Sagem Sécurité
SAFRAN Group

Security Target

Morpho-ePass V3

Public Version

Common Criteria version 2.3
EAL 4 Augmented

(ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

Version 1.1

Sagem Sécurité
SAFRAN Group

2008

Sagem Sécurité
SAFRAN Group

TABLE OF CONTENT

1. SECURITY TARGET INTRODUCTION

1.1 SECURITY TARGET IDENTIFICATION

Document identification:

Title	:	Security Target : Morpho-ePass V3, Public version
Version	:	1.1**Erreur ! Source du renvoi introuvable.**
Document identifier	:	SSE-0000070468**Erreur ! Source du renvoi introuvable.**

TOE identification:

Commercial names	:	Morpho-ePass V3 Morpho-Citiz64
Chip identifier	:	ST19NR66-A
TOE identifier	:	MORPHOEPASSCC/ST19NR66-A/1.0.2
Administration guidance	:	SSE-0000070088 - Pre-personalisation manual SSE-0000067414 - Personalisation manual
User guidance	:	SSE-0000067415 - User manual
Installation procedure	:	SSE-0000068096 - Installation procedure
Delivery procedure	:	SSE-0000067784 - Delivery procedure

CC conformance:

Version	:	2.3
Assurance level	:	EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.
Strength of function	:	SOF – High
Chip certificate reference	:	2007/23

1.2 SECURITY TARGET OVERVIEW

This security target defines the security objectives and requirements for Morpho-ePass V3 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 of ICAO Doc 9303 [5], it also addresses Active Authentication of ICAO Doc 9303 [5].

1.3 CC CONFORMANCE

This security target claims conformance to [1], [2], [3]:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

as follows:

- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

Application note: For interoperability reasons it is assumed the receiving State cares for sufficient measures against eavesdropping within the operating environment of the inspection systems. Otherwise the MRTD may protect the confidentiality of some less sensitive assets (e.g. the personal data of the MRTD holder which are also printed on the physical MRTD) for some specific attacks only against low attack potential (AVA_VLA.2).

This security target is also compliant with [PP-EAC]:

- Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control – BSI-PP-0026 – version 1.2, 19th November 2007.

1.4 DOCUMENT REFERENCE

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001.

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-003

[5] ICAO Doc 9303, Sixth Edition, 2007

[8] Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standards (DES), Reaffirmed 1999 October 25, U.S. Department Of Commerce / National Institute of Standards and Technology.

[15] ISO/IEC 15946 : Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3 : Key establishment, 2002.

[16] PKCS#3 : Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993.

[20] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.1, TR-03110, Bundesamt für Sicherheit in des Informationstecnik (BSI).

[21] Technical Guideline :Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.

[22] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004

[CPS] EMV CPS 1.0 Final 16 June 2003

[IAS v1] Plate-forme commune pour l'eAdministration – Spécification technique – Version 1.0.1, Erratum à la version 1.0.1

[ISO-7816] ISO 7816: Identification Cards – Integrated Circuit(s) Cards with Contacts

[PP-EAC] Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control – BSI-CC-PP-0026 – version 1.2, 19th November 2007.

1.5 GLOSSARY

Active Authentication
Security mechanism defined in [5] by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization.

Application note
Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the use of the ST.

Audit records
Write-only-once non-volatile memory area of the MRTD's chip to store the Initialization Data and Pre-personalization Data.

Authenticity
Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.

Basic Access Control
Security mechanism defined in [5] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Basic Access Keys (see there).

Basic Inspection System (BIS)
An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys drawn from printed MRZ data for reading the logical MRTD.

Biographical data (biodata)
The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa [5].

Biometric reference data
Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.

Certificate chain
Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).

Counterfeit
An unauthorized copy or reproduction of a genuine security document made by whatever means [5].

Country Signing CA Certificate (CCSCA)
Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority stored in the inspection system.

Country Verifying Certification Authority
The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing Country or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.

Current date
The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.

CVCA link Certificate
Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.

Document Basic Access Key Derivation Algorithm
The [5] normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

Document Basic Access Keys
Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [5]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.

Document Security Object (SOD)
A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS) [5].

Document Verifier
Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations

Eavesdropper
A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.

Enrolment
The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity [5].

Extended Access Control
Security mechanism identified in [5] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.

Extended Inspection System
A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Extended Inspection System (EIS)
A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.

Forgery
Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait [5].

General Inspection System
A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.

Global Interoperability
The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs [5].

IC Dedicated Support Software
That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

IC Dedicated Test Software
That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

Impostor
A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document [5].

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 [5].

Initialization Data
Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).

Inspection
The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity[5].

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

Integrated Circuit (IC)
Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.

Integrity
Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization.

Issuing Organization
Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer) [5].

Issuing State
The Country issuing the MRTD [5].

Logical Data Structure (LDS)
The collection of groupings of Data Elements stored in the optional capacity expansion technology [5]. The capacity expansion technology used is the MRTD's chip.

Logical MRTD
Data of the MRTD holder stored according to the Logical Data Structure [5] 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
- the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
- the digitized portraits (EF.DG2),
- the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and
- the other data according to LDS (EF.DG5 to EF.DG16).

Logical travel document
Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to):

- data contained in the machine-readable zone (mandatory),
- digitized photographic image (mandatory) and
- fingerprint image(s) and/or iris image(s) (optional).

Machine readable travel document (MRTD)
Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read [5].

Machine readable visa (MRV)
A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport [5].

Machine readable zone (MRZ)
Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods [5].

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 [5].

MRTD application
Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes :

- the file structure implementing the LDS [5],
- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13 and EF.DG16) and

- the TSF Data including the definition the authentication data but except the authentication data itself.

MRTD Basic Access Control
Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.

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

MRTD's Chip
A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO, [5], p. 14.

MRTD's chip Embedded Software
Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.

Optional biometric reference data
Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.

Passive authentication
(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.

Personalization
The process by which the portrait, signature and biographical data are applied to the document [5].

Personalization Agent
The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.

Personalization Agent Authentication Information
TSF data used for authentication proof and verification of the Personalization Agent.

Personalization Agent Authentication Key
Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.

Physical travel document
Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) :

- biographical data,
- data of the machine-readable zone,
- photographic image and
- other data.

Pre-personalization Data
Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2

and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.

Pre-personalized MRTD's chip
MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.

Receiving State
The Country to which the MRTD holder is applying for entry [5].

Reference data
Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

Secondary image
A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means [5].

Secure messaging in encrypted mode
Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4

Skimming
Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.

Terminal Authorization
Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be all valid for the Current Date.

Travel document
A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel [5].

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

TSF data
Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).

Unpersonalized MRTD
MRTD material prepared to produce a personalized MRTD containing an initialized and pre-personalized MRTD's chip.

User data
Data created by and for the user that does not affect the operation of the TSF (CC part 1 [1]).

Verification
The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template [5].

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.

1.6 ACRONYMS

AAP	Active Authentication Protocol
BAC	Basic Access Control
BIS	Basic Inspection System
BT	Basic Terminal
CA	Certification Authority
CAP	Chip Authentication Protocol
CC	Common criteria
CVCA	Country Verifying Certification Authority
DG	Data Group
DH	Diffie-Hellman
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EIS	Extended Inspection System
GIS	General Inspection System
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IS	Inspection System
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRV	Machine Readable Visa
MRZ	Machine Readable Zone
OCR	Optical Character Recognition
OSP	Organizational Security Policies
PKI	Public Key Infrastructure
PP	Protection Profile
PT	Personalization Terminal
SAR	Security Assurance Requirements

SFR	Security Functional Requirements
ST	Security Target
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSP	TOE Security Policy
TSF	TOE Security Functions

2. TOE DESCRIPTION

2.1 TOE DEFINITION

The Target Of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [5] and providing Basic Access Control and Extended Access Control according to the ICAO Doc 9303[5] and BSI TR-03110 [20], respectively. The TOE may also provide Active Authentication according to [5].

The TOE comprises of:

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

Application note :

- The IC is the ST19NR66-A and is provided by STMicroelectronics. The ST19NR66-A has been evaluated at EAL5+ level and certified with certificate reference 2007/23. The IC embeds libraries (system ROM library, cryptographic library for DES, Elliptic Curves Cryptography and RSA algorithm).
- As the antenna has no relevant impact on the security of the product, the TOE reaches the same level of assurance with any antenna. Therefore no specific antennae is identified, neither any inlay design.
- The IC dedicated software has been evaluated during the chip evaluation. Moreover, the IC Dedicated Test software is invalidated after TOE delivery.
- Personalization of the Morpho-ePass V3 is performed by a dedicated application.
- Another application is embedded in the Morpho-ePass V3, but is not included in the TOE boundary.
- A contact interface compliant with [ISO-7816] may also be available to communicate with the TOE.

2.2 TOE USAGE AND SECURITY FEATURES FOR OPERATIONAL USE

State or Organization issues MRTD to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary

(MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

In 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) logical MRTD as data of the MRTD holder stored according to the Logical Data Structure [5] 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) [5]. 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 [5]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism and the Extended Access Control Mechanism. This security target addresses the Chip Authentication described in [20] as an alternative to the Active Authentication stated in [5].

The Basic Access Control is a security feature that shall be mandatory implemented by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip

provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [5] normative appendix 5.

This security target requires the TOE to implement the Chip Authentication defined in [20]. The Chip Authentication prevents data traces described in [5] normative 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 a 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. it could apply the Chip Authentication Private Key corresponding to the Chip Authentication Public Key for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

Application note: The Active Authentication, described in [5], may also be available, as an additional feature to those described in the PP MRTD ICAO [PP-EAC]. Active Authentication is a digital security feature that prevents cloning by introducing a chip-individual key pair:

- *The public key is stored in data group EF.DG15 and is thus protected by Passive Authentication.*
- *The corresponding private key is stored in a secure manner and may only be used internally by the MRTD chip and cannot be read out.*

Thus, the chip can prove knowledge of this private key in a challenge-response protocol, which is called Active Authentication. In this protocol the MRTD chip digitally signs a challenge randomly chosen by the inspection system. The inspection system recognizes that the MRTD chip is genuine if and only if the returned signature is correct.

This security target requires the TOE to implement the Extended Access Control as defined in [20]. 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) established secure messaging, which is used by Terminal Authentication, to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication can only be performed if Chip Authentication has been successfully executed. The Terminal Authentication Protocol consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

2.3 EMBEDDED SOFTWARE ARCHITECTURE

The Morpho-ePass V3 embeds the following applications:

- AIP Application, compliant with **[CPS]**, which performs the pre-personalization and the personalization operations of the Morpho-ePass V3. This application is not accessible once in Operational Use phase.

- ICAO Application, which performs all the electronic passport operations during the Operational Use phase.

- IAS Application, compliant with **[IAS v1]**, which performs electronic administration operations during the Operational Use phase. There might be none, one or several instances of the IAS application. This application is outside the scope of the evaluation.

The application manager is in charge of the use of the different applications: the application manager dispatches each received command to the right application, therefore enforcing domain separation between applications.

The architecture of the Morpho-ePass V3 is given in Fig 1.

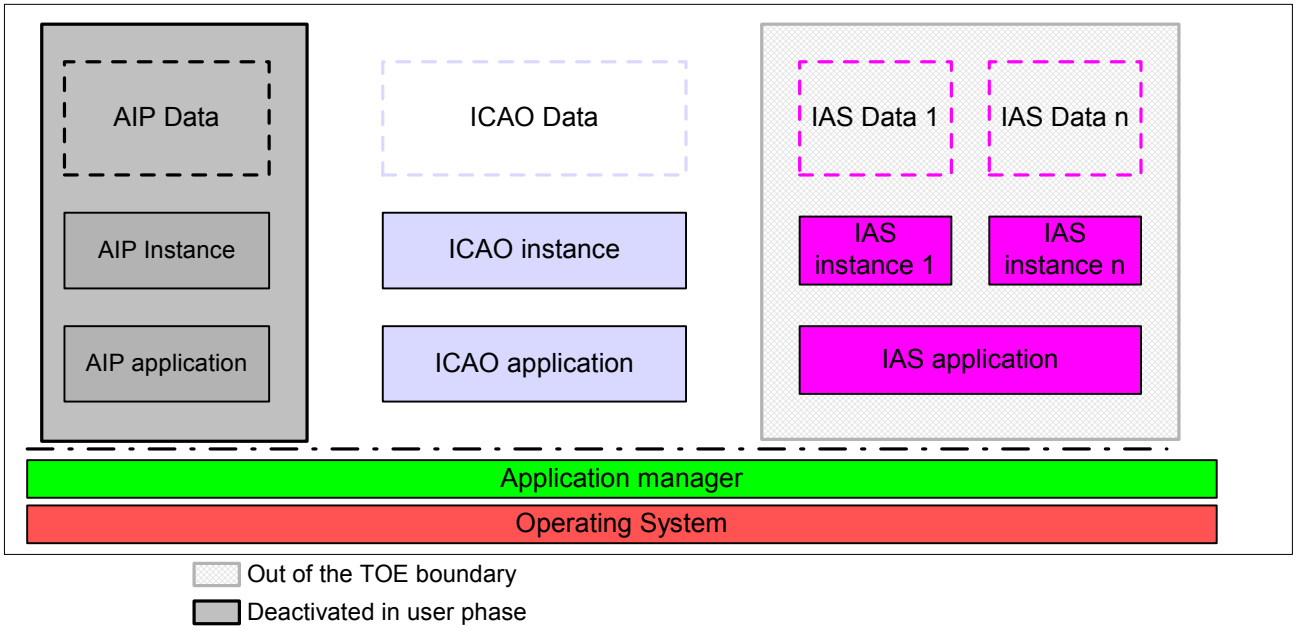

Fig 1 : Architecture of the Morpho-ePass V3

2.4 TOE LIFE CYCLE

The life cycle of the TOE as a MRTD is described in terms of the four life cycle phases.

Phase 1 "Development"

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.

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

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

Phase 2 "Manufacturing"

In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material

during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

The MRTD manufacturer (i) adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance E²PROM) if necessary, (ii) creates the MRTD application, (iii) equips MRTD's chips with pre-personalization Data, and (iv) combines the IC with hardware for the contactless interface in the passport book.

Application Note : The IC manufacturer might perform some of the tasks of the MRTD manufacturer, such as adding parts of the IC Embedded Software in the non-volatile programmable memories or equips MRTD's chips with some pre-personalization Data for instance. As Manufacturer is a generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip and as the TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer, this has no impact on the TOE.

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.

Application Note: The TOE is considered to be already protected during encapsulation, inlay manufacturing (steps 4 and 5 of the smart card life cycle) and inclusion of the inlay in the booklet, as these steps have no security impact on the TOE. Moreover, the TOE may not yet be included in the passport booklet at TOE delivery to the Personalization Agent. As the passport booklet provides no protection to the TOE, this has no security impact on the TOE.

Phase 3 "Personalization of the MRTD"

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) the writing of the TSF Data into the logical MRTD and 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.

Application note : This security target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [5]. This approach allows but does not enforce the separation of these roles.

Phase 4 "Operational Use"

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

The TOE is a smart card, whose life cycle may be divided into 7 steps:

Step 1 Development of the smart card embedded software
Sagem Sécurité is in charge of the development of the smart card integrated software and of the specification requirements for the initialization of the integrated circuit.

Step 2 Integrated Circuit (IC) Development
STMicroelectronics designs the IC, develops the dedicated software IC and transmits the information, the software and the tools to the developer's embedded software (Sagem Sécurité), by protected verification and delivery procedures. From the integrated circuit, the dedicated software and the embedded software, they build the integrated circuit smart card data base, indispensable for creating the integrated circuit mask.

Step 3 Manufacture and test of the integrated circuit
STMicroelectronics is in charge of the production of the integrated circuit which occurs in three principal steps: manufacture, test and initialization of the integrated circuit.

Step 4 Encapsulation and test of the integrated circuit
The integrated circuit packaging manufacturer is in charge of packaging (encapsulation) and testing of the integrated circuit.

Step 5 Smart card product Finish
The smart card manufacturer is in charge of finishing and testing the smart card.

Step 6 Smart card personalization
The personalizer is in charge of personalizing the smart card and performing final tests.

Step 7 Smart card use
The smart card issuer is in charge of product delivery to the end user, as well as for the end of the life cycle.

The whole TOE life cycle is summarized in Fig 2.

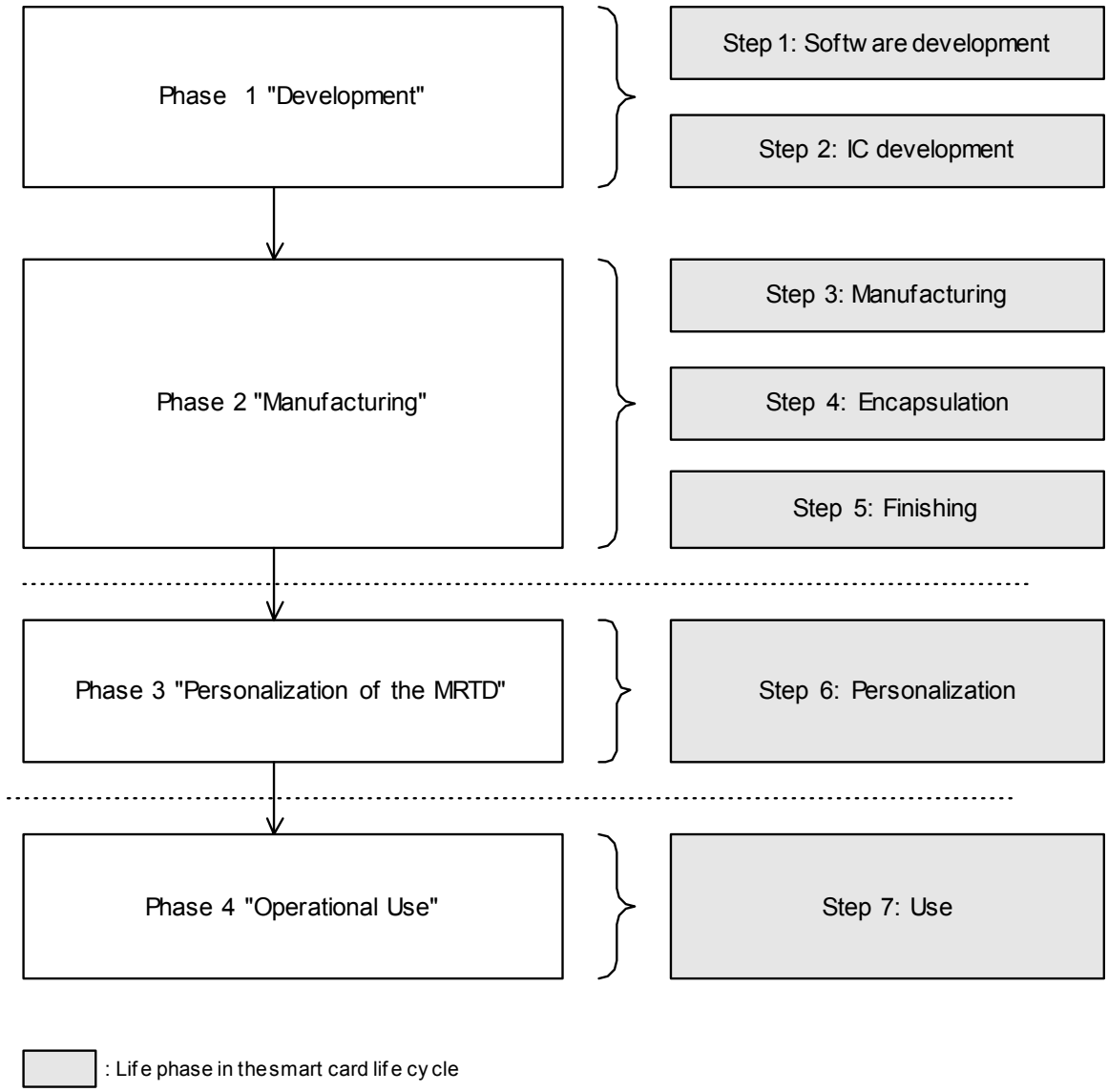

Fig 2 : TOE life cycle

3. TOE SECURITY ENVIRONMENT

3.1 ASSETS

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

Logical MRTD Data

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [5]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG14) is used by the inspection system for the Chip Authentication. The EF.DG15 is dedicated to contain the Active Authentication public key to be used by the inspection system for the Active Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Even if all assets could be protected with a high security level (with the EAC mechanisms), some of them called later "standard data", have to be accessible through a mechanisms with a lower security level (BAC mechanisms). This is due to interoperability reasons as the ICAO Doc 9303 [5] specifies only the BAC mechanisms.

Logical MRTD standard User Data

- Personal Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG16)
- Active Authentication Public Key in EF.DG15
- Chip Authentication Public Key in EF.DG14
- Document Security Object (SOD) in EF.SOD
- Common data in EF.COM

Logical MRTD sensitive User Data

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

A sensitive asset is the following more general one.

Authenticity of the MRTD's chip

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

3.2 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

This 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 define in [5].

Country Verifying Certification Authority

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

Document Verifier

The Document Verifier (DV) enforces the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The 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 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 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 additional the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (iii) 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.

Application note: The Extended Inspection System may also implement the terminal part of the Active Authentication Protocol.

Application note : According to [5] the support of (i) the Passive Authentication mechanism is mandatory, and (ii) the Basic Access Control is optional. In the context of this security target the Primary Inspection System does not implement the terminal part of the Basic Access Control. It is therefore not able to read

the logical MRTD because the logical MRTD of the TOE is protected by Basic Access Control. Therefore this security target will not consider the use of Primary Inspection System by the receiving State or Organization. The TOE of the current security target does not allow the Personalization Agent to disable the Basic Access Control for use with Primary Inspection Systems.

MRTD Holder

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

Traveler

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

Attacker

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

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

3.3 ASSUMPTIONS

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

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 bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A_Pers_Agent_Active_Auth ***Personalization of the MRTD's chip including Active Authentication***

The Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip. 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 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 [5]. The Basic Inspection System reads the logical MRTD being 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_Insp_Sys_Active_Auth ***Inspection Systems for global interoperability supporting Active Authentication***

The Extended Inspection System in addition may also support the terminal part of the Active Authentication Protocol.

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 (i) securely generates, stores and uses the Country Signing CA Key pair, and (ii) manages the MRTD's Chip Authentication Key Pairs. The CA keeps the Country Signing CA Private Key secret and distributes 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 aver 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 and distributes them to the receiving States or Organizations.

A.Auth_PKI **PKI for Inspection System**

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.

3.4 THREATS

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

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

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

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTS's chip by establishing or listening a communication through the contactless communication interface. The attacker cannot read optically and does not know in advance the physical MRTD.

T.Skimming **Skimming the logical MRTD**

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker cannot read and does not know in advance the physical MRTD.

T.Read_Sensitive_Data Read the sensitive biometric reference data

An attacker with high attack potential knowing the document Basic Access Keys is trying 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 threats T.Skimming in respect of the attack path (communication interface) and 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 visual readable on the physical MRTD as well.

T.Forgery Forgery of data on MRTD's chip

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose 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 forge MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveler into an other 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 in another contactless chip.

T.Counterfeit MRTD's chip

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.

The TOE shall avert the threats as specified below.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in TOE operational 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.

T.Infomation_Leakage Information Leakage from MRTD's chip

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 to actively enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Phys-Tamper Physical Tampering

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 TDF 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.

T.Malfunction Malfunction due to Environmental Stress

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 (iii) 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.

3.5 ORGANIZATIONAL SECURITY POLICIES

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

P.Manufact Manufacturing of the MRTD's chip

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing. 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 Sate or Organization only.

P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are

intended to be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an inspection system. Additional to the Basic Access Control Authentication defined by ICAO in [5] the MRTD's chip shall protect the confidentiality and integrity of the personal data during transmission to the General Inspection system after chip authentication.

Application note : The organizational security policy P.Personal_Data is drawn from the ICAO document [5]. Note, that the Document Basic Access Key is defined by the TOE environment and loaded by the Personalization Agent.

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. The issuing State or Organization authorizes the Document Verifiers if the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate.

4. SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [5] 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) cannot be changed by write access after personalization.

(2) The Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly.

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.Data_Conf Confidentiality of personal data

The TOE must ensure the confidentiality of the data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 and the Document Security Object of the logical MRTD by granting read access to terminals successfully authenticated by as (i) Personalization Agent or (ii) Basic Inspection System or (iii) Extended Inspection System. The TOE implements the Basic Access Control as defined by ICAO [5] and enforces Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the General Inspection system after Chip Authentication.

Application note : The traveler grants the authorization for reading the standard user data to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication independent on the quality of the Document Basic Access Keys which is defined by the TOE environment and loaded into the TOE by the Personalization Agent. Any attack based on decision of the ICAO document [5] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective OT.Data_Conf (Cf. CEM [4], section 8.10.3.4, para. 1625).

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 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 Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 « Manufacturing » and Phase 3 « Personalization of the MRTD ». In Phase 4 « Operational Use », the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

Application note : The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 « Manufacturing » and for traceability and/or to secure shipment of the TOE from Phase 2 « Manufacturing » into the Phase 3 « Personalization of the MRTD ». The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing environment as described in its security objective OD.Material. In the Phase 4 « Operational Use » the TOE is identified by the passport number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit serial number ICCSN) or a MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

OT.Chip_Auth_Proof Proof of MRTD's chip authenticity

The TOE must support the General Inspection System 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 [20]. The authenticity prove 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 fit to 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 [5] and (ii) the hash value of the Authentication Public Key in the Document Security Object signed by the Document Signer.

OT.Active_Auth_Proof Proof of MRTD's chip authenticity by Active Authentication

The TOE may support the Extended Inspection System 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 [5].

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

OT.PROT_Abuse-Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded

Software, (iii) to manipulate Soft-coded Smartcard 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 chip 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.

Application note : In order to meet the security objective OT.Prot_Phys-Tamper the TOE must designed and fabricated so that it requires a high combination complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack. This is addressed by the security objective OD.Assurance.

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.

4.2 SECURITY OBJECTIVES FOR THE DEVELOPMENT AND MANUFACTURING ENVIRONMENT

OD.Assurance Assurance Security Measures in Development and manufacturing environment

The developer and manufacturer ensure that the TOE is designed and fabricated such that it requires a combination of complex equipment, knowledge, skill and time to be able to derive detailed design information or other information which could be used to compromise security through attack. This includes the use of Initialization Data for unique identification of the TOE and the pre-personalization of the TOE including the writing of the Personalization Agent Authentication key(s). The developer provides necessary evaluation evidence that the TOE fulfills its security objectives and is resistant against obvious penetration attacks with high attack potential.

OD.Material Control over MRTD Material

The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, initialize, pre-personalize genuine MRTD's materials and to personalize authentic MRTDs in order to prevent counterfeit of MRTDs using MRTD materials.

4.3 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

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 Signing 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 Signing 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 [5].

OE.Auth_Key_MRTD MRTD Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's 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 he Document Security Object.

OE.Active_Auth_Key_MRTD ***MRTD Active Authentication Key***

The issuing State or Organization may establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) 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 he 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.

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 must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key, and (ii) implements the terminal part of the Basic Access Control [5]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

OE.Exam_MRTD_Active_Auth ***Examination of the MRTD passport book using Active Authentication***

During examination of the MRTD presented by the traveler, the Extended Inspection Systems may perform the Active 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 Public Key and the Document Signing Public Key maintaining their authenticity and availability in all inspection systems.

OE.Prot_Logical_MRTD **Protection of data of the logical MRTD**

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

Application note : The figure 2.1 in [20] 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 after which 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 PP. 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.

5. SECURITY FUNCTIONAL REQUIREMENTS

5.1 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.

Tab 1 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. [20] 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.
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.
Active Authentication Key Pair	The Active Authentication Key Pair (KPrAA, KPuAA) is used for Active Authentication Protocol: RSA according to ISO9796-2 Digital Signature scheme 1
Active Authentication Public Key	The Active Authentication Public Key (KPuAA) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Active Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.

Name	Data
Active Authentication Private Key	The Active Authentication Private Key (KPrAA) is used by the TOE to authenticate itself as authentic MRTD's chip using the Active Authentication protocol. 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 System 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.

Tab 1 : Keys and certificates overview

Application note: The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same country 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 country as the Country Verifying Certification Authority. From MRTD's point of view the domestic Document Verifier belongs to the issuing Country or Organization.

5.1.1 Class FAU Security Audit

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

FAU_SAS.1 Audit storage

FAU_SAS.1.1	The TSF shall provide **[assignment : authorized users]** with the capability to store **[assignment : list of audit information]** in the audit records.
Assignment	Authorized users : **the Manufacturer** List of Audit Information : **the IC Identification Data**

Application note : The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS). The security measures in the manufacturing environment assessed under ADO_IGS and ADO_DEL ensure that the audit records will be used to fulfill the security objective OD.Assurance.

5.1.2 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 keys generation algorithms to be implemented and key to be generated by the TOE.

FCS_CKM.1/KDF_MRTD Cryptographic key generation – Key Derivation Function by the MRTD

FCS_CKM.1.1 / KDF_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment : cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	Cryptographic key generation algorithm : **Document Basic Access Key Derivation Algorithm** Cryptographic key sizes : **112 bits** List of standards : **[5] normative appendix 5**

Application note :The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [5] normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC BAC Session Keys for secure messaging by the algorithm in [5] normative appendix 5, A5.1. The TOE uses this key derivation function to derive other session keys from shared secrets established by the Chip Authentication Protocol for the secure messaging required by FCS_COP.1/ENC_MRTD and FCS_COP.1/MAC_MRTD as well. The TOE may use this key derivation function for authentication of the Personalization Agent. The algorithm uses the random number RND.ICC generated by the TSF as required by FCS_RND.1/MRTD.

FCS_CKM.1/DH_MRTD Cryptographic key generation – Key Derivation Function by the MRTD

FCS_CKM.1.1 / DH_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment : cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	Cryptographic key generation algorithm : ***See Tab 2*** Cryptographic key sizes : ***See Tab 2*** List of standards : **[20], Annex A.1**

Cryptographic key generation algorithm	Cryptographic key size	Standard
Diffie-Hellman Protocol (PKCS#3)	***1024, 1536 and 2048 bits***	***[20], Annex A.1 and [16]***
ECDH (ISO 15946)	***192, 224 and 256 bits***	***[20], Annex A.1 and [15]***

Tab 2 : Cryptographic key generation methods

Application note : The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [20], sec. 3.1 and Annex A.1. This protocol is based on the Diffie-Hellman Protocol compliant to PKCS#3 (i.e. a modulo arithmetic based cryptographic algorithm, cf. [16]) or on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf.[20], Annex A.1, [21] and [15] for details). The shared secret value is used to derive the 112 bit Triple-DES key for encryption and the 112 bit Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [5] normative appendix 5, A5.1, for the TSF required by FCS_COP.1/ENC_MRTD and FCS_COP.1/MAC MRTD.

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 – MRTD

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment : cryptographic key destruction method]** that meets the following : **[assignment : list of standards]**.
Assignment	Cryptographic key destruction method : ***Overwriting of data*** List of standards : ***none***

Application note : The TOE shall destroy the BAC Session Keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip authentication Protocol. The TOE shall destroy the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

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

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

FCS_COP.1.1 / SHA_MRTD	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **hashing** Cryptographic algorithm : ***SHA-1, SHA224, SHA-256*** Cryptographic key sizes : **none** List of standards : **FIPS 180-2**

Application note : The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism (cf. [5] normative appendix 5, A5.1). The Chip Authentication Protocol may use SHA-1 (cf. [20], Annex A.1.1). The TOE implements additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol (cf. [20], Annex A.2.2 for details).

FCS_COP.1/TDES_MRTD Cryptographic operation – Encryption / Decryption Triple DES

FCS_COP.1.1 /	The TSF shall perform **[assignment : list of cryptographic operations]** in

TDES_MRTD	accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **secure messaging – encryption and decryption** Cryptographic algorithm : **Triple-DES in CBC mode** Cryptographic key sizes : **112 bits** List of standards : **FIPS 46-3 [8] and [5] normative appendix 5, A5.3**

Application note : This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of (i) the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/KDF_MRTD or (ii) the Chip Authentication Protocol according to the FCS_CKM.1/DH_MRTD. Note the Triple-DES in CBC mode with zero initial vector include also the Triple-DES in ECB mode for blocks of 8 byte used to check the authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

FCS_COP.1.1 / MAC_MRTD	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **secure messaging – message authentication code** Cryptographic algorithm : **Retail MAC** Cryptographic key sizes : **112 bits** List of standards : **ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)**

Application note : This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism as part of (i) the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/KDF_MRTD or (ii) the Chip Authentication Protocol according to the FCS_CKM.1/DH_MRTD.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD

FCS_COP.1.1 / SIG_VER	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **digital signature verification** Cryptographic algorithm : ***See Tab 3***

	Cryptographic key sizes : ***See Tab 3*** List of standards : ***See Tab 3***

Cryptographic algorithm	Cryptographic key size	Standard
RSA	***1024, 1536 and 2048 bits***	***RSASSA-PKCS1-v1_5***
ECDSA	***192, 224 and 256 bits***	***ISO15946 ECDSA***

Tab 3 : Cryptographic signature verification methods

Application note : The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

The TOE shall meet the requirement « Quality metric for random numbers (FCS_RND.1) » as specified below (Common Criteria Part 2 extended).

FCS_COP.1/SIG_GEN Cryptographic operation – Signature generation by MRTD

FCS_COP.1.1 / SIG_VER	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : ***digital signature generation*** Cryptographic algorithm : ***RSA*** Cryptographic key sizes : ***1024, 1536 and 2048 bits*** List of standards : ***ISO9796-2 Digital Signature scheme 1***

Application note : The signature generation is used during the Active Authentication Protocol.

FCS_RND.1/MRTD Quality metric for random numbers

FCS_RND.1.1 / MRTD	The TSF shall provide a mechanism to generate random numbers that meet **[assignment : a defined quality metric]**.
Assignment	A defined quality metric: ***AIS31 Class P2 quality metric***

Application note : This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4/MRTD. *Those random numbers are 8 byte long and are generated by the TOE to prevent authentication replay.*

5.1.3 Class FIA Identification and Authentication

Application note : Tab 4 provides an overview on the authentication mechanism used.

Name	**SFR for the TOE**	**SFR for the TOE environment (terminal)**	**Algorithms and key sizes according to [5] normative appendix 5 and [20]**

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [5] normative appendix 5 and [20]
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys
Basic Access Control Authentication Mechanism	FIA_AFL.1, FIA_UAU.4/MRTD FIA_UAU.6/MRTD	FIA_UAU.4/BT FIA_UAU.6/BT	Triple-DES, 112 bit keys and Retail-MAC, 112 bit keys
Chip Authentication Protocol	FIA_API.1/CAP, FIA_UAU.5/MRTD FIA_UAU.6/MRTD	FIA_UAU.4/GIS FIA_UAU.5/GIS FIA_UAU.6/GIS	DH or ECDH and Retail-MAC, 112 bit keys
Active Authentication Protocol	*FIA_API.1/CAP*	*FIA_UAU.4/EIS*	*ISO9796-2 Digital Signature scheme 1*
Terminal Authentication Protocol	FIA_UAU.5/MRTD	FIA_API.1/EIS	RSASSA-PKCS1-v1_5 or EC-DSA with SHA

Tab 4 : Overview on authentication SFR

Note the Chip Authentication Protocol includes the asymmetric key agreement and 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 TOE shall meet the requirement « Timing of identification (FIA_UID.1) » as specified below (Common Criteria Part 2).

FIA_UID.1 Timing of identification

FIA_UID.1.1	The TSF shall allow **[assignment : list of TSF-mediated actions]** on behalf of the user to be performed before the user is identified.
Assignment	List of TSF-mediated actions: **(1) to established the communication channel,** **(2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS**
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note : The MRTD's chip and the terminal establish the communication channel through the contactless following type B protocol. The protocol type B is managed through the commands "Answer to Request" and "Answer to Attrib". Note, that the terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal for communication with more than one RFID.

Application note : In the "Operation Use" phase the MRTD must not allow anybody to read the ICCSN or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note, that the terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal for communication with more than one RFID.

Application note : The identifier used by the terminal and the MRTD's chip for communication is randomly selected, so it does not violate the OT.Identification.

Application note : In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System. After successful authentication as Basic Inspection System the terminal may identify itself as Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or (ii) if necessary and available as Personalization Agent by selection of the Personalization Agent Authentication Key.

Application note: The Manufacturer loads the Personalization Agent key and switches the card to the Personalization phase. In the Personalization phase, the Personalization Agent is the only user role known to the TOE. The Personalization Agent writes in the MRTD all the secret authentication keys. Then the Personalization Agent switches the card to the Operational Use phase. The Personalization Agent authentication is no more available in Operational Use phase.

The TOE shall meet the requirement « Timing of authentication (FIA_UAU.1) » as specified below (common criteria part 2).

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow **[assignment : list of TSF-mediated actions]** on behalf of the user to be performed before the user is authenticated.
Assignment	List of TSF-mediated actions: **(1) to established the 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**
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

The TOE shall meet the requirement of « Single-use authentication mechanism (FIA_UAU.4) » as specified below (common criteria part 2).

FIA_UAU.4/MRTD Single-use authentication mechanism – Single-use authentication of the Terminal by the TOE

FIA_UAU.4.1 / MRTD	The TSF shall prevent reuse of authentication data related to **[assignment : identified authentication mechanism(s)]**.
Assignment	Identified authentication mechanism(s): **(1) Basic Access Control Authentication Mechanism,** **(2) Terminal Authentication Protocol,** **(3) Authentication Mechanism based on Triple-DES**

Application note : All listed authentication mechanisms use a challenge of 8 Bytes freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt: The Basic Access Control Authentication Mechanism, the Terminal Authentication Protocol and the Authentication Mechanism based on Triple-DES use RND.ICC [20].

Application note : The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [5]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In the first step the TOE sends a randomly chosen challenge which shall contain sufficient entropy to prevent T.Chip_ID. In the second step the MRTD's chip provides a challenge-response-pair which allows the terminal a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop the communication with the terminal not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

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

FIA_UAU.5/MRTD Multiple authentication mechanisms

FIA_UAU.5.1 / MRTD	The TSF shall provide **[assignment : list of multiple authentication mechanisms]** to support user authentication.
Assignment	List of multiple authentication mechanisms: **(1) Basic Access Control Authentication Mechanism,** **(2) Terminal Authentication Protocol,** **(3) Secure messaging in MAC-ENC mode,** **(4) Symmetric Authentication Mechanism based on Triple-DES**
FIA_UAU.5.2 / MRTD	The TSF shall authenticate any user's claimed identity according to the **[assignment : rules describing how the multiple authentication mechanisms provide authentication]**.
Assignment	Rules describing how the multiple authentication mechanisms provide authentication: **(1) The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms:** **a) the Basic Access Control Authentication Mechanism with Personalization Agent Keys,** **b) the Symmetric Authentication Mechanism with Personalization Agent Key,** **c) the Terminal Authentication Protocol with Personalization Agent Keys.** **(2) The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.** **(3) After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging with the key agreed upon with the authenticated terminal by means of the Basic Access Control Authentication Mechanism.** **(4) After run of the Chip Authentication Mechanism 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.**

	(5) The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism.

Application note : Depending on the authentication methods used the Personalization Agent holds (i) a pair of a Triple-DES encryption key and a retail-MAC key for the Basic Access Control Mechanism specified in [5], or (ii) a Triple-DES key for the Symmetric Authentication Mechanism or (iii) an asymmetric key pair for the Terminal Authentication Protocol (e.g. provided by the Extended Access Control PKI in a valid card verifiable certificate with appropriate encoded access rights). The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

Application note : In the context of this Security Target, the Personalization Agent only holds a Triple-DES key for the Symmetric Authentication Mechanism to get authenticated to the TOE and can only get authenticated to the TOE in Personalization Phase.

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

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

FIA_UAU.6.1 / MRTD	The TSF shall re-authenticate the user under the conditions **[assignment : list of conditions under which re-authentication is required]**.
Assignment	List of conditions under which re-authentication is required: **(1) Each command sent to the TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS.** **(2) Each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.**

Application note : The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [5] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC_MRTD for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accept only those commands received from the initially authenticated user.

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

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1	The TSF shall detect when **[selection : [assignment : positive integer number], an administrator configurable positive integer within [assignment : range of acceptable values]** unsuccessful authentication attempts occur related to **[assignment : list of authentication events]**.

Selection	***32 successive***
Assignment	List of authentication events: ➢ ***Failure of a TDES based Authentication attempt***
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment : list of actions]**.
Assignment	List of actions : ***Blocking the cryptographic key related to the authentication***

Application note : These assignments have been assigned to ensure especially the high strength of authentication function as terminal part of the Basic Access Control Authentication Protocol or (if necessary) of the Extended Access Control Authentication Protocol. The terminal challenge eIFD and the TSF response eICC are described in [20], Appendix C. The refinement by inclusion of the word "consecutive" allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the "consecutive unsuccessful authentication attempts" are count independent on power-on sessions but reset to zero after successful authentication only.

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

FIA_API.1/CAP	**Authentication Proof of Identity - MRTD**
FIA_API.1.1 / CAP	The TSF shall provide a **[assignment : authentication mechanism]** to prove the identity of the **[assignment : authorized user or rule]**.
Assignment	Authentication mechanism: **Chip Authentication Protocol according to [20]** Authorized user or rule : **TOE**

Application note : This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [20]. 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 [5] 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/AAP	***Authentication Proof of Identity – MRTD using Active Authentication***
FIA_API.1.1 / CAP	The TSF shall provide a **[assignment : authentication mechanism]** to prove the identity of the **[assignment : authorized user or rule]**.
Assignment	Authentication mechanism: ***Active Authentication Protocol according to [5]*** Authorized user or rule : ***TOE***

Application note : The TOE may implement the Active Authentication Mechanism specified in [5]. The terminal randomly generates a challenge, then the MRTD chip digitally signs this challenge using RSA and finally the terminal verifies that the returned signature is correct.

5.1.4 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
FDP_ACC.1.1	The TSF shall enforce the **[assignment : access control SFP]** on **[assignment: list of subjects, objects and operations among subjects and objects covered by the SFP]**.
Assignment	Access control SFP : **Access Control SFP** List of subject, objects and operations among subjects and objects covered by the SFP : **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD**

Application note : The Basic Access Control SFP addresses the configuration of the TOE for usage with Basic Inspection Systems only.

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
FDP_ACF.1.1	The TSF shall enforce the **[assignment : access control SFP]** to objects based on the following : **[assignment : list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]**.
Assignment	Access control SFP : **Access Control SFP** List of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes: **(1) Subjects :** **a) Personalization Agent,** **b) Basic Inspection System,** **c) Extended Inspection System** **d) Terminal,** **(2) Objects :** **e) Data EF.DG1 to EF.DG16 of the logical MRTD,** **f) Data in EF.COM,** **g) Data in EF.SOD,** **(3) Security attributes :** **h) Authentication status of terminals,** **i) 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 : **[assignment : rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]**.
Assignment	Rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects : **(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 Basic Inspection System is allowed**

	to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, **(3) the successfully authenticated Extended Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,** **(4) the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG3 according to the Terminal Authorization,** **(5) the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG4 according to the Terminal Authorization.**
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following sensitive rules: **[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]**.
Assignment	Rules, based on security attributes, that explicitly authorize access of subjects to objects : **none**
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rule: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.
Assignment	Rules, based on security attributes, that explicitly deny access of subjects to objects : **(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) the Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.**

Application note : The TOE verifies the certificate chain established by the Country Verifier Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifier Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

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

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

FDP_UCT.1.1 / MRTD	The TSF shall enforce the **[assignment : access control SFP(s) and/or information flow control SFP(s)]** to be able to **[selection : transmit, receive]** objects in a manner protected from unauthorized disclosure **after Chip**

	Authentication.
Assignment	Access control SFP(s) and/or information flow control SFP(s): **Access Control SFP**
Selection	**Transmit and receive**

The TOE shall meet the requirement “Basic data exchange integrity (FDP_UIT.1)” as specified below (Common Criteria Part 2).

FDP_UIT.1/MRTD	**Basic data exchange integrity - MRTD**
FDP_UIT.1.1 / MRTD	The TSF shall enforce the **[assignment : access control SFP(s) and/or information flow control SFP(s)]** to be able to **[selection : transmit, receive]** user data in a manner protected from **[selection : modification, deletion, insertion, replay]** errors **after Chip Authentication**.
Assignment	Access control SFP(s) and/or information flow control SFP(s): **Access Control SFP**
Selection	**transmit and receive** **modification, deletion, insertion and replay**
FDP_UIT.1.2 / MRTD	The TSF shall be able to determine on receipt of user data, whether **[selection : modification, deletion, insertion, replay]** has occurred **after Chip Authentication**.
Selection	**modification, deletion, insertion and replay**

Application note : FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication to the General Inspection System. The authentication mechanism as part of Basic Access Control Mechanism and the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

5.1.5 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**
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions **[assignment : list of security management functions to be provided by the TSF]**.
Assignment	List of security management functions to be provided by the TSF : **(1) Initialization,** **(2) Personalization,** **(3) Configuration.**

Application note : The configuration capabilities of the TOE are available during the pre-personalization (initialization) and personalization phases.

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

FMT_SMR.1	**Security roles**
FMT_SMR.1.1	The TSF shall maintain the roles **[assignment : the authorized identified roles]**.
Assignment	The authorized identified roles: **(1) Manufacturer,** **(2) Personalization Agent,** **(3) Country Verifier Certification Authority,** **(4) Document Verifier,** **(5) Basic Inspection System,** **(6) Domestic Extended Inspection System,** **(7) Foreign Extended Inspection System.**
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application note : In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE. In the Phase 3 “Personalization” of the TOE” the Personalization Agent is the only user role known to the TOE. In phase 4 “Operational Use”, Country Verifier Certification Authority, Document Verifier, Basic Inspection System, Domestic Extended Inspection System and Foreign Extended Inspection System are the only user role know to the TOE.

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**
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]**.
Assignment	Limited capability and availability policy : **Deploying Test Features after TOE Delivery does not allow:** **(1) User Data to be disclosed or manipulated,** **(2) TSF data to be disclosed or manipulated** **(3) software to be reconstructed and**

	(4) substantial information about construction of TSF to be gathered which may enable other attacks.

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

FMT_LIM.2	**Limited availability**
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capability (FMT_LIM.1)” the following policy is enforced: **[assignment : Limited capability and availability policy]**.
Assignment	Limited capability and availability policy : **Deploying Test Features after TOE Delivery does not allow,** **(1) User Data to be disclosed or manipulated,** **(2) TSF data to be disclosed or manipulated** **(3) software to be reconstructed and** **(4) substantial information about construction of TSF to be gathered which may enable other attacks.**

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**
FMT_MTD.1.1 / INI_ENA	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **write**
Assignment	List of TSF data : **Initialization Data and Pre-Personalization Data** The authorized identified roles : **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 Authentication Key.

FMT_MTD.1/INI_DIS	**Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization data**
FMT_MTD.1.1 / INI_DIS	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **disable read access for users to**

Assignment	List of TSF data : **Initialization Data** The authorized identified roles : **the Personalization Agent**

Application note : According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Prepersonalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides an unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

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

FMT_MTD.1.1 / CVCA_INI	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **write**
Assignment	List of TSF data : **(1) initial Country Verifying Certification Authority Public Key,** **(2) initial Country Verifier Certification Authority Certificate,** **(3) initial Current Date.** The authorized identified roles : ***Personalization Agent***

Application note : The initial Country Verifying Certification Authority Public Key (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifier Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

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

FMT_MTD.1.1 / CVCA_UPD	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **update**
Assignment	List of TSF data : **(1) Country Verifier Certification Authority Public Key,** **(2) Country Verifier Certification Authority Certificate,** The authorized identified roles : **Country Verifier Certification Authority**

Application note : The Country Verifier Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifier CA Link-Certificates (cf. [20], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifier CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [20], sec. 2.2.3 and 2.2.4).

FMT_MTD.1/DATE	**Management of TSF data – Current date**
FMT_MTD.1.1 / DATE	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	**Modify**
Assignment	List of TSF data : **Current date** The authorized identified roles : **(1) Country Verifier Certification Authority,** **(2) Document Verifier,** **(3) Domestic Extended Inspection System.**

Application note : The authorized roles are identified in their certificate (cf. [20], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [20], annex A.3.3, for details).

FMT_MTD.1/KEY_WRITE	**Management of TSF data – Key Write**
FMT_MTD.1.1 / KEY_WRITE	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **write**
Assignment	List of TSF data : **Document Basic Access Keys** The authorized identified roles : **the Personalization Agent**

Application note : The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.

FMT_MTD.1/CAPK	**Management of TSF data – Chip Authentication Private Key**
FMT_MTD.1.1 / CAPK	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations: [selection: create, load]]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : ***load***
Assignment	List of TSF data : **Chip authentication Private Key** The authorized identified roles : ***Personalization Agent***

Application note : The component FMT_MTD.1/CAPK is refined by defining a selection between “create” and “load” for the assignment “other operations”. “Load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. “Create” means here that the Chip Authentication Private Key is generated by the TOE itself.

FMT_MTD.1/AAPK	***Management of TSF data – Chip Authentication Private Key***
FMT_MTD.1.1 / CAPK	The TSF shall restrict the ability to **[selection: change_default, query, modify,**

	delete, clear, [assignment: other operations: [selection: create, load]]] the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : ***load***
Assignment	List of TSF data : ***Active authentication Private Key*** The authorized identified roles : ***Personalization Agent***

Application note : The component FMT_MTD.1/AAPK is refined by defining a selection between “create” and “load” for the assignment “other operations”. “Load” means here that the Active Authentication Private Key is generated securely outside the TOE and written into the TOE memory. “Create” means here that the Active Authentication Private Key is generated by the TOE itself.

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

FMT_MTD.1.1 / KEY_READ	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **read**
Assignment	List of TSF data : **(1) Document Basic Access Keys,** **(2) Chip Authentication Private Key,** **(3) Personalization Agent Keys,** ***(4) Active Authentication Private Key*** The authorized identified roles : **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

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

5.1.6 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_EMSEC.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 SFR “Non-bypassability of the TSP (FPT_RVM.1)” and “TSF domain separation (FPT_SEP.1)” together with “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

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

FPT_EMSEC.1	**TOE Emanation**
FPT_EMSEC.1.1	The TSF 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]**.
Assignment	Types of emissions : ***side channel*** Specified limits : ***limits of the state of the art*** List of types of TSF data : **Personalization Agent Authentication Key and Chip Authentication Private Key *and Active Authentication Private Key*** List of types of user data : ***none***
FPT_EMSEC.2.1	The TSF shall ensure **[assignment: types of users]** are unable to use the following interface **[assignment: types of connection]** to gain access to **[assignment: list of types of TSF data]** and **[assignment: list of types of user data]**.
Assignment	Types of users : **any users** Types of connection : **smart card circuit contacts** List of types of TSF data : **Personalization Agent Authentication Key and Chip Authentication Private Key *and Active Authentication Private Key*** List of types of user data : ***none***

Application note : The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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**
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur : **[assignment: list of types of failures in the TSF]**.
Assignment	List of types of failures in the TSF : **(1) Exposure to operating conditions where therefore a malfunction could occur,** **(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**
FPT_TST.1.1	The TSF shall run a suite of self tests **[selection : during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment : conditions under which self test should occur]]** to demonstrate the correct operation of the TSF.
Selection	***During initial start-up***
FPT_TST.2.1	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.3.1	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Application note: the FPT_TST.1 requirement describes requirement for the Personalization and Operational Use phases. Self-tests during the Manufacturing phase are described in the chip security target and have been evaluated during the chip evaluation.

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**
FPT_PHP.3.1	The TSF shall resist **[assignment: physical tampering scenarios]** to the **[assignment: list of TSF devices/elements]** by responding automatically such that the TSP is not violated.

Assignment	Physical tampering scenarios : **physical manipulation and physical probing** List of TSF devices/elements : **TSF**

Application note : The TOE implements 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.

The following security functional requirements protect the TSF against bypassing and support the separation of TOE parts.

The TOE shall meet the requirement “Non-bypassability of the TSP (FPT_RVM.1)” as specified below (Common Criteria Part 2).

FPT_RVM.1	**Non-bypassability of the TSP**
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

The TOE shall meet the requirement “TSF domain separation (FPT_SEP.1)” as specified below (Common Criteria Part 2).

FPT_SEP.1	**TSF domain separation**
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

Application note : The parts of the TOE which support the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” should be protected from interference of the other security enforcing parts of the MRTD’s chip Embedded Software.

5.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The minimum strength of function is SOF-high.

Application note : The high minimum strength of function covers but is not limited to the TSF required by the SFR FIA_UAU.4, FCS_RND.1 and FPT_FLS.1 as far as probabilistic or permutational mechanisms are involved, e.g. due to challenges generated by the TOE and sent to the terminal or probabilistic self tests.

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 low attack potential (AVA_VLA.2).

This security target does not contain any security functional requirement for which an explicit stated strength of function claim is required.

5.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

This section describes the security functional requirements for the IT environment using the CC part 2 components.

Due to CCIMB Final Interpretation #58 these components are editorial changed to express the security requirements for the components in the IT environment where the original components are directed for TOE security functions. The editorial changes are indicated in **bold**.

5.3.1 Passive Authentication

The ICAO, the issuing States or Organizations and the receiving States or Organizations run a public key infrastructure for the Passive Authentication. This public key infrastructure distributes and protects the Country Signing CA Keys and the Document Signing Keys to support the signing of the User Data (EF.DG1 to EF.DG16) by means of the Document Security Object. The ICAO Doc 9303 [5] describes the requirements to the public key infrastructure for the Passive Authentication.

The Document Signer of the issuing State or Organization shall meet the requirement “Basic data authentication (FDP_DAU.1)” as specified below (Common Criteria Part 2).

FDP_DAU.1/DS	**Basic data authentication – Passive authentication**
FDP_DAU.1.1 / DS	The **Document Signer** shall provide a capability to generate evidence that can be used as a guaranty of the validity of **[assignment : list of objects or information types]**.
Assignment	List of objects or information types : **logical the MRTD (EF.DG1 to EF.DG16) and the Document Security Object**
FDP_DAU.1.1 / DS	The **Document Signer** shall provide **[assignment : list of subjects]** with the ability to verify evidence of the validity of the indicated information.
Assignment	List of subjects : **Inspection Systems of receiving States or Organizations**

5.3.2 Extended Access Control PKI

The CVCA and the DV shall establish a Document Verification PKI by generating asymmetric key pairs and certificates for the CVCA, DV and IS which may be verified by the TOE. The following SFR use the term “PKI” as synonym for entities like CVCA, DV and IS which may be responsible to perform the identified functionality.

FCS_CKM.1/PKI	**Cryptographic key generation – Document Verification PKI Keys**
FCS_CKM.1.1 / PKI	The **PKI** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment : cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment :**

	cryptographic key sizes] that meet the following : **[assignment : list of standards]**.
Assignment	Cryptographic key generation algorithm : ***See Tab 5*** Cryptographic key sizes : ***See Tab 5*** List of standards : **[20], Annex A**

Cryptographic algorithm	Cryptographic key size	Standard
RSA key generation	***1024, 1536 and 2048 bits***	**[20], Annex A**
ECDSA key generation	***192, 224 and 256 bits***	**[20], Annex A**

Tab 5 : PKI cryptographic key generation methods

FCS_COP.1/CERT_SIGN Cryptographic operation – Certificate Signing

FCS_COP.1.1 / CERT_SIGN	The **PKI** shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **digital signature creation** Cryptographic algorithm : ***See Tab 6*** Cryptographic key sizes : ***See Tab 6*** List of standards : ***See Tab 6***

Cryptographic algorithm	Cryptographic key size	Standard
RSA	***1024, 1536 and 2048 bits***	***RSASSA-PKCS1-v1.5***
ECDSA	***192, 224 and 256 bits***	***ISO15946 ECDSA***

Tab 6 : PKI cryptographic signature creation methods

Application note : Signature algorithms key lengths and standards are those used by CVCA and DV to create certificates which will be verified by FCS_COP.1/SIG_VER implemented by the TOE for the Terminal Authentication Protocol (cf. [20], Annex A.2.1.1 and C.3).

5.3.3 Basic Terminal

This section describes common security functional requirements to the Basic Inspection Systems and the Personalization Agent if it uses the Basic Access Control Mechanism with the Personalization Agent Authentication Keys. Both are called “Basic Terminals” (BT) in this section.

The Basic Terminal shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (Common Criteria Part 2).

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

FCS_CKM.1.1 / KDF_BT	The **Basic Terminal** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment : cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	Cryptographic key generation algorithm : Document Basic Access Key Derivation Algorithm Cryptographic key sizes : **112 bits** List of standards : **[5] normative appendix 5**

Application note : The required standard for the Document Basic Access Key Derivation Algorithm ensures that the Basic Inspection Terminal derives the same Document Basic Access Key as loaded by the Personalization Agent into the TOE and used by the TOE for FIA_UAU.4/BAC_MRTD. Indeed, the [5] normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data. *Any other standard used by Basic Inspection Terminal to derive Document Basic Access Key shall also ensure to derive the same Document Basic Access Key as loaded by the Personalization Agent into the TOE and used by the TOE for FIA_UAU.4/BAC_MRTD.*

The Basic Terminal shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (Common Criteria Part 2).

FCS_CKM.4/BT Cryptographic key destruction – MRTD

FCS_CKM.4.1 / BT	The **Basic Terminal** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment : cryptographic key destruction method]** that meets the following : **[assignment : list of standards]**.
Assignment	Cryptographic key destruction method : ***Key overwriting*** List of standards : ***None***

Application note : The basic terminal shall destroy the Document Basic Access Keys of the MRTD and the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging after inspection of the MRTD.

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

FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal

FCS_COP.1.1 / SHA_BT	The **Basic Terminal** shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.

Assignment	List of cryptographic operations : **hashing** Cryptographic algorithm : **SHA-1** Cryptographic key sizes : **none** List of standards : **FIPS 180-2**

Application note : This SFR requires the terminal to implement the hash function SHA-1 for the cryptographic primitive to generate the Document Basic Access Keys according to FCS_CKM.1/KDF_BT.

FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal

FCS_COP.1.1 / ENC_BT	The **Basic Terminal** shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **secure messaging – encryption and decryption** Cryptographic algorithm : **Triple-DES in CBC mode** Cryptographic key sizes : **112 bits** List of standards : **FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)**

Application note : This SFR requires the Basic Terminal to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The key is agreed between the TOE and the terminal during the execution of the Basic Access Control Authentication Mechanism. The key size of 112 bits is chosen to resist attacks with high attack potential.

FCS_COP.1/MAC_BT Cryptographic operation – Secure Messaging Message Authentication Code by the Basic Terminal

FCS_COP.1.1 / MAC_BT	The **Basic Terminal** shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **secure messaging – message authentication code** Cryptographic algorithm : **Retail-MAC** Cryptographic key sizes : **112 bits** List of standards : **FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)**

Application note : This SFR requires the terminal to implement the cryptographic primitive for secure messaging with message authentication code over the transmitted data. The key is agreed or defined as

the key for secure messaging encryption. The key size of 112 bits is chosen to resist attacks with high attack potential.

The Basic Terminal shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

FCS_RND.1/BT	**Quality metric for random numbers – Basic Terminal**
FCS_RND.1.1 / BT	The **Basic Terminal** shall provide a mechanism to generate random numbers that meet **[assignment : a defined quality metric]**.
Assignment	A defined quality metric: ***AIS31 Class P2 quality metric***

Application note : This SFR requires the terminal to generate random numbers used in the authentication protocols as required by FCS_CKM.1/KDF_BT and FIA_UAU.4 The quality metric shall be chosen to ensure at least the strength of function Basic Access Control Authentication for the challenges.

The Basic Terminal shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

FIA_UAU.4/BT	**Single-use authentication mechanisms – Basic Terminal**
FIA_UAU.4.1 / BT	The **Basic Terminal** shall prevent reuse of authentication data related to **[assignment : identified authentication mechanism(s)]**.
Assignment	Identified authentication mechanism(s): **Basic Access Control Authentication Mechanism**

Application note : The Basic Access Control Authentication Mechanism [5] uses a challenge RND.IFD freshly and randomly generated by the terminal to prevent reuse of a response generated by a MRTD’s chip and of the session keys from a successful run of authentication protocol.

The Basic Terminal shall meet the requirement “Re-authentication (FIA_UAU.6)” as specified below (Common Criteria Part 2).

FIA_UAU.6/BT	**Re-authenticating – Basic Terminal**
FIA_UAU.6.1 / BT	The **Basic Terminal** shall re-authenticate the user under the conditions **[assignment : list of conditions under which re-authentication is required]**.
Assignment	List of conditions under which re-authentication is required: **each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism**

Application note : The Basic Access Control Mechanism specified in [5] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The terminal checks by secure messaging in MAC_ENC mode each MRTD’s chip response to a command based on Retail-MAC whether it was sent by the successfully authenticated MRTD’s chip. The authentication fails if any response is received with incorrect message authentication code.

5.3.4 General Inspection System

The General Inspection System (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism. Therefore it has to fulfill all security requirements of the Basic Inspection System as described above.

The General Inspection System verifies the authenticity of the MRTD's by the Chip Authentication Mechanism during inspection and establishes new secure messaging with keys. The reference data for the Chip Authentication Mechanism is the Chip Authentication Public Key read form the logical MRTD data group EF.DG14 and verified by Passive Authentication (cf. to FDP_DAU.1/DS). Note, that the Chip Authentication Mechanism requires the General Inspection System to verify at least one message authentication code of a response sent by the MRTD to check the authenticity of the chip.

The General Inspection System shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2).

FCS_CKM.1/DH_GIS	**Cryptographic key generation – Diffie-Hellman Keys by the GIS**
FCS_CKM.1.1 / DH_GIS	The **General Inspection System** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment : cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	Cryptographic key generation algorithm : ***See Tab 7*** Cryptographic key sizes : ***See Tab 7*** List of standards : **[20], Annex A.1**

Cryptographic key generation algorithm	Cryptographic key size	Standard
Diffie-Hellman Protocol (PKCS#3)	***1024, 1536 and 2048 bits***	**[20], Annex A.1 and [16]**
ECDH (ISO 15946)	***192, 224 and 256 bits***	**[20], Annex A.1 and [15]**

Tab 7 : GIS cryptographic DH key generation methods

Application note : The GIS generates a shared secret value with the terminal during the Chip Authentication Protocol, see [20], sec. 3.1 and Annex A.1. This protocol may be based on the Diffie-Hellman Protocol compliant to PKCS#3 (i.e. a modulo arithmetic based cryptographic algorithm, cf. [16]) or on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [20], Annex A.1, [21] and [15] for details). Even the General Inspection System shall support only the concrete algorithm implemented in the TOE it is expected that the General Inspection System will support both of them for interoperability reasons. The shared secret value is used to derive the 112 bit Triple-DES key for encryption and the 112 bit Retail-MAC keys according to the Document Basic Access Key Derivation Algorithm [5] normative appendix 5, A5.1, for the TSF required by FCS_COP.1/ENC_MRTD and FCS_COP.1/MAC_MRTD.

The General Inspection System shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2).

FCS_COP.1/SHA_GIS	**Cryptographic operation – Hash for Key Derivation by GIS**
FCS_COP.1.1 / SHA_GIS	The **General Inspection System** shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **hashing**

	Cryptographic algorithm : ***SHA-1*** Cryptographic key sizes : **none** List of standards : **FIPS 180-2**

Application note : The hash algorithm supported by the GIS is consistent with the hash function used by the TOE for Chip Authentication.

The General Inspection System shall meet the requirement "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4/GIS	**Single-use authentication mechanism – Single-use authentication of the MRTD chip by the GIS**
FIA_UAU.4.1 / GIS	The **General Inspection System** shall prevent reuse of authentication data related to **[assignment : identified authentication mechanism(s)]**.
Assignment	Identified authentication mechanism(s): **(1) Basic Access Control Authentication Mechanism,** **(2) Chip Authentication Protocol.**

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

FIA_UAU.5/GIS	**Multiple authentication mechanisms - General Inspection System**
FIA_UAU.5.1 / GIS	The **General Inspection System** shall provide **[assignment : list of multiple authentication mechanisms]** to support user authentication.
Assignment	List of multiple authentication mechanisms: **(1) Basic Access Control Authentication Mechanism,** **(2) Chip Authentication Protocol**
FIA_UAU.5.2 / GIS	The **General Inspection System** shall authenticate any user's claimed identity according to the **[assignment : rules describing how the multiple authentication mechanisms provide authentication]**.
Assignment	Rules describing how the multiple authentication mechanisms provide authentication: following rules : **(1) The General Inspection System accepts the authentication attempt as MRTD only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys,** **(2) After successful authentication as MRTD and until the completion of the Chip Authentication Mechanism the General Inspection System accepts only received response codes with correct message authentication code sent by means of secure messaging with key agreed with the authenticated MRTD by means of the Basic Access Control Authentication Mechanism.** **(3) After run of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip**

	Authentication Mechanism.

Application note : Basic Access Control Mechanism includes the secure messaging for all commands and response codes exchanged after successful mutual authentication between the inspection system and the MRTD. The inspection system shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys drawn from the second, optical readable MZR line and the secure messaging after the mutual authentication. The General Inspection System and the MRTD shall use the secure messaging with the keys generated by the Chip Authentication Mechanism after the mutual authentication.

The General Inspection System shall meet the requirement « Re-authenticating (FIA_UAU.6) » as specified below (Common Criteria Part 2).

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

FIA_UAU.6.1 / MRTD	The **General Inspection System** shall re-authenticate the user under the conditions **[assignment : list of conditions under which re-authentication is required]**.
Assignment	List of conditions under which re-authentication is required: **(1) Each response sent to the General Inspection System after successful authentication of the MRTD with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall have a correct MAC created by means of secure messaging keys agreed upon by the Basic Access Control Authentication Mechanism.** **(2) Each response sent to the General Inspection System after successful run of the Chip Authentication Protocol shall have a correct MAC created by means of secure messaging keys generated by Chip Authentication Protocol.**

Application note : The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [5] include secure messaging for all commands and responses exchanged after successful authentication of the inspection system. The General Inspection System checks by secure messaging in MAC_ENC mode each response based on Retail-MAC whether it was sent by the successfully authenticated MRTD (see FCS_COP.1/MAC_MRTD for further details). The General Inspection System does not accept any response with incorrect message authentication code. Therefore the General Inspection System re-authenticate the user for each received command and accept only those responses received from the authenticated user.

The General Inspection System shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

FDP_UCT.1/GIS Basic data exchange confidentiality – General Inspection System

FDP_UCT.1.1 / GIS	The **General Inspection System** shall enforce the **[assignment : access control SFP(s) and/or information flow control SFP(s)]** to be able to **[selection : transmit, receive]** objects in a manner protected from unauthorized disclosure **after Chip Authentication**.
Assignment	Access control SFP(s) and/or information flow control SFP(s): **Access Control SFP**
Selection	**Transmit and receive**

The General Inspection System shall meet the requirement “Data exchange integrity (FDP_UIT.1)” as specified below (Common Criteria Part 2).

FDP_UIT.1/GIS	**Data exchange integrity - General Inspection System**
FDP_UIT.1.1 / GIS	The **General Inspection System** shall enforce the **[assignment : access control SFP(s) and/or information flow control SFP(s)]** to be able to **[selection : transmit, receive]** user data in a manner protected from **[selection : modification, deletion, insertion, replay]** errors **after Chip Authentication**.
Assignment	Access control SFP(s) and/or information flow control SFP(s): **Basic Access Control SFP**
Selection	**Transmit and receive** **modification, deletion, insertion and replay**
FDP_UIT.1.2 / GIS	The **General Inspection System** shall be able to determine on receipt of user data, whether **[selection : modification, deletion, insertion, replay]** has occurred **after Chip Authentication**.
Selection	**modification, deletion, insertion and replay**

5.3.5 Extended Inspection System

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

FCS_COP.1/SIG_SIGN_EIS	**Cryptographic operation – Signature creation by EIS**
FCS_COP.1.1 / SIG_SIGN_EIS	The **Extended Inspection System** shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **signature creation** Cryptographic algorithm : ***see Tab 8*** Cryptographic key sizes : ***see Tab 8*** List of standards : ***see Tab 8***

Cryptographic algorithm	Cryptographic key size	Standard
RSA	***1024, 1536 and 2048 bits***	***RSASSA-PKCS1-v1.5***
ECDSA	***192, 224 and 256 bits***	***ISO15946 ECDSA***

Tab 8 : EIS cryptographic signature creation methods

Application note : The signature algorithms key lengths and standards to be implemented by the Extended Inspection system for the Terminal Authentication Protocol are compliant with the TOE (cf. [20], Annex A.2.1.1 and C.3 for details).

FCS_COP.1/SHA_EIS	**Cryptographic operation – Hash for Key Derivation by EIS**
FCS_COP.1.1 / SHA_EIS	The **Extended Inspection System** shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **hashing** Cryptographic algorithm : ***SHA-1*** Cryptographic key sizes : **none** List of standards : **FIPS 180-2**

Application note : The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism (cf. [5] normative appendix 5, A5.1). The TOE implements additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol (cf. [20], Annex A.2.1.1 and C.3 for details).

Application note: The EIS may also implement the hash functions SHA-224 and SHA-256 in addition to SHA-1 for the Terminal Authentication Protocol.

FCS_COP.1/SIG_VER_EIS	***Cryptographic operation – Signature verification by EIS***
FCS_COP.1.1 / SIG_SIGN_EIS	The **Extended Inspection System** shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : ***signature verification*** Cryptographic algorithm : ***ISO9796-2 Digital Signature scheme 1*** Cryptographic key sizes : ***1024, 1536 and 2048 bits*** List of standards : ***[5]***

Application note: This SFR requires the terminal to perform RSA signature verification for the Active Authentication protocol.

The Extended Inspection System shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

FCS_RND.1/EIS	***Quality metric for random numbers – Basic Terminal***
FCS_RND.1.1 / BT	The **Basic Terminal** shall provide a mechanism to generate random numbers that meet **[assignment : a defined quality metric]**.

Assignment	A defined quality metric: ***AIS31 Class P2 quality metric***

Application note: This SFR requires the terminal to generate random numbers used in the Active Authentication protocol.

The General Inspection System shall meet the requirement "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4/EIS Single-use authentication mechanism – Single-use authentication of the MRTD chip by the EIS

FIA_UAU.4.1 / GIS	The **Extended Inspection System** shall prevent reuse of authentication data related to **[assignment : identified authentication mechanism(s)]**.
Assignment	Identified authentication mechanism(s): ***Active Authentication Protocol.***

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

FIA_API.1/EIS Authentication Proof of Identity – Extended Inspection System

FIA_API.1.1 / EIS	The **Extended Inspection System** shall provide a **[assignment : authentication mechanism]** to prove the identity of the **[assignment : authorized user or rule]**.
Assignment	Authentication mechanism: **Terminal Authentication Protocol according to [20]** Authorized user or rule : **Extended Inspection System**

Application note : This SFR requires the Extended Inspection system to implement the Terminal Authentication Mechanism specified in [20], sec. 3.3. The Extended Inspection system requests a challenge of 8 Byte from the MRTD and generates a digital signature using RSA or ECDSA (cf. [20], appendix A.2.1 for details).

5.3.6 Personalization Terminals

The TOE supports different authentication and access control mechanisms which may be used for the Personalization Agent depending on the personalization scheme of the issuing State or Organization :

(1) The Basic Access Control Mechanism which may be used by the Personalization Terminal with a Personalization Agent Secret Key Pair. The Basic Access Control Mechanism establishes strong cryptographic keys for the secure messaging to ensure the confidentiality by Triple-DES and integrity by Retail-MAC of the transmitted data. This approach may be used in a personalization environment where the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

(2) The Personalization Terminal may use the Terminal Authentication Protocol like a Extended Inspection System but using the Personalization Agent Keys to authenticate themselves to the TOE. This approach may be used in a personalization environment where (i) the Personalization Agent want to authenticate the MRTD's chip and (ii) the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

(3) In a centralized personalization scheme the major issue is high productivity of personalization in a high secure environment. In this case the Personalization Agent may wish to reduce the protocol to symmetric authentication of the terminal without secure messaging. Therefore the TOE and the

Personalization Terminal support a simple the Symmetric Authentication Mechanism with Personalization Agent Key as requested by the SFR FIA_UAU.4/MRTD and FIA_API.1/SYM_PT.

The Personalization Terminal shall meet the requirement “Authentication Prove of Identity (FIA_API.1)” as specified below (Common Criteria Part 2 extended) if it uses the Symmetric Authentication Mechanism with Personalization Agent Key.

FIA_API.1/SYM_PT Authentication Proof of Identity – Personalization Terminal Authentication with Symmetric Key

FIA_API.1.1 / SYM_PT	The **Personalization Terminal** shall provide a **[assignment : authentication mechanism]** to prove the identity of the **[assignment : authorized user or rule]**.
Assignment	Authentication mechanism: **Authentication Mechanism based on Triple-DES** Authorized user or rule : **Personalization Agent**

Application note : The Symmetric Authentication Mechanism for Personalization Agents is intended to be used in a high secure personalization environment only. It uses the symmetric cryptographic Personalization Agent Authentication Secret key of 112 bits to encrypt a challenge of 8 Bytes with Triple-DES which the terminal receives from the MRTD’s chip e.g. as response of a GET CHALLENGE. The answer may be sent by means of the EXTERNAL AUTHENTICATE command according to ISO 7816-4 [22] command. In this case the communication may be performed without secure messaging (note, that FIA_UAU.5.2 requires secure messaging only after run of Basic Access Control authentication).

Application note: The authentication mechanism based on TDES used to authenticate the Personalization Agent must be compliant with [CPS].

6. TOE SPECIFICATIONS

6.1 TOE SECURITY FUNCTIONS SPECIFICATIONS

6.1.1 Chip security functions

FS_INTEGRITY

This security function is responsible for detecting and reporting integrity errors on CPU usage, stack overflow and E²PROM.

FS_PHYSICAL_TAMPERING

This security functions ensures that:
- The TOE detects clock and voltage supply operating changes by the environment,
- The TOE detects attempts to violate its physical integrity,
- The TOE is always clocked with shape and timing within specified operating conditions.

FS_SECURITY_ADMIN

This security function ensures the management of the following security violation attempts:
- Access to unavailable or reserved memory locations,
- Unauthorized access to memories,
- Bad CPU usage,
- Bad ROM or E²PROM use,
- E²PROM single bit fails,
- Clock and voltage supply operating changes,
- TOE physical integrity abuse.

FS_UNOBSERVABILITY

This security functions ensures that all end-users are unable to observe the following operations:
- read access to the ROM, the RAM, the E²PROM or a register,
- write access to the RAM,
- program (erase&write) on ROM or E²PROM,
- erase E²PROM.

This security function also prevents the disclosure of user data and of TSF data when it is transmitted between separate parts of the TOE (the different memories, the CPU and other functional units of the TOE such as a cryptographic co-processor are seen as separated parts of the TOE): User Data and TSF data shall not be accessible from the TOE except when the Smartcard Embedded Software decides to communicate the User Data via an external interface.

FS_SYM_CRYPTO

This security function provides DES and TDES data encryption / decryption capability, in order to compute Message Authentication code (MAC) or the encrypted data.

FS_ASYM_CRYPTO

This security function provides:
- RSA encryption/decryption with and without CRT with an RSA modulo up to 2176 bits,
- Elliptic curves cryptography on GF(p): point addition and point multiplication
- SHA-1 hash function chaining blocks of 512 bits to get a 160 bits result.

FS_ALEAS

This security function provides a hardware Random Number Generator (RNG) to support security operations performed by cryptographic applications. The RNG complies with the AIS31 Class P2 quality metric.

6.1.2 Low level security functions

FS_PROTECTION

This security function provides random delay and desynchronisation capability in order to protect the TOE.

6.1.3 Operating system security functions

FS_ACCESS

This security function manages the access to objects (files, directories, data and keys) stored in the TOE.

FS_INIT

This security function performs TOE testing and initialization after each reset of the TOE.

FS_MEMOIRE

This security function manages E²PROM and RAM erasure.

FS_OTP

This security function manages the OTP area in E²PROM and in particular the « life cycle parameter », enforcing non-reversibility of the life cycle.

FS_CPLC

This security function manages the CPLC area. The CPLC area contains Manufacturing data, pre-personalization data and Personalization data. The CPLC area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Read access to the CPLC area is allowed during Personalization phase. During Operational Use phase, the CPLC area read access is only possible after BAC authentication.

FS_CHECK

This security function performs data integrity checks.

FS_TEST

This security function performs self-tests at start-up and monitores code integrity during excution.

FS_AUDIT

This security function reacts when a fault or an anomaly is detected.

6.1.4 Application manager security functions

FS_GESTION

This security function manages:
- Management of the secure state of the TOE.
- Application selection.
- Application separation.

6.1.5 Application security functions

FS_SECRET

This security function ensures secure management of secret such as cryptographic keys.

FS_CRYPTO

This security function performs high level cryptographic operations.

FS_BAC_AUTH

FS_BAC_AUTH performs the Basic Access Control mechanism, as described in [5], in order to authenticate the Inspection System.

FS_TERM_AUTH

FS_TERM_AUTH performs the Terminal Authentication to authenticate the terminal.

The Strength Of Function claimed for FS_TERM_AUTH is high.

FS_TDES_AUTH

FS_TDES_AUTH performs an authentication mechanism based on TDES.

The Strength Of Function claimed for FS_TDES_AUTH is high.

FS_CHIP_AUTH

This security function manages the capability of the TOE to authenticate itself to the terminal using the Chip Authentication Protocol as defined in [20].

FS_ACTIVE_AUTH

This security function manages the capability of the TOE to authenticate itself to the terminal using the Active Authentication Protocol as defined in [5].

FS_RATIF

A counter may be associated to an authentication secret, which is used to count the number of successive unsuccessful authentication attempts.