ID-One™ ePass 64 v2.0 with EAC RSA

Public security Target

Date	Version
April 9th 2008	V1.0 – Original version

Oberthur Technologies

TABLE OF CONTENT

FIGURES

TABLES

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

Complete identification of the TOE is described in §2.2

This Security Target deals with the evaluation of the application software, as well as the composition with the evaluation of the Integrated Circuit (IC). It claims the Protection Profile EAC [R10] and extends it with the Active authentication mechanism [R4].

This security target refers to the micro-controller P5CD080 V0B security target [R2] that is compliant to BSI 0002 Protection Profile [R3].

The Active Authentication (AA) mechanism is optional.

The TOE name will be Access World.

This evaluation is sponsorized by Oberthur Card Systems, whose new name is Oberthur Technologies.

1.2 ST OVERVIEW

The TOE is a Machine readable travel document implementing the Basic Access Control as defined in [R4] and [R5] and the Extended Access Control as described in [R7].

The main objectives of this security target are:

- To describe the Target of Evaluation (TOE). This ST focuses on the Machine readable travel document, designed to be embedded in a Smart card integrated circuit.
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by its environment.
- To describe the security objectives of the TOE and its supporting environment.
- To specify the security requirements which include the TOE security functional requirements and the TOE security assurance requirements.
- To specify the TOE summary specification, which includes the TOE security functions specifications and the assurance measures.
- To give a rationale to this ST.

The assurance level for this product and its documentation is EAL4 augmented

The strength level for the TOE security functional requirements is "SOF high" (Strength Of Functions high).

1.3 CC CONFORMANCE

The ST is built on [R10] and is conformant to this PP. It extends the Protection Profile with the Active Authentication [R4]

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, August 2005, version 2.3, CCIMB-2005-8-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Introduction and general model, August 2005, version 2.3, CCIMB-2005-8-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, August 2005, version 2.3, CCIMB-2005-8-003

including

- 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 1

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).

1.4 Reference

[R1] Common Methodology for Information Technology Security - Evaluation Methodology - CCIMB-2004-01-003, version 2.2, January 2004

[R2] Smartcard IC Platform Protection Profile v 1.0 - BSI-PP-0002-2001 Jul 2001

[R3] P5CD080 V0B Security Target Lite v1.1 -9 May 2007

MRTD specifications

[R4] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[R5] Machine readable Travel Documents – Supplements 9303

[R6] Development of a logical data structure – LDS for optional capacity expansion technologies Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

[R7] Advanced Security Mechanisms for Machine readable travel documents – Extended Access control (EAC) – TR03110 – v1.11

[R8] ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

Protection Profiles

[R9] Machine readable travel documents with "ICAO Application", Basic Access control – BSI-PP-0017

[R10] Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0026 v1.2

Standards

[R11] ISO7816-4 – Organization, security and commands for interchange

[R12] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006

[R13] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[R14] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[R15] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[R16] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993

[R17] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[R18] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 septembre 1998

[R19] Jakob Jonsson and Burt Kaliski. Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1. RFC 3447, 2003.

[R20] RSA Laboratories. PKCS#1 v2.1: RSA cryptography standard. RSA Laboratories Technical Note, 2002.

Misc

[R21] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[R22] Smart Card Integrated Circuit With Embedded Software Protection Profile, version 2.0, June 1999. Certified under the reference PP/9911, DCSSI

[R23] NOTE-10 - Interpretation with e-passport PP_courtesy translation-draft v0.1

2 TOE Description

This part of the Security Target describes the TOE as an aid to the understanding of its security requirements. It addresses the product type, the intended usage and the main features of the TOE.

This part includes :

- Introduction
- TOE identification
- TOE overview
- TOE logical structure
- TOE life-cycle,
- Limits of the TOE
- TOE environment
- TOE scope

2.1 Introduction

The Target of Evaluation (TOE) is the contact-less integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [R4] and providing the Basic Access Control according to the ICAO document [R4] and the Extended Access control according to [R7].

The TOE comprises of:

- The circuitry of the MRTD's chip (the integrated circuit: IC) with hardware for the contact-less interface, e.g. antennae, capacitors,
- The IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- The IC Embedded Software (operating system: OS) loaded on the ROM
- The optional code loaded on EEPROM
- The MRTD application
- The associated guidance documentations.

NB: Although it is included in the TOE, the antenna is out of the evaluation scope.

Physical overview of the TOE

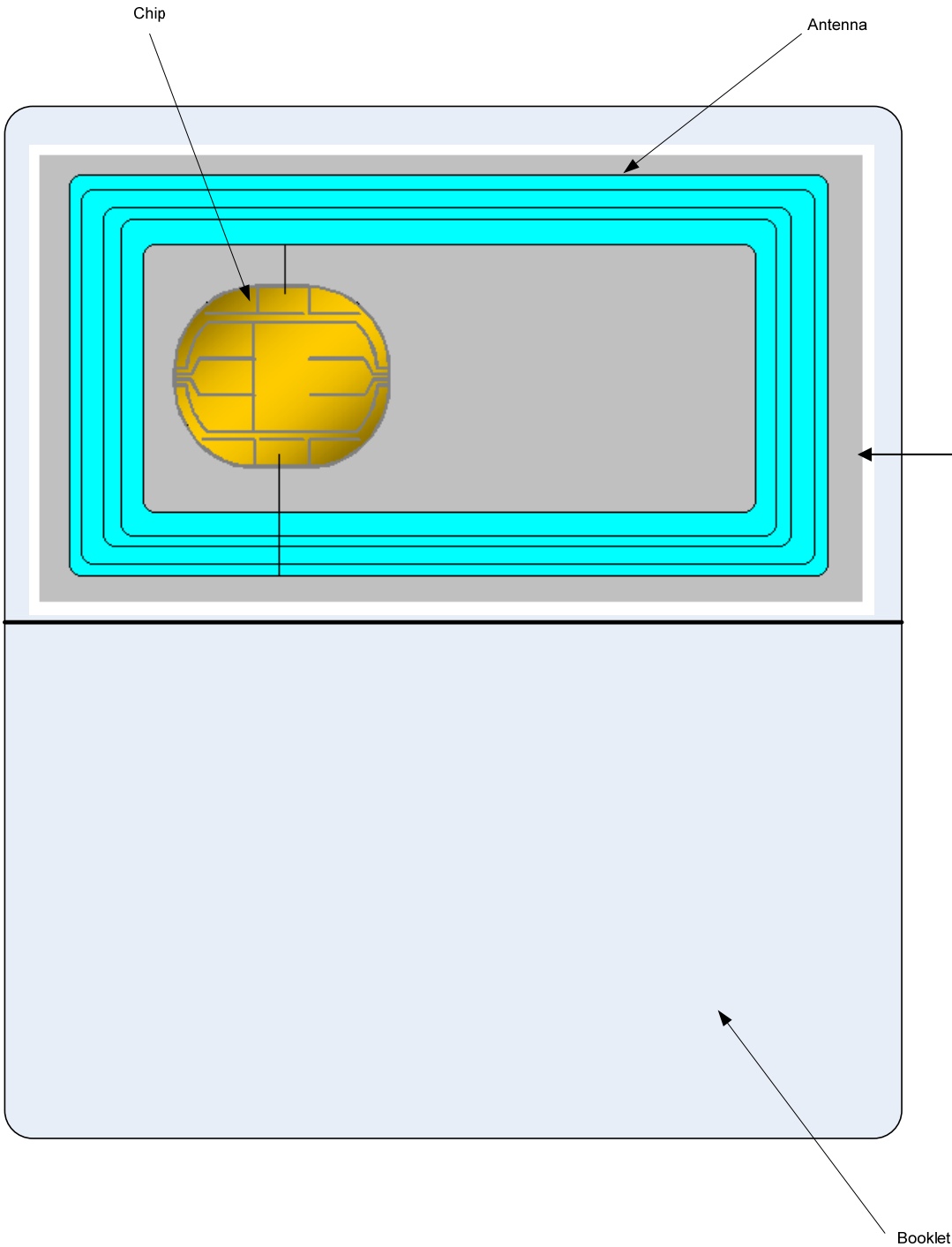


Figure 1 : Physical TOE overview

2.2 TOE Identification

TOE is composed of the following components :

- MicroController: NXP P5CD080UA / T0B16100
- ROM code of the mask : OCS Reference P06011 /067511
- Optional Code : OCS Reference P06011/067841

The optional code, the ROM code, the configuration of the TOE, as well as the PP claim can be identified using the dedicated file EF.TOE_Identification, in which all the relevant data are stored in phase 2.

```
EF.TOE_Identification ::= SEQUENCE_OF{
                                        BYTE STRING ROMCodeIdentifier
                                        BYTE STRING OptionalCodeIdentifier
                                        BYTE STRING PPIdentifier
                                        BYTE STRING CertificateIdentifier
                                        BYTE STRING ProprietaryData
                                    }
```

In which

- ROMCodeIdentifier = 067511
- OptionalCodeIdentifier = 067843
- PPIdentifier = 26
- CertificateIdentifier = 03

Commercial name of the TOE is :

ID-One ePass 64 v2.0 with EAC RSA

2.3 TOE overview

State or organisation issues MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his/her identity. The MRTD in context of this security target contains:

- Visual (eye readable) biographical data and portrait of the holder printed in the booklet
- A separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ)

- And data elements stored on the MRTD's chip for contact-less machine reading.

The authentication of the traveller is based on:

- The possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and
- The Biometric matching performed on the Inspection system using the reference data stored in the MRTD.

The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of:

(a) The **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
   (1) The biographical data on the biographical data page of the passport book,
   (2) The printed data in the Machine-Readable Zone (MRZ) and
   (3) The printed portrait.

(b) The **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [R4] as specified by ICAO on the contact-less integrated circuit. It presents contact-less readable data including (but not limited to) personal data of the MRTD holder
   (1) The digital Machine Readable Zone Data (digital MRZ data, DG1),
   (2) The digitized portraits (DG2),
   (3) The optional biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both
   (4) The other data according to LDS (DG5 to 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 organisational security measures (e.g. control of materials, personalization procedures). 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 specifications [R4] & [R5] define the baseline security methods such as the Passive Authentication and the Basic Access Control to protect the data retrieval. Theses two features are mandatory.

The Basic Access Control is a security feature that is supported by the TOE. The inspection system

(i) reads the printed data in the MRZ

(ii) authenticates themselves as inspection system by means of keys derived from MRZ data. 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.

The Active Authentication of the MRTD's chip (described in [R4]) is an optional feature that may be implemented. It ensures that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the MRTD's chip. For this purpose the chip contains its own Active Authentication RSA Key pair. A hash representation of Data Group 15 Public Key is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key is stored in the chip's secure memory.
The TOE supports the loading and generation of the Active Authentication RSA Key pair.

The Extended Access Control (defined in [R7]) enhances the later security features and ensures a strong and mutual authentication of the passport and the Inspection system. This step is required to access the biometric data such as the fingerprint and/or the iris. In particular, the authentication steps ensures a strong secure channel able to provide confidentiality of the biometric data that are read and authentication of the Inspection system retrieving the date to perform a Match on Terminal comparison.
The Extended Access Control authentication steps the TOE implements may be realized either with elliptic curve cryptography, or with RSA cryptography.

This security target addresses the following security features of the logical MRTD:

(i) Protection in integrity by write only-once access control and by physical means

(ii) Authentication between the passport holder and the Inspection system prior to any border control by the Basic Access Control Mechanism

(iii) Protection in integrity and confidentiality of data read by the secure messaging

(iv) Authentication of the genuine chip by the Active Authentication mechanism (if activated)

(v) Strong authentication of the chip and the Inspection system prior to any biometric data retrieval

2.4 TOE logical structure

The TOE contains an application embedded in the chip. This application fullfills the requirements described beforehand and in [R4], [R5], [R7].
This application is made of :

- A file system compliant with [R11]
- A software, executing operation to protect the files (some) and using data stored within the files (some)
- Other data structure that are not files

Roughly, the embedded application, when powered, is seen as a master file, containing a Dedicated file (DF) for the LDS.
This dedicated file is selected by means of the Application Identifier (AID) of the LDS application.
Once the LDS dedicated file is selected, the file structure it contains may be accessed, provided the access conditions are fulfilled.

Structure of the File system

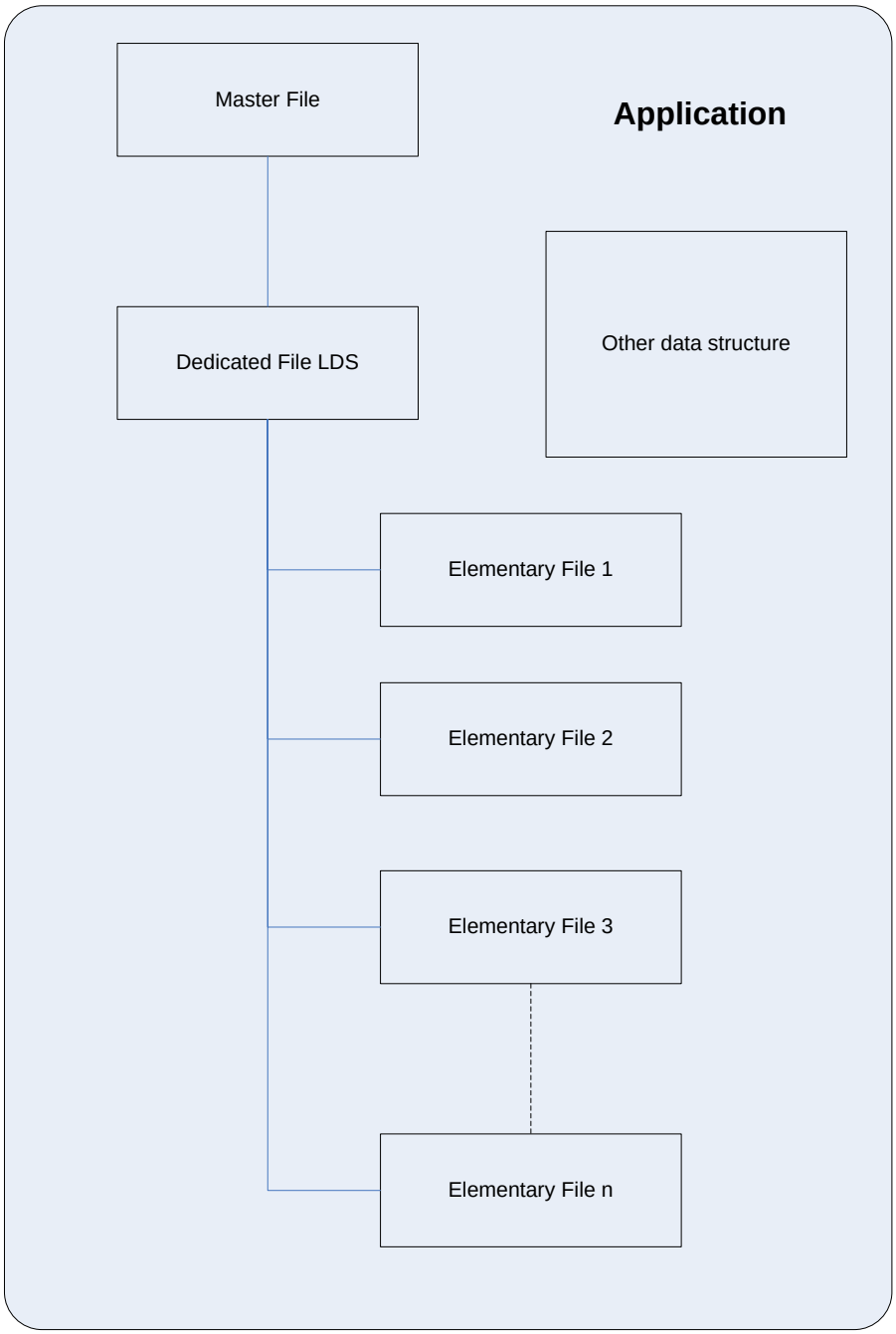


Figure 2 : Structure of the File system

2.4.1 Software Architecture of the TOE

The Figure below shows the logical structure of the TOE, showing the layered architecture used to combine the subsystems lightly described below:

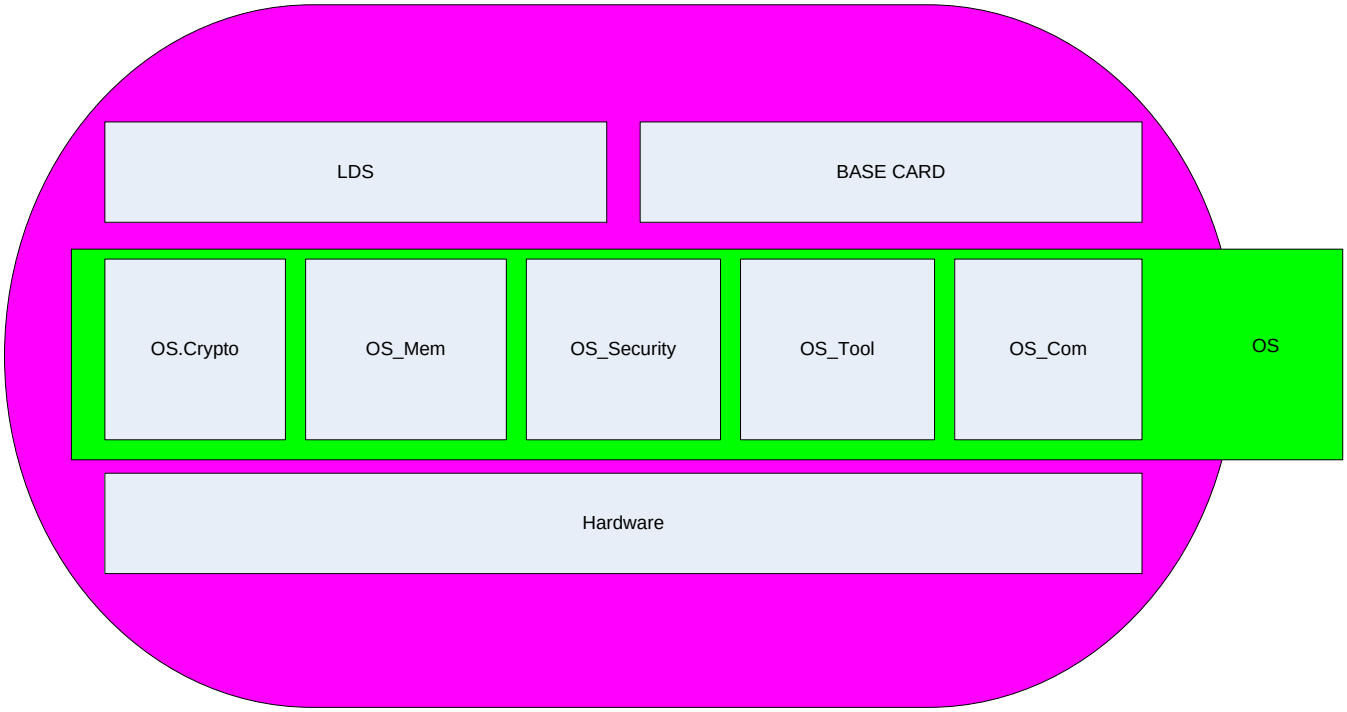


Figure 3 : Logical structure of the TOE

- **LDS***:* This subsystem fulfils the following functionalities*:*
  - Implