGD PRE document - eTravel v3.1	D1574817, Rev 1.2 11/05/2023	Electronic document via secure file download
Document	AGD OPE document - eTravel v3.1	D1582202, Rev 1.211/05/2023	Electronic document via secure file download
Document	Global Dispatcher Personalization Applet	D1390286R November 4th, 2022	Electronic document via secure file download

2.5.5 Involved Thales-DIS sites

- **Development and Project Managment**
  - La Ciotat (France)
    - CC project management
  - Meudon (France)
    - eTravel development
  - Singapore
    - Platform & eTravel development
  - Vantaa
    - eTravel development support
- **Manufacturing**
  - Gémenos, Singapore, Vantaa, Tczew, Curitiba, Chanhassen, Pont-Audemer
- **IT activities**
  - Gémenos, Calamba, Les Clayes, Marcoussi, Pune

3. CONFORMANCE CLAIMS

3.1 CC CONFORMANCE CLAIM

This security target claims conformance to

- [CC-1]
- [CC-2]
- [CC-3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- [CEM] has to be taken into account.

3.2 PP CLAIM,

The MultiApp V5.1 eTravel 3.1 EAC/BAC security target claims strict conformance to the Protection Profile [PP-MRTD-EAC].
The MultiApp V5.1 eTravel 3.1 EAC/BAC security target is a composite security target, including the IC security target [ST-AQU-IC]. However the security problem definition, the objectives, and the SFR of the IC are not described in this document.

3.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC-3].

3.4 CONFORMANCE STATEMENT

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

4. SECURITY PROBLEM DEFINITION

4.1 INTRODUCTION

4.1.1 Assets

4.1.1.1 MRTD assets

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

Logical MRTD sensitive User Data

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

Application note: Due to interoperability reasons the 'ICAO Doc 9303' [ICAO-9303] requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG16. As the BAC mechanisms may not resist attacks with high attack potential, security of other Data Groups of the logical MRTD are covered by another ST (cf. [ST-BAC]).

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 traveller to prove his possession of a genuine MRTD.

4.1.1.2 TSF Data

D.JCS_CODE

The code of the Java Card System.
To be protected from unauthorized disclosure and modification.

D.JCS_DATA

The internal runtime data areas necessary for the execution of the Java Card VM, such as, for instance, the frame stack, the program counter, the class of an object, the length allocated for an array, any pointer used to chain datastructures.
To be protected from monopolization and unauthorized disclosure or modification.

4.1.1.3 OS-Update Assets

The following assets are related to patch management in post-issuance phase (phase 7). There is no patch associated to the present TOE, however the patch mechanisms are within the evaluation scope.

D.OS-UPDATE_DEC-KEY	Refinement of D.APP_KEYS. A cryptographic key, owned by the OS Developer, and used by the TOE to decrypt the additional code to be loaded. Note: No assumption is made on the type of this decryption key, i.e. it can be either a symmetric key or the secret component of an asymmetric key pair. To be protected from unauthorised disclosure and modification.
D.OS-UPDATE_SGNVER-KEY	Refinement of D.APP_KEYS. A cryptographic key, owned by the OS Developer, and used by the TOE to verify the signature of the additional code to be loaded. Note: No assumption is made on the type of this signature verification key, i.e. it can be either a symmetric key or the public component of an asymmetric key pair. In case of a symmetric key: to be protected from unauthorised disclosure and modification.

	In case of an asymmetric public key: to be protected from unauthorised modification.
D.OS-UPDATE_ADDITIONALCODE	The code to be added to the OS after TOE issuance. The additional code has to be signed by the OS Developer. After successful verification of the signature by the Initial TOE, the additional code is loaded and installed through an atomic activation (to create an Updated TOE). To be protected from unauthorised disclosure and modification.
D.OS-UPDATE-CODE-ID	The identification data associated with the additional code. It is loaded and/or updated in the same atomic operation as additional code loading. To be protected from unauthorised modification. Application Note: The identification data (D.OS-UPDATE-CODE-ID) may also be protected from unauthorised disclosure (confidentiality requirement) by not permitting an attacker to determine whether a given TOE has been updated or not (even if it is not possible to distinguish between functional and security updates). However, confidentiality is not mandatory since in most cases the identification data must be readily available on the field through technical commands, even in the TERMINATED state.

4.1.2 Subjects

This protection profile 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.

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

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

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

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

Inspection system (IS)
A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The

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

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

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

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

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

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.

Embedded Software Developer
The additional code to the entity responsible to its deployment. It is represented in TOE by D.ACODE_ SGNVER-KEY and invoked during verification of signature of additional code.

Deployment Additional code Agent
The agent is acting on behalf of the issuing State or Organization to deploy the additional code for the post-Issuance loading. It is at delivery point the entity authorized to receive the additional code from Embedded Software Developer to produce the CVCA Link certificate including the additional code. This actor is represented in TOE by a key used to verify the certificate including the additional code.

Post-Issuance Additional code Agent / Terminal
The agent or terminal is acting on behalf of the issuing State or Organization to perform the loading of additional code at post-Issuance. It is represented in TOE by authentication key used to perform authentication required prior additional code loading.

4.2 ASSUMPTIONS

4.2.1 MRTD 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.

A.Insp_Sys Inspection Systems for global interoperability
The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.
The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

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

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

4.2.2 OS Update Assumptions

A.OS-UPDATE-EVIDENCE

For additional code loaded pre-issuance, it is assumed that:

- Evaluated technical and/or audited organizational measures have been implemented to ensure that the additional code:
  - (1) has been issued by the genuine OS Developer
  - (2) has not been altered since it was issued by the genuine OS Developer.

For additional code loaded post-issuance, it is assumed that the OS Developer provides digital evidence to the TOE in order to prove the following:

(1) he is the genuine developer of the additional code and

(2) the additional code has not been modified since it was issued by the genuine OS Developer.

A.SECURE_ACODE_MANAGEMENT

It is assumed that:

- The Key management process related to the OS Update capability takes place in a secure and audited environment.
- The cryptographic keys used by the cryptographic operations are of strong quality and appropriately secured to ensure confidentiality, authenticity and integrity of those keys.

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.

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

4.3.1 MRTD Threats

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

T.Read_Sensitive_Data Read the sensitive biometric reference data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip.
The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [PP-MRTD-BAC]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.

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

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

T.Forgery Forgery of data on MRTD's chip

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

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

Asset: authenticity of logical MRTD data,

T.Counterfeit MRTD's chip

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

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

Asset: authenticity of logical MRTD data,

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 "Operational Use" phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.
This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

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

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

T.Information_Leakage 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 high 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 high attack potential, being in possession of a legitimate MRTD

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

T.Malfunction Malfunction due to Environmental Stress

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

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

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

4.3.2 OS Update Threats

The following threats are related to patch loading in post-issuance.

T.UNAUTHORISED-TOE-CODE-UPDATE

An attacker attempts to update the TOE code with a malicious update that may compromise the security features of the TOE.
Threat agent: Attacker
Targeted asset(s): D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA .

T.FAKE-SGNVER-KEY

An attacker modifies the signature verification key used by the TOE to verify the signature of the additional code. Hence, he is able to sign and successfully load malicious additional code inside the TOE.
Threat agent: Attacker
Targeted assets: D.OS-UPDATE_SGNVER-KEY, D.OS-UPDATE_ADDITIONALCODE.

T.WRONG-UPDATE-STATE

An attacker prevents the OS Update operation to be performed atomically, resulting in an inconsistency between the resulting TOE code and the identification data:

- The additional code is not loaded within the TOE, but the identification data is updated to mention that the additional code is present;
- The additional code is loaded within the TOE, but the identification data is not updated to indicate the change.

Threat agent: Attacker
Targeted asset: D.OS-UPDATE-CODE-ID.

T.INTEG-OS-UPDATE_LOAD

The attacker modifies (part of) the additional code when it is transmitted to the TOE for installation.
Threat agent: Attacker
Targeted assets: D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.

T.CONFID-OS-UPDATE_LOAD

The attacker discloses (part of) the additional code when it is transmitted to the TOE for installation.
Threat agent: Attacker
Targeted assets: D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.

T.CONFID-OS-UPDATE_LOAD

The attacker discloses (part of) the additional code when it is transmitted to the TOE for installation.
Threat agent: Attacker
Targeted assets: D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.

4.4 Organizational Security Policies

4.4.1 MRTD OSP

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

P.BAC-PP Fulfillment of the Basic Access Control Protection Profile.
The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the 'ICAO Doc 9303' [ICAO-9303] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP-MRTD-BAC] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

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

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

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.Active_Auth Active Authentication

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

4.4.2 OS Update OSP

OSP.ATOMIC_ACTIVATION
Additional code has to be loaded and installed on the TOE through an atomic activation.
Each additional code shall be identified with unique Identification Data. During such atomic activation, identification Data of the TOE have to be updated to clearly identify the Updated TOE.
In case of interruption or incident during activation, the TOE shall remain in its initial state or set in a failed secure state.

OSP.TOE_IDENTIFICATION
Identification Data of the resulting Updated TOE shall identify the Initial TOE and the activated additional code. Identification Data shall be protected in integrity.

OSP.ADDITIONAL_CODE_SIGNING
The additional code has to be signed with a cryptographic key pair according to relevant standard and the generated signature is associated to the additional code.
The additional code signature must be checked during loading to assure its authenticity and integrity and to assure that loading is authorized on the TOE.
The cryptographic key used to sign the additional code shall be of sufficient quality and the process for key generation and storage shall be appropriately secured to ensure the authenticity, integrity and confidentiality of the key. The process to deliver the key for signature verification shall be appropriately secured to ensure the authenticity, integrity and confidentiality of the key (not applicable if public key).

OSP.ADDITIONAL_CODE_ENCRYPTION
The additional code has to be encrypted according to relevant standard in order to ensure its confidentiality when it is transmitted to the TOE for loading and installation.
The encryption key shall be of sufficient quality and the process for key generation and storage shall be appropriately secured to ensure the confidentiality, authenticity and integrity of the key.

5. SECURITY OBJECTIVES

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

5.1 SECURITY OBJECTIVES FOR THE TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organisational 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.DG3 to EF.DG16 are added.

Application note:The OT.AC_Pers implies that

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

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

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

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).

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

Application note: The OT.Chip_Auth_Proof implies the MRTD’s chip to have (i) a unique identity as given by the MRTD’s Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD’s chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD’s chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [ICAO-9303] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

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

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

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.

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

OT.Prot_Phys-Tamper 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 high attack potential by means of

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

with a prior

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

OT.Prot_Malfunction 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.

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

OT.Active_Auth_Proof Proof of MRTD's chip authenticity through AA
The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the 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.

5.2 Security objectives for OS-Agility

Security Target of a TOE embedding a Loader shall include the following Security Objectives.

O.SECURE_LOAD_ACODE

The TOE shall check an evidence of authenticity and integrity of the additional code to be loaded.

The TOE enforces that only an allowed version of the additional code can be loaded. The TOE shall forbid the loading of an additional code not intended to be assembled with the TOE.

During the loading of the additional code, the TOE shall remain secure.

The additional code can be loaded from a terminal at border control

- Document Verifier entities generate new Terminal certificates signed by the new DV certificates and propagate the certificate chain to all the border controls.
- At border control the EAC mechanism is enforced on the Inspection System with the use of the new certificate chain.
- TOE application is updated during the document verification (Terminal Authentication).

The additional code can be loaded from a terminal as the user mobile

- Document Verifier entities or Thales generate new Terminal certificate (Certificate Holder Authorization Template set to inexistent DG for security reason) signed by the new DV certificates and embed it with a mobile application
- The mobile application is provided to the citizen from an application store.
- Citizen uses the mobile application and scans the MRZ of the document with the camera of the smartphone
- BAC/SAC followed by EAC is performed. TOE application is updated. Citizen is informed that the TOE application has been updated by mobile application.

The additional code can be loaded using a tool in personalization phase

- TOE application is updated during the document personalization (Issuer Authentication).

O.SECURE_AC_ACTIVATION

Activation of the additional code and update of the Identification Data shall be performed at the same time in an atomic way. All the operations needed for the code to be able to operate as in the Updated TOE shall be completed before activation.

If the atomic activation is successful, then the resulting product is the Updated TOE, otherwise (in case of interruption or incident which prevents the forming of the Updated TOE), the TOE shall preserve a secure state.

O.TOE_IDENTIFICATION

The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data.

After atomic activation of the additional code, the Identification Data of the Updated TOE allows identifications of both the Initial TOE and additional code.

The user must be able to uniquely identify Initial TOE and additional code(s) which are embedded in the Updated TOE.

O.CONFID-OS-UPDATE.LOAD

The TOE shall decrypt the additional code prior installation.

Application Note: Confidentiality protection must be enforced when the additional code is transmitted to the TOE for loading (See OE.OS-UPDATE-ENCRYPTION). Confidentiality protection can be achieved either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.

5.3 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 to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO-9303].

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

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

OE.BAC_PP Fulfillment of the Basic Access Control Protection Profile.
It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP-MRTD-BAC]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

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 CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

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

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

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

OE.Ext_Insp_Systems Authorization of Extended Inspection Systems
The Document Verifier of receiving States or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical MRTD. The Extended Inspection System authenticates themselves to the MRTD's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

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.

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.

5.4 Security objectives for the operational environment for OS Agility

The following security objectives for the operational environment shall also be considered for the present evaluation:

OE.OS-UPDATE-EVIDENCE	For additional code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that the additional code (1) has been issued by the genuine OS Developer (2) has not been altered since it was issued by the genuine OS Developer. For additional code loaded post-issuance, the OS Developer shall provide digital evidence to the TOE that (1) he is the genuine developer of the additional code and (2) the additional code has not been modified since it was issued by the genuine OS Developer.
OE.OS-UPDATE-ENCRYPTION	For additional code loaded post-issuance, the OS Developer shall encrypt the additional code so that its confidentiality is ensured when it is transmitted to the TOE for loading and installation.
OE.SECURE_ACODE_MANAGEMENT	Key management processes related to the OS Update capability shall take place in a secure and audited environment. The key generation processes shall guarantee that cryptographic keys are of sufficient quality and appropriately secured to ensure confidentiality, authenticity and integrity of the keys.

5.5 SECURITY OBJECTIVE RATIONALE

5.5.1 Rationale between objectives and threats, assumptions, OSP

The following table provides an overview for security objectives coverage.
Table and following explanations are copied from [PP-MRTD-EAC]. Only the shaded parts are added.

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.BAC-PP	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_Systems	OE.Active.Auth_Sign	OE.Active_Auth_Verif	OE.OS-UPDATE-EVIDENCE	OE.OS-UPDATE-ENCRYPTION	OE.SECURE_ACODE_MANAG	O.SECURE_LOAD_ACODE	O.SECURE_AC_ACTIVATION	O.TOE_IDENTIFICATION	O.CONFID-OS-UPDATE.LOAD
T.UNAUTHORISED-TOE-CODE-UPDATE																											X			
T.FAKE-SGNVER-KEY																											X			
T.WRONG-UPDATE-STATE																												X	X	
T.INTEG-OS-UPDATE_LOAD																											X			
T.CONFID-OS-UPDATE_LOAD																														X
T.Read_Sensitive_Data			X													X					X									
T.Forgery	X	X						X						X				X	X											
T.Counterfeit					X										X			X												
T.Abuse-Func						X																								
T.Information_Leakage							X																							
T.Phys-Tamper								X																						
T.Malfunction									X																					
P.BAC-PP																	X													
P.Sensitive_Data			X													X					X									
P.Manufact				X																										
P.Personalization	X			X									X																	
P.Active_Auth										X												X	X							
OSP.ATOMIC_ACTIVATION																												X		
OSP.TOE_IDENTIFICATION																													X	
OSP.ADDITIONAL_CODE_SIGNING																											X			
OSP.ADDITIONAL_CODE_ENCRYPTION																									X					X
A.MRTD_Manufact											X																			
A.MRTD_Delivery												X																		
A.Pers_Agent													X																	
A.Insp_Sys																		X		X										
A.Signature_PKI														X				X												
A.Auth_PKI																X					X									
A.OS-UPDATE-EVIDENCE																								X						
A.SECURE_ACODE_MANAGEMENT																										X				

Table 2: Security Objective Rationale

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

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.Personalisation** “Personalisation of the MRTD by issuing State or Organisation only” addresses the (i) the enrolment of the logical MRTD by the Personalisation Agent as described in the security objective for the TOE environment **OE.Personalisation** “Personalisation 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 Personalisation of logical MRTD”. Note the manufacturer equips the TOE with the Personalisation 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 the management of TSF to the Personalisation Agent.

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

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.Counterfeit** "MRTD's chip addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing State or Organisation. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_MRTD.** "MRTD Authentication Key". According to **OE.Exam_MRTD** "Examination of the physical part of the travel document" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the travel MRTD's chip.

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

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 respectively 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.

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

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

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

The threat **T.UNAUTHORISED-TOE-CODE-UPDATE** is covered by the O.SECURE_LOAD_ACODE security objective that ensures the authenticity and the integrity of the additional code. It ensure also that that only the allowed code will be load in a secure process.

The threat **T.FAKE-SGNVER-KEY** is covered by the O.SECURE_LOAD_ACODE security objective which ensures the authenticity and the integrity of the additional code to avoid loading malicious additional code.

The threat **T.WRONG-UPDATE-STATE** is covered by the O.SECURE_AC_ACTIVATION and O.TOE_IDENTIFICATION security objective that ensures that the update state stay secure during all the loading process

The threat **T.INTEG-OS-UPDATE_LOAD** is covered by the O.SECURE_LOAD_ACODE security objective that ensures the authenticity and the integrity of the additional code.

The threat **T.CONFID-OS-UPDATE_LOAD** is covered by the O.CONFID-OS-UPDATE.LOAD security objective that ensures the confidentiality of the additional code when transmitted until installation.

The **OSP.ADDITIONAL_CODE_ENCRYPTION** is enforced by the TOE security objective O.CONFID-OS-UPDATE.LOAD and the security objective of environment OE.OS-UPDATE-ENCRYPTION which ensure the confidentiality of the additional code

The **OSP.ADDITIONAL_CODE_SIGNING** is enforced by the TOE security objective of the O.SECURE_LOAD_ACODE which ensure the integrity of the additional code

The **OSP.ATOMIC_ACTIVATION** is enforced by the TOE security objective O.SECURE_AC_ACTIVATION which ensure the atomicity of the activation of the additional code

The **OSP.TOE_IDENTIFICATION** is enforced by the TOE security objective O.TOE_IDENTIFICATION which ensure the identification of the additional code

The assumption **A.OS-UPDATE-EVIDE**NCE is upheld by the security objective on the operational environment OE.OS-UPDATE-EVIDENCE that guarantees that the additional code has been issued by the genuine OS Developer, has not been altered since it was issued by the genuine OS Developer.

The assumption **A.SECURE_ACODE_MANAGEMENT** is upheld by the security objective on the operational environment OE.SECURE_ACODE_MANAGEMENT that guarantees that cryptographic keys are of sufficient quality and appropriately secured to ensure confidentiality, authenticity and integrity of the keys.

5.5.2 Justifications for adding objectives on the environment

Additions to [PP-MRTD-EAC]

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-EAC]. Therefore the added objectives on the environment do not weaken the TOE.

5.5.2.1 Addition for OS Update feature

The additional objectives on the environment for ES update are:

- OE.OS-UPDATE-EVIDENCE,
- OE.OS-UPDATE-ENCRYPTION,
- OE.SECURE_ACODE_MANAGEMENT.

These additional objectives on the environment for OS update does not directly interact with objectives on the environment for MRTD application.

5.5.3 Compatibility between objectives of [ST-EAC] and [ST-AQU-IC]

5.5.3.1 Compatibility between objectives for the TOE

The following table lists the relevant security objectives of the IC and provides the link to the security objectives related to the composite product, showing that there is no contradiction between the two.

IC objective label	Platform objective short description (refer to [AQU-IC-CCI] for the full description)	Link to the composite-product
O.Phys-Manipulation	Protection against Physical Manipulation	OT.Prot_Phys-Tamper
O.Phys-Probing	Protection against Physical Probing	OT.Prot_Phys-Tamper, OT.Data_Int
O.Malfunction	Protection against Malfunction	OT_Prot_Malfunction
O.Leak-Inherent	Protection against Inherent Information Leakage	OT.Prot_Inf_Leak
O.Leak-Forced	Protection against Forced Information Leakage	OT.Prot_Inf_Leak
O.Abuse-Func	Protection against Abuse of Functionality	OT.Prot_Abuse-Func
O.Identification	TOE Identification	OT.Identification
O.RND	Random Numbers	This platform security objectives is used to endure the security of the composite TOE
O.Cap_Avail_Loader	Capability and availability of the Loader Valid only for the TOE derivatives delivered with activated Flash Loader.	No direct link with the composite product security objectives, but this platform security objective is used to endure the security of the composite TOE
O.Authentication	Authentication to external entities Valid only for the TOE derivatives delivered with activated Flash Loader	
O.Ctrl_Auth_Loader	Access control and authenticity for the Loader - valid only for the TOE derivatives delivered with activated Flash Loader	
O.Mem Access	Area based Memory Access Control	OT.Sens_Data_Conf OE.Prot_Logical_MRTD
O.Prot_TSF_Confidentiality	Protection of the confidentiality of the TSF	OT.Sens_Data_Conf OE.Prot_Logical_MRTD

The other objectives of the platform are not relevant for this composite TOE.

OT.AC_Pers, OT.Chip_Auth_Proof and OT.Active_Auth_Proof are specific to [ST-EAC] and they do not conflict with the objectives of [ST-AQU-IC].

O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION and O.CONFID-OS-UPDATE.LOAD are objectives added to this Security Target and it does no conflict with the objectives of [ST-AQU-IC].
We can therefore conclude that the objectives for the TOE of [ST-EAC] and [ST-AQU-IC] are consistent.

5.5.3.2 Compatibility between objectives for the environment

IC Environment objective label	Platform Environment Objective short description (refer to [AQU-IC-CCI] for the full description)	Link to the composite-product
OE.Resp-Appl	Treatment of User data of the Composite TOE	For Phase 1 - No direct link with the composite product security objectives
OE.Process-Sec-IC	Protection during composite product manufacturing	OE.Personalization OE.MRTD_Manufact OE.MRTD_Delivery
OE.Lim_Block_Loader	Limitation of capability and blocking the loader.	No direct link with the composite product security objectives, but this platform security objective is used to endure the security of the composite TOE
OE.TOE_Auth	Authentication to external entities	
OE.Loader_Usage	Secure communication and usage of the Loader	

OE.Auth_Key_MRTD, OE.Authoriz_Sens_Data, OE.BAC_PP, OE.Exam_MRTD, OE.Prot_Logical_MRTD, OE.Pass_Auth_Sign, OE.Passive_Auth_Verif, OE.Ext_Insp_Systems, OE.Active_Auth_Sign, OE.Active_Auth_Verif are specific to [ST-EAC] and they do no conflict with the objectives of [ST-AQU-IC].

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

6. EXTENDED COMPONENTS DEFINITION

This security target uses components defined as extensions to CC part 2. Some of these components are defined in protection profile [PP-IC-0002]; others are defined in the protection profile [PP-MRTD-EAC].

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.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.

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*].

6.4 Definition of the Family FMT_LIM

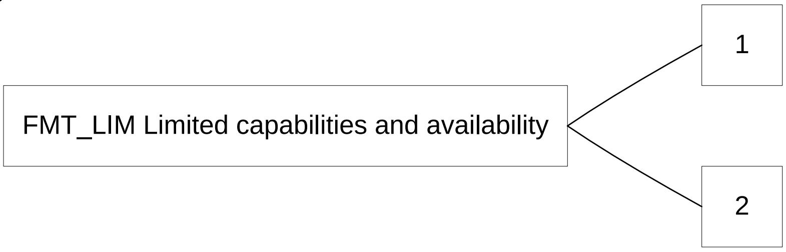
The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class 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*].

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.

6.5 Definition of the Family FPT_EMS

The sensitive family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [CC-2].

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

Family behaviour
This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS.1 TOE emanation has two constituents:

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

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

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

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

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components
Dependencies: No dependencies.

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

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

7. Security Requirements

The definition of the subjects "Manufacturer", "Pre-personalizer", "Personalization Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 2.4.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 10 "Glossary and Acronyms" 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 authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR-EAC], A.5.1); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA
	DV (domestic)	roles defined in the certificate used for authentication (cf. [TR-EAC], A.5.1); Terminal is authenticated as domestic Document Verifier after successful CA and TA
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR-EAC], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA and TA
	IS	roles defined in the certificate used for authentication (cf. [TR-EAC], A.5.1); Terminal is authenticated as Extended Inspection System after successful CA and TA
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [TR-EAC], A.5.1)
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR-EAC], A.5.1)
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [TR-EAC], A.5.1)

The following table provides an overview of the keys and certificates used:

Name	Data
Country Verifying Certification Authority Private Key (SKCVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SKCVCA) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PKCVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PKCVCA) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (CCVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [TR-EAC] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PKCVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.

Name	Data
Document Verifier Certificate (CDV)	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PKDV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (CIS)	The Inspection System Certificate (CIS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PKIS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SKICC, PKICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PKICC)	The Chip Authentication Public Key (PKICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SKICC)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

Application note 20: The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization.

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-EAC], and in bold font when the refinement is done in this ST. When the SFR is refined in the [PP-MRTD-EAC] and additionally refined in this ST then the font is bold and underline.

For this section, a presentation choice has been selected. Each SFR present 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 with the capability to store the IC Identification Data in the audit records.

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/CA Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys

Hierarchical to: No other components
Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]]: fulfilled by **FCS _COP.1/CA_MAC**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**

FCS_CKM.1.1 /CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Table 3 algorithm column** and specified cryptographic key sizes **Table 3 Key size column** that meet the following: **Table 3 standard column**.

Algorithm type	algorithm	Key size	standard
/TDESsession-DH	**DH Key Agreement Algorithm - PKCS#3 – 1024, 1280, 1536 and 2048 bits**	**112 bits**	**Diffie-Hellman key derivation protocol compliant to [PKCS#3]**
/AESsession-DH	**DH Key Agreement Algorithm - PKCS#3 – 1024, 1280, 1536 and 2048 bits**	**128, 192, and 256 bits**	***Diffie-Hellman key derivation protocol compliant to [PKCS#3]***
/TDESsession-ECDH	**ECDH Key Agreement Algorithm - ISO 15946 – 160, 192, 224, 256, 320, 384, 512 and 521 bits**	**112 bits**	***[TR-EAC] , based on an ECDH protocol compliant to [TR-ECC]***
/AESsession-ECDH	**ECDH Key Agreement Algorithm - ISO 15946 – 160, 192, 224, 256, 320, 384, 512 and 521 bits**	**128, 192, and 256 bits**	***[TR-EAC] , based on an ECDH protocol compliant to [TR-ECC]***

Table 3: FCS_CKM.1/CA iteration explanation

FCS_CKM.1/KeyPair Cryptographic key generation for AA and CA Key Pair

Hierarchical to: No other components
Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]: fulfilled by **FCS_COP.1/AA**, **FCS_COP.1/CA_MAC** and **FCS_COP.1/SYM**
FCS_CKM.4 Cryptographic key destruction: not fulfilled, see application note

FCS_CKM.1.1 /KeyPair The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Table 4 algorithm column** and specified cryptographic key sizes **Table 4 Key size column** that meet the following: **Table 4 standard column**.

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**	***FIPS 186-3 Appendix B.4.1***
CA/DH	**DH key generation**	**1024, 1280, 1536 and 2048 bits**	**ANSI X9.42**
CA/ECDH	**ECDH Key generation**	**160, 192, 224, 256, 320, 384, 512 and 521 bits**	**[IEEE-P1363]**

Table 4: FCS_CKM.1/KeyPair iteration explanation

Application notes:

- The dependency of FCS_CKM1/KeyPair on FCS_COP.1 is partly fulfilled by FCS_COP.1/CA_MAC and FCS_COP.1/SYM. This dependence is not direct: FCS_CKM1/KeyPair generates a static key which in turn generate session keys, via FCS_CKM1/CA. These session keys then use FCS_COP.1/CA_MAC and FCS_COP.1/SYM.
- The dependency of FCS_CKM1/KeyPair on FCS_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.

FCS_CKM.1/PERSO Cryptographic key generation for Session keys

Hierarchical to: No other components
Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]: fulfilled by **FCS_COP.1/PERSO**
FCS_CKM.4 Cryptographic key destruction]: fulfilled by **FCS_CKM.4**

FCS_CKM.1.1 /PERSO The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Table 5 algorithm column** and specified cryptographic key sizes **Table 5 Key size column** that meet the following: **Table 5 standard column**.

Algorithm type	algorithm	Key size	standard
/TDES	**TDES ISK key derivation**	**112 bits**	**[ICAO-9303] normative appendix 5**
/GP	**GP session keys**	**112, 128 bits (and 192 & 256 bits for SCP03)**	**[GP211] SCP01, SCP02, or SCP03**

Table 5: FCS_CKM.1/PERSO iteration explanation

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]: fulfilled by **FCS_CKM.1/CA**, and **FCS_CKM.1/PERSO**.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Secure erasing of the value** that meets the following: **None**.

Application note: Secure erasing of data is performed by overwriting the data with random numbers.

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** in accordance with a specified cryptographic algorithm **SHA-1, SHA-224, SHA-256, SHA-384, SHA-512** and cryptographic key sizes **none** that meet the following: **FIPS 180-2**.

FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption

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/CA**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**

FCS_COP.1.1 /SYM The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm **Table 6 algorithm** and cryptographic key sizes **Table 6 Key size** that meet the following: **Table 6 list of standards**.

Algorithm type	algorithm	Key size	List of standards
/ENC_TDES	**TDES in CBC mode**	**112 bits**	**ISO 10116, [TR-EAC]**
/ENC_AES	**AES in CBC mode**	**128, 192, 256**	**ISO 10116, [TR-EAC]**

Table 6: FCS_COP.1/SYM iteration explanation

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification 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]: fulfilled by **FCS_CKM.1/CA**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**
.

FCS_COP.1.1 /SIG_VER The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **Table 7 algorithm** and cryptographic key sizes **Table 7 Key size** that meet the following: **Table 7 list of standards**.

Algorithm type	algorithm	Key size	List of standards
/RSA_VER	**RSA (STD)**	**1024, 1280, 1536, 2048, 3072, and 4096**	**RSA SHA PKCS#1** **RSA SHA PKCS#1 PSS**
/ECC_VER	**ECC**	**160, 192, 224, 256, 320, 384, 512, 521**	**[TR-ECC] ECDSA SHA**

Table 7: FCS_COP.1/SIG_VER iteration explanation

FCS_COP.1/CA_MAC Cryptographic operation – 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]: fulfilled by **FCS_CKM.1/CA**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /CA_MAC The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm **Table 8 algorithm** and cryptographic key sizes **Table 8 Key size** that meet the following: **Table 8 list of standards**.

Algorithm type	algorithm	Key size	List of standards
/MAC_TDES	**TDES Retail MAC**	**112 bits**	**ISO 9797-1, [TR-EAC]**
/MAC_AES	**AES CMAC**	**128, 192, 256**	**[NIST-800-38B], [TR-EAC]**

Table 8: FCS_COP.1/CA_MAC iteration explanation

Remark: this SFR is renamed **FCS_COP.1/CA_MAC instead of FCS_COP.1/MAC**

FCS_COP.1/PERSO Cryptographic operation – Symmetric encryption, decryption, and MAC during manufacturing

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/PERSO**.
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /PERSO The TSF shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm **Table 9 algorithm column** and cryptographic key sizes **Table 9 Key size column** that meet the following: **Table 9 List of standards column**.

Algorithm type	algorithm	Key size	List of standards
/ENC_TDES	**TDES encryption and decryption**	**112 bits**	**[SP 800-67]**
/ENC_AES	**AES encryption and decryption**	**128, 192, 256**	**[FIPS 197]**
/MAC_TDES	**TDES Retail MAC**	**112 bits**	**ISO 9797-1**
/MAC_AES	**AES CMAC**	**128, 192, 256**	**[NIST-800-38B]**

Table 9: FCS_COP.1/ PERSO iteration explanation

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/KeyPair**
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 **Table 10 algorithm** and cryptographic key sizes **Table 10 Key size** that meet the following: **Table 10 List of standards**.

Algorithm type	algorithm	Key size	List of standards
/AA_RSA	**RSA**	**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 10: 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], [AIS20/31]** and **[SP 800-90] with seed entropy at least 128 bits**.

Application note: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

7.1.3 Class FIA Identification and Authentication

Table 11 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE
Authentication Mechanism for Pre-personalisation and Personalisation Agents	**FIA_UAU.1/PERSO FIA_AFL.1/PERSO**
Authentication Mechanism for Pre-Personalisation and Personalisation Agents	**FIA_UAU.4**
Chip Authentication Protocol v.1	**FIA_UAU.5**
Terminal Authentication Protocol v.1	**FIA_UAU.5**
Passive Authentication	**FIA_UAU.5**

Table 11: Overview on authentication SFR

Note the Chip Authentication Protocol as defined in this protection profile[19] includes

- the BAC authentication protocol as defined in 'ICAO Doc 9303' [ICAO-9303] in order to gain access to the Chip Authentication Public Key in EF.DG14,
- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol,

- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The BAC mechanism does not provide a security function on their own. The Chip Authentication Protocol may be used independent of the Terminal Authentication Protocol. But if the Terminal Authentication Protocol is used the terminal shall use the same public key as presented during the Chip Authentication Protocol.

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

FIA_AFL.1/PERSO Authentication failure handling during pre-personalization and personalization phases

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication: fulfilled by **FIA_UAU.1/PERSO**

FIA_AFL.1.1 /Perso The TSF shall detect when ‘**Number’ column in Table 12** unsuccessful authentication attempts occurs related to ‘**Authentication type’ column in Table 12**.

FIA_AFL.1.2 /Perso When the defined number of unsuccessful authentication attempts has been met, the TSF shall perform ‘**Actions’ column in Table 12**.

Authenticaton type	Number	Actions
GP	**3**	**Block GP authentication**.
ISK key	**3**	**Block ISK Key**.

Table 12: FIA_AFL.1/PERSO iteration explanation

FIA_UID.1/PERSO Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 /PERSO The TSF shall allow
1. to establish a communication channel,
2. to carry out the mutual authentication Protocol according to [GP]
on behalf of the user to be performed before the user is identified.

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

FIA_UID.1/MRTD Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/MRTD The TSF shall allow
1. to establish a communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
3. to carry out the Chip Authentication Protocol
on behalf of the user to be performed before the user is identified.

FIA_UID.1.2//MRTD 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/PERSO Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by **FIA_UID.1/PERSO**
FIA_UAU.1.1 /PERSO	The TSF shall allow **1. to establish a communication channel,** **2. to carry out the mutual authentication Protocol according to [GP]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 /PERSO	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

- FIA_AFL.1/PERSO and FIA_UID.1/PERSO are extensions to [PP-MRTD-EAC], in order to deal with identification and authentication in pre-personalisation and personalisation phases.

FIA_UAU.1/MRTD Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by **FIA_UID.1/MRTD**
FIA_UAU.1.1/MRTD	The TSF shall allow 1. to establish a communication channel, 2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS 3.to identify themselves by selection of the authentication key 4,to carry out the Chip Authentication Protocol on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/MRTD	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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. Terminal authentication, 2. Authentication Mechanism based on **Triple-DES, AES**

Application note: The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.

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

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 Pre-personalization Agent by the Symmetric Authentication Mechanism with the Pre-personalization Agent Key.**
2. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication mechanism.
3. The TOE accepts:

the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism

4. the authentication attempt as Personalization Agent by **the Symmetric Authentication Mechanism with Personalization Agent Key**.

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 after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.

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

FIA_API.1/CA Authentication Proof of Identity – Chip Authentication

Hierarchical to: No other components
Dependencies: No dependencies

FIA_API.1.1/CA The TSF shall provide a Chip Authentication Protocol v.1 according to [TR-EAC] to prove the identity of the TOE.

Application note: This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [TR-EAC]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO-9303], normative appendix 5, A5.1. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

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]** to prove the identity of the **TOE**.

Application note: This SFR requires the TOE to implement the Active Authentication Mechanism specified in [ICAO-9303]. The terminal generates a challenge 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).

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

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

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

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; fulfilled by **FDP_ACC.1** FMT_MSA.3 Static attribute initialization

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

1. Subjects:
   a. Personalization Agent,
   b. Extended Inspection System
2. Terminal Objects:
   a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, of the logical MRTD
   b. data in EF.DG3 and EF.DG4 of the logical MRTD
   c. data in EF.COM,
   d. data in EF.SOD
3. Security attributes:
   a. authentication status of terminal,
   b. Terminal Authorization

.

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

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data of the EF.DG3 of the logical MRTD,

3. the successfully authenticated Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data of the EF.DG4 of the logical MRTD.

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

FDP_ACF.1.4
1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,
5. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
6. Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD

Application note: Note the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG16 of the logical MRTD. These security features of the MRTD are not subject of this ST.

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

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 Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure after Chip Authentication.

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

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 Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication.

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

Rationale for Refinement: Note that the Access Control SFP (cf. FDP_ACF.1.2) allows the Extended Inspection System (as of [ICAO-9303] and [PP-MRTD-BAC]) to access the data EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD. Nevertheless there is explicitly no rule for preventing access to these data. More over their data integrity (cf. FDP_UIT.1) and confidentiality (cf. FDP_UCT.1) is ensured by the BAC mechanism being addressed and covered by [PP-MRTD-BAC]. The fact that the BAC mechanism is not part of the ST in hand is addressed by the refinement “after Chip Authentication”.

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.

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 fulfilled by **FIA_UID.1/PERSO.**

FMT_SMR.1.1 The TSF shall maintain the roles
1. Manufacturer,
2. Personalization Agent,
3. Country Verifying Certification Authority,
4. Document Verifier,
5. domestic Extended Inspection System,
6. foreign Extended Inspection System.

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

Application note: The MRTD also maintains the role Basic Inspection System due to a direct consequence of P.BAC-PP resp. OE.BAC-PP. Nevertheless this role is not explicitly listed in FMT_SMR.1.1, above since the TSF cannot maintain the role with respect to the assumed high attack potential due to the known weaknesses of the Document Basic Access Keys.

Application note : The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.
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 capabilities: fulfilled by **FMT_LIM.2**.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow,
1. User Data to be manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.

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: fulfilled by **FMT_LIM.1**.

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

Application note: The term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application note: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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: fulfilled by **FMT_SMF.1**
FMT_SMR.1 Security roles: fulfilled by **FMT_SMR.1**

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

Application note: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

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: fulfilled by **FMT_SMF.1**
FMT_SMR.1 Security roles: fulfilled by **FMT_SMR.1**

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

FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date

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

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

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

to **the Personalization Agent**.

FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifying Certification Authority

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

FMT_MTD.1.1/ CVCA_UPD The TSF shall restrict the ability to update the
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate

to Country Verifying Certification Authority.

FMT_MTD.1/DATE Management of TSF data – Current date

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

FMT_MTD.1.1/ DATE The TSF shall restrict the ability to modify the Current date to
1. Country Verifying Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System.

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

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

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

FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key

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

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

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: fulfilled by **FMT_SMF.1**
FMT_SMR.1 Security roles: fulfilled by **FMT_SMR.1**

FMT_MTD.1.1/ AAK **The TSF shall restrict the ability to create and load the Active Authentication Private Key to the Personalization Agent.**

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

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

FMT_MTD.1.1/ KEY_READ The TSF shall restrict the ability to read the
1. Document Basic Access Keys,
2. Chip Authentication Private Key,
3. **Active Authentication Private Key**
4. Personalization Agent Keys

to none.

The TOE shall meet the requirement “Secure TSF data (FMT_MTD.3)” as specified below (Common Criteria Part 2):

FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components
Dependencies:	FMT_MTD.1 Management of TSF data: fulfilled by : **FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD**

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

Refinement: The certificate chain is valid if and only if

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

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

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

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

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

Application note: The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.

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: No dependencies.

FPT_EMS.1.1 The TOE shall not emit **electromagnetic and current emissions** in excess of **intelligible threshold** enabling access to Personalization Agent Key(s) and Chip Authentication Private Key and **Active Authentication Key, EF.DG3 and EF.DG4**.

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

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: No dependencies.

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

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

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: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests to demonstrate the correct operation of **the TSF**, **at the conditions**:

1. **During initial start-up**
2. **Periodically during normal operation**
3. **After cryptographic computation**
4. **Before any use or update of TSF data**

The description of the self test is the following (for each corresponding number):

1. **RNG live test, sensor test, FA detection, Integrity Check of NVM ES**
2. **RNG monitoring, FA detection**
3. **FA detection**
4. **FA detection, Integrity Check of related TSF data**

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

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

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: No dependencies.

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

Application note: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

7.1.7 Security Functional Requirements for Patch Management

FMT_SMR.1/OS-UPDATE Security roles

FMT_SMR.1.1/OS-UPDATE The TSF shall maintain the roles **OS Developer, OS Patch Loader, Issuer**.

FMT_SMR.1.2/OS-UPDATE The TSF shall be able to associate users with roles.

FMT_SMF.1/OS-UPDATE Specification of Management Functions

FMT_SMF.1.1/OS-UPDATE The TSF shall be capable of performing the following management functions: **activation of additional code.**

Application Note:

Once verified and installed, additional code is become immediately effective.

FIA_ATD.1/OS-UPDATE User attribute definition

FIA_ATD.1.1/OS-UPDATE The TSF shall maintain the following list of security attributes belonging to individual users: **additional code ID for each activated additional code**.

Refinement: "Individual users" stands for additional code.

FDP_ACC.1/OS-UPDATE Subset access control

FDP_ACC.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** on **the following list of subjects, objects and operations:**

- **Subjects: S.OS-Developer is the representative of the OS Developer within the TOE, who responsible for verifying the signature and decrypting the additional code before authorizing its loading, installation and activation, [None]**
- **Objects: additional code and associated cryptographic signature**
- **Operations: loading, installation and activation of additional code**

FDP_ACF.1/OS-UPDATE Security attribute based access control

FDP_ACF.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to objects based on the following:

- **Security Attributes:**
  - **The additional code cryptographic signature verification status**
  - **The Identification Data verification status (between the Initial TOE and the additional code)**

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

- **The verification of the additional code cryptographic signature (using D.OS-UPDATE_SGNVER-KEY) by S.OS-Developer is successful.**
- **The decryption of the additional code prior installation (using D.OS-UPDATE_DEC-KEY) by S.OS-Developer is successful.**
- **The comparison between the identification data of both the Initial TOE and the additional code demonstrates that the OS Update operation can be performed.**
- **[None]**

FDP_ACF.1.3/OS-UPDATE The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[None]**.

FDP_ACF.1.4/OS-UPDATE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[None].**

Application Note:

Identification data verification is necessary to ensure that the received additional code is actually targeting the TOE and that its version is compatible with the TOE version.

Confidentiality protection must be enforced when the additional code is transmitted to the TOE for loading (See OE.OS-UPDATE-ENCRYPTION). Confidentiality protection can be achieved either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.

FMT_MSA.3/OS-UPDATE Security attribute initialisation

FMT_MSA.3.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/OS-UPDATE The TSF shall allow the **OS Developer** to specify alternative initial values to override the default values when an object or information is created.

Application Note:

The additional code signature verification status must be set to “Fail” by default, therefore preventing any additional code from being installed until the additional code signature is actually successfully verified by the TOE.

FTP_TRP.1/OS-UPDATE Trusted Path

FTP_TRP.1.1/OS-UPDATE The TSF shall provide a communication path between itself and **remote** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[none]**.

FTP_TRP.1.2/OS-UPDATE The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/OS-UPDATE The TSF shall require the use of the trusted path for **the transfer of the additional code to the TOE.**

Application Note:

During the transmission of the additional code to the TOE for loading the confidentiality shall be ensured either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.

In case that the additional code is encrypted independently of the trusted path the ST writer can select 'none' in FTP_TRP.1.1/OS-UPDATE.

Otherwise, the trusted path shall ensure the confidentiality of the transmitted additional code. In this case the ST writer shall select 'disclosure' in FTP_TRP.1.1/OS-UPDATE.

FCS_COP.1/OS-UPDATE-DEC Cryptographic operation

FCS_COP.1.1/OS-UPDATE-DEC The TSF shall perform **Decryption of the additional code prior installation** in accordance with a specified cryptographic algorithm **[AES-CBC]** and cryptographic key sizes **[AES-256]** that meet the following: **[assignment:** AES-CBC ISO9797-M2 NIST SP800-38A**]**.

FCS_COP.1/OS-UPDATE-VER Cryptographic operation

FCS_COP.1.1/OS-UPDATE-VER The TSF shall perform **digital signature verification of the additional code to be loaded** in accordance with a specified cryptographic algorithm **[AES-CMAC]** and cryptographic key sizes **[AES-256]** that meet the following: **[assignment:** NIST SP800-38B**]**.

FPT_FLS.1/OS-UPDATE Failure with preservation of secure state

FPT_FLS.1.1/OS-UPDATE The TSF shall preserve a secure state when the following types of failures occur: **interruption or incident which prevents the forming of the Updated TOE**.

Application Note:

The OS Update operation must be either successful, or fail securely. The TOE code and identification data must be updated in an atomic way in order to always be consistent. In case of interruption or incident during the OS Update operation, the OS Developer may choose to implement any technical behavior, provided that the TOE remains in a secure state, for example by canceling the operation (the TOE remains the Initial TOE) or entering an error state, and consistency is maintained between the TOE code and the ID data. The ST writer shall describe the "secure state" to which the OS update might lead.

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 5 (EAL5) and augmented by taking the following components: ALC_DVS.2 and AVA_VAN.5.

Application note : The TOE shall protect the assets against high attack potential under the assumption that the inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol (OE.Prot_Logical_MRTD). Otherwise the confidentiality of the standard data shall be protected against attacker with at least Enhanced-Basic attack potential (AVA_VAN.3).

7.3 Security Requirements Rationale

7.3.1 Security Functional Requirements Rationale

7.3.1.1 Security Functional Requirements Rationale for MRTD

The rationale in this paragraph comes from [PP-MRTD-EAC] §6.3.1. Additions due to Active Authentication and secure messaging in personalisation are shaded.

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.Active_Auth_Proof
FAU_SAS.1				X						
FCS_CKM.1/CA	X	X	X		X					
FCS_CKM.1/KeyPair					X					X
FCS_CKM.1/PERSO		X	X							
FCS_CKM.4	X	X	X							
FCS_COP.1/SHA	X	X	X		X					
FCS_COP_1_SYM	X	X	X		X					
FCS_COP.1/SIG_VER	X		X							
FCS_COP.1/CA_MAC	X	X	X		X					
FCS_COP.1/PERSO		X	X							
FCS_COP.1/AA										X
FCS_RND.1	X		X							
FIA_AFL.1/PERSO		X	X							
FIA_UID.1/PERSO		X	X							
FIA_UAU.1/PERSO		X	X							
FIA_UID.1/MRTD	X	X	X							
FIA_UAU.1/MRTD	X	X	X							
FIA_UAU.4	X	X	X							
FIA_UAU.5	X	X	X							
FIA.UAU.6	X	X	X							
FIA_API.1/CA					X					
FIA_API.1/AA										X
FDP_ACC.1	X	X	X							
FDP_ACF.1	X	X	X							
FDP_UCT.1			X							
FDP_UIT.1		X								
FMT_SMF.1	X	X								
FMT_SMR.1	X	X								
FMT_LIM.1						X				
FMT_LIM.2						X				
FMT_MTD.1/INI_ENA				X						
FMT_MTD.1/INI_DIS				X						
FMT_MTD.1/CVCA_INI			X							
FMT_MTD.1/CVCA_UPD			X							
FMT_MTD.1/DATE			X							
FMT_MTD.1/KEY_WRITE	X									
FMT_MTD.1/CAPK		X	X		X					
FMT_MTD.1/AAK										X
FMT_MTD.1/KEY_READ	X	X	X		X					X
FMT_MTD.3			X							
FPT_EMS.1	X						X			
FPT_FLS.1							X		X	
FPT_TST.1							X		X	
FPT_PHP.3							X	X		

Table 13: 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 FIA_UID.1/MRTD, FIA_UAU.1/MRTD, FDP_ACC.1 and FDP_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5. If the Personalisation Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalisation Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the case where the CA keys are generated by the card itself), FCS_COP.1/SHA (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/SYM and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6 (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Symmetric Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/SYM (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMS.1 the confidentially of these keys.

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 in 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 in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1/MRTD and FIA_UAU.1/MRTD before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.
The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6. The SFR FIA_UAU.6 and FDP_UIT.1 requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret), FCS_CKM.1/PERSO (for secure communication during personalization phase), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.
The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.
In pre-personalisation, the SFR FCS_CKM.1/PERSO and FCS_COP.1/PERSO ensure the authenticity of data transfers after successful authentication of the pre-personalisation agent according to FIA_UID.1/PERSO and FIA_UAU.1/PERSO, with the support of FIA_AFL.1/PERSO.

The security objective **OT.Sense_Data_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP_ACC.1 and FDP_ACF.1 allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a validly verifiable certificate according FCS_COP.1/SIG_VER.
The SFR FIA_UID.1/MRTD and FIA_UAU.1/MRTD requires the identification and authentication of the inspection systems. The SFR FIA_UAU.5 requires the successful Chip Authentication (CA) before any authentication attempt as Extended Inspection System. During the protected communication following the CA the reuse of authentication data is prevented by FIA_UAU.4. The SFR FIA_UAU.6 and FDP_UCT.1 requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret), FCS_CKM.1/PERSO (for secure communication during personalization phase), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/CA_MAC for the

ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

In pre-personalisation, the SFR FCS_CKM.1/PERSO and FCS_COP.1/PERSO ensure the confidentiality of data transfers after successful authentication of the pre-personalisation agent according to FIA_UID.1/PERSO and FIA_UAU.1/PERSO, with the support of FIA_AFL.1/PERSO.

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

The security objective **OT.Identification** "Identification and Authentication of the TOE" address the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.
The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification.

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

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 travel document'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.

The security objective **OT.Prot_Malfuntion** "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.

The security objective **OT.Active_Auth_Proof** "Proof of MRTD's chip authenticity through AA" is covered by FIA_API.1/AA that proves the identity of the TOE. FCS_COP.1/AA provides the signature. FMT_MTD.1/AAK and FMT_MTD.1/KEY_READ participate to confidentiality of AA private key.

7.3.2 Security Functional Requirements Rationale for Patch Management

	O.SECURE_LOAD_ACODE	O.SECURE_AC_ACTIVATION	O.TOE_IDENTIFICATION	O.CONFID-OS-UPDATE.LOAD
FDP_ACC.1/OS-UPDATE	X	X	X	X
FDP_ACF.1/OS-UPDATE	X	X	X	X
FIA_ATD.1/OS-UPDATE			X	
FMT_MSA.3/OS-UPDATE	X	X	X	X
FMT_SMR.1/OS-UPDATE	X	X	X	X
FMT_SMF.1/OS-UPDATE	X	X	X	X
FTP_TRP.1/OS-UPDATE				X
FCS_COP.1/OS-UPDATE-DEC				X
FCS_COP.1/OS-UPDATE-VER	X			
FPT_FLS.1/OS-UPDATE	X	X	X	

Table 14: Security Functional Requirement Rationale for Patch Management

O.SECURE_LOAD_ACODE This security objective specifies that the TOE shall check the authenticity and the integrity of the additional code to be loaded. This is covered by FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, SFR FCS_COP.1/OS-UPDATE-VER that define the different access control policies for the authenticity and the integrity.
Any interruption or incident will prevent the forming and activation of the additional code. It is covered by the FPT_FLS.1/OS-UPDATE.

O.SECURE_AC_ACTIVATION This security objective specifies that the activation of the additional code and update of the Identification Data shall be performed at the same time in an atomic way. This is covered by FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE that define the different access control policies.
Any interruption or incident will prevent the forming and activation of the additional code. It is covered by the FPT_FLS.1/OS-UPDATE.

O.TOE_IDENTIFICATION This security objective specifies the identifications of both the Initial TOE and additional code. This is covered by FDP_ACC.1/OS-UPDATE , FDP_ACF.1/OS-UPDATE, FIA_ATD.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE
Any interruption or incident will prevent any change of the identification data. It is covered by the FPT_FLS.1/OS-UPDATE.

O.CONFID-OS-UPDATE.LOAD This security objective specifies that The TOE shall decrypt the additional code prior installation. This is covered by FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, FTP_TRP.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC to cover this confidentiality objective.

7.3.3 Dependency Rationale

7.3.3.1 SFR Dependencies for MRTD

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

SFR	Dependencies	Support of the dependencies
FAU_SAS.1	No dependencies	
FCS_CKM.1/CA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	**FCS_COP.1/CA_MAC,** **FCS_CKM.4**
FCS_CKM.1/KeyPair	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	**FCS_COP.1/AA**, **FCS_COP.1/CA_MAC** and **FCS_COP.1/SYM**, **FCS_CKM.4** Not fulfilled, see note in SFR description in 7.1.2-Class Cryptographic Support (FCS))
FCS_CKM.1/PERSO	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	**FCS_COP.1/PERSO,** **FCS_CKM.4**
FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1]	**FCS_CKM.1/CA** **FCS_CKM.1/PERSO**
FCS_COP.1/SHA	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	justification note 2 for non-satisfied dependencies **FCS_CKM.4**
FCS_COP.1/SYM	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/CA** **FCS_CKM.4**
FCS_COP.1/SIG_VER	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/CA** **FCS_CKM.4**
FCS_COP.1/CA_MAC	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/CA** **FCS_CKM.4**
FCS_COP.1/PERSO	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/PERSO** **FCS_CKM.4**
FCS_COP.1/AA	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/KeyPair** **FCS_CKM.4** Not fulfilled: see note 1
FCS_RND.1	No dependencies	
FIA_AFL.1/PERSO	FIA_UAU.1	**FIA_UAU.1/PERSO**
FIA_UID.1/PERSO	No dependencies	
FIA_UAU.1/PERSO	FIA_UID.1	**FIA_UID.1/PERSO**
FIA_UID.1/MRTD	No dependencies	
FIA_UAU.1/MRTD	**FIA_UID.1**	**FIA_UID.1/MRTD**
FIA_UAU.4	No dependencies	
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_API.1/CA	No dependencies	
FIA_API.1/AA	No dependencies	
FDP_ACC.1	FDP_ACF.1	**FDP_ACF.1**

SFR	Dependencies	Support of the dependencies
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	**FDP_ACC.1**, Not fulfilled: see note 3
FDP_UCT.1	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1, or FTP_TRP.1]	**FDP_ACC.1**, justification 4 for non-satisfied dependencies
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1, or FTP_TRP.1]	**FDP_ACC.1**, justification 4 for non-satisfied dependencies
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1	**FIA_UID.1/MRTD**
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/CVCA_INI	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1, FMT_SMR.1**
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1, FMT_SMR.1**
FMT_MTD.1/DATE	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/CAPK	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**
FMT_MTD.1/KEY_READ	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1, FMT_SMR.1**
FMT_MTD.3	FMT_MTD.1	**FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD**
FPT_EMS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_PHP.3	No dependencies	

Table 15: Security functional requirement dependencies

Notes:

No. 1: The dependency between FCS_COP.1/AA and FCS_CKM.4 is not fulfilled because the key is permanently stored on the card.

No. 2: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary

No. 3: The access control TSF according to FDP_ACF.1 uses security attributes having been defined during the personalisation and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

No. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1, FTP_ITC.1, FDP_IFC.1 are not applicable here.

7.3.3.2 SFR Dependencies for OS-Agility

SFRs	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/OS-UPDATE	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1/OS-UPDATE
FDP_ACF.1/OS-UPDATE	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/OS-UPDATE FMT_MSA.3/OS-UPDATE
FIA_ATD.1/OS-UPDATE	No Dependencies	No Dependencies
FMT_MSA.3/OS-UPDATE	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	See note 1 FMT_SMR.1/OS-UPDATE
FMT_SMR.1/OS-UPDATE	FIA_UID.1 Timing of identification	FIA_UID.1/CM
FMT_SMF.1/OS-UPDATE	No Dependencies	No Dependencies
FTP_TRP.1/OS-UPDATE	No Dependencies	No Dependencies
FCS_COP.1/OS-UPDATE-DEC	(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	See note 2
FPT_FLS.1/OS-UPDATE	No Dependencies	No Dependencies
FCS_COP.1/OS-UPDATE-VER	(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	See note 2

Table 16: SFR Dependencies for OS Update

Note 1: The dependency **FMT_MSA.1** of **FMT_MSA.3/OS-UPDATE** is unsupported. No history information has to be kept by the TOE.

Note 2: **FDP_ITC.1** or **FDP_ITC.2** concerns import of user data and there is no user data (only TSF code) imported by such operation. There is no key generation FCS_CKM.1 or deletion FCS_CKM.4 for OS update. Keys are imported in Pre-Personalisation and are never erased.

7.3.4 Security Assurance Requirements Rationale

EAL5 was chosen because it provides a high level of independently assured security in a planned development. It requires a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.
The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.
The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

For these additional assurance components, all dependencies are met or exceeded in the EAL5 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL5)		
ALC_DVS.2	no dependencies	-
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.5
	ADV_TDS.3	ADV_TDS.4
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.3

Table 17: SAR Dependencies

7.3.5 Security Requirements – Mutual support and internal consistency

Cf [PP-MRTD-EAC] §6.3.4

8. TOE SUMMARY SPECIFICATION

8.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the eTravel 3.1 embedded software (including the optional NVM ES) and by the chip.

8.1.1 TSFs provided by the eTravel 3.1 (MultiApp V5.1) Software

SF	Description
SF.REL	Protection of data
SF.AC	Access control
SF.SYM_AUTH	Symmetric authentication
SF.SM	Secure messaging
SF.CA	Chip Authentication
SF.TA_CER	Validity of the Certificate Chain
SF.TA_AUT	Terminal Authentication Mechanism
SF.AA	Active Authentication
SF.OSAGILITY	OS Agility Management

Table 18: Security Functions provided by the eTravel 3.1 Software

8.1.2 TSFs provided by the Thales [ST-AQU-IC]

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+. These SF are the same for the IC considered in this ST;

SF	Description
SF_PMODE	Manages the different steps of the product life cycle. At each step (boot mode, test mode and user mode), registers, data and memories accesses are limited or not. This allows to restrict product access according to the step (from manufacturing phase to final user phase). In addition, it is not possible to come back to test mode after the deployment of the product.
SF_AUDIT_STORAGE	Allows to store specific data which shall remain permanent in the system such as the unique identification of the product stored in the Flash memory, pre-personalization data and security information.
SF_AUTHENT	Provides mutual authentication between the TOE and the “Terminal” based on cryptographic mechanisms. Authentication is done before the loading operation.
SF_CONF_INT	Provides confidentiality and integrity to data stored in the memories (ROM, RAM, FLASH), in registers and in buses. The SF_CONF_INT prevents the disclosure of internal user data thanks to: ▪ Memories encryption. ▪ Buses encryption. ▪ Register masking and cycling. ▪ Address scrambling. ▪ Integrity mechanisms on memories, buses and registers.
SF_EXEC	Provides protection against an un-correct execution of the code such as: ▪ Mechanisms to detect code re-routing.

	▪ Mechanisms to detect illegal opcode execution. ▪ Mechanisms to control the operating conditions. In case of detection of an abnormal execution, an alarm is sent. Ensures also the correct operating conditions of the product during the execution and prevents any malfunction using sensors.
SF_MEM_ACCESS	Provides: ▪ A Memory Protection Unit (MPU) that defines access permission on different memories areas. ▪ A Flash Protection Unit that defines access permission on NVR areas. Provides also an access control to user data stored in Flash during the deployment of the Loader and after.
SF_PHY_PRO	Provides physical protection to the product against physical manipulation and physical probing. The following features are used: ▪ Active Shield. ▪ Countermeasures added during the layout design.
SF_ALARM	Enables to trig either an interrupt or a hardware reset. This TSF provides preservation of secure state in case of exposure to operation conditions which are not tolerated.
SF_RANDOM	Provides mechanisms to prevent access to sensitive assets during the use by the Secure Embedded Software thanks to: ▪ Generate variation of the clock frequency around a range of frequency. ▪ Randomize the clock stealer. Randomize the execution of the commands.
SF_RNG	Provides a random number generator (PTRNG) that meets PTG.2 class of BSI-AIS31 (German Scheme). It is used for key generation or for security measures.
SF_SEC_LOAD	Allows to load some code in the product in a secure way and, after the loading, to lock the loading mechanism.

Table 19: Security Functions provided by the Thales (THALES DIS FRANCE SAS) AQUARIUS_CA_09 chips

These SF are described in [ST-AQU-IC].

9. GLOSSARY AND ACRONYMS

Glossary

Term	Definition
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.
Agreement	This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Application note	Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the evaluation or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the travel document's chip to store the Initialisation Data and Pre-personalisation Data.
Authenticity	Ability to confirm that the travel document itself and the data elements stored in were issued by the travel document Issuer
Basic Access Control (BAC)	Security mechanism defined in [PKI] by which means the travel document's chip proves and the basic inspection system (with BAC) protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on travel document's chip according to LDS.
Basic Inspection System with Basic Access Control protocol (BIS-BAC)	A technical system being used by an official organisation[1] and operated by a governmental organisation and verifying correspondence between the stored and printed MRZ. BIS-BAC implements the terminal's part of the Basic Access Control protocol and authenticates itself to the travel document using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (travel document details data and biographical data) stored on the travel document. See also par. 1.2.5; also [PKI].
Biographical data (biodata)	The personalised details of the travel document holder appearing as text in the visual and machine readable zones of and electronically stored in the travel document. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document as (i) digital portrait and (ii) optional biometric reference data (e.g. finger and iris).
Card Access Number (CAN)	A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Passport), semi-static (e.g. printed on a label on the Passport) or dynamic (randomly chosen by the electronic travel document and displayed by it using e.g. ePaper, OLED or similar technologies), see [ICAO-TR-SAC]
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means [PKI].
Country Signing CertA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority and stored in the rightful terminals.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the ePass Issuer with respect to confirming correctness of user and TSF data stored in the ePass. The CSCA represents the country specific root of the PKI for the ePasss and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [PKI], 5.5.1.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KBENC) and message authentication (key KBMAC) of data

[1] an inspecting authority; concretely, by a control officer

Term	Definition
	transmitted between the TOE and an inspection system using BAC [PKI]. They are derived from the MRZ and used within BAC to authenticate an entity able to read the printed MRZ of the passport book; see [PKI].
Document Details Data	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SOD)	A RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups: A hash for each Data Group in use shall be stored in the Security Data. It is stored in the ePassport application (EF.SOD) of the travel document. It may carry the Document Signer Certificate (CDS); see [PKI], sec. A.10.4.
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the ePass for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS)(CDS), see [PKI]. This role is usually delegated to a Personalisation Agent.
Eavesdropper	A threat agent reading the communication between the travel document and the terminal to gain the data on the travel document.
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; see [PKI].
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [ICAO-TR-SAC].
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [PKI].
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 utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all travel documents; see [PKI].
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life cycle phases.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.
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; see [PKI].
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required; see [PKI].
Initialisation Data	Any data defined by the travel document manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as travel document material (IC identification data).

Term	Definition
Inspection	The act of an official organisation (inspection authority) examining an travel document presented to it by an travel document presenter and verifying its authenticity as the travel document holder. See also [PKI].
Inspection system	see BIS-BAC for general information
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements stored upon have not been altered from that created by the travel document Issuer.
Issuing Organisation	Organisation authorised to issue an official travel document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [PKI].
Issuing State	The country issuing the travel document; see [PKI].
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [PKI]. The capacity expansion technology used is the travel document's chip.
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods; see [PKI]. The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for both PACE and BAC.
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; see [PKI].
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life-cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
PACE password	A password needed for PACE authentication, e.g. CAN or MRZ.
PACE Terminal (PCT)	A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ePass using a shared password (CAN or MRZ).
Passive authentication	Security mechanism implementing (i) verification of the digital signature of the Card/Chip or Document Security Object and (ii) comparing the hash values of the read data fields with the hash values contained in the Card/Chip or Document Security Object. See [PKI].
Passport (physical and electronic)	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Passport is used in order to verify that identity claimed by the Passport presenter is commensurate with the identity of the Passport holder stored on/in the card.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [ICAO-TR-SAC]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document.
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:

Term	Definition
	(i)establishing the identity of the travel document holder for the biographic data in the travel document, (ii)enrolling the biometric reference data of the travel document holder, (iii)writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [PKI], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [PKI] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalisation Data	A set of data incl. (i) individual-related data (biographic and biometric data,) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life cycle phase card issuing.
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised travel document and/or to secure shipment within or between the life cycle phases manufacturing and card issuing.
Pre-personalised travel document's chip	travel document's chip equipped with a unique identifier and a unique Authentication Key Pair of the chip.
Receiving State	The Country to which the travel document holder is applying for entry; see [PKI].
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.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443]
Rightful equipment (rightful terminal or rightful Card)	A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either BIS-PACE (see Inspection System).
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [PKI].
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
Skimming	Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact communication channel of the TOE without knowledge of the printed MRZ and CAN dataPACE password.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [ICAO-TR-SAC], namely (i) PACE and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.
Supplemental Access Control	A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.
Terminal	A Terminal is any technical system communicating with the TOE through a contactless / contact interface.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document

Term	Definition
Travel document	Official document issued by a state or organisation 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; see [PKI] (there "Machine readable travel document").
Travel document (electronic)	The contactless/contact smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
Travel document holder	A person for whom the ePass Issuer has personalised the travel document.
Travel document Issuer (issuing authority)	Organisation authorised to issue an electronic Passport to the travel document holder
Travel document presenter	A person presenting the travel document to a terminal and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC-1]).
Unpersonalised travel document	travel document material prepared to produce a personalised travel document containing an initialised and pre-personalised travel document's chip.
User Data	All data (being not authentication data) (i)stored in the context of the ePassport application of the travel document as defined in [PKI]and (ii)being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-SAC]). CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC-1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC-2]).
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.

Acronyms

Acronym	Term
AA	Active Authentication
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [9])
BIS-PACE	Basic Inspection System with PACE
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
RF	Radio Frequency
SAC	Supplemental Access Control
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure, see [ICAO-TR-SAC]
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)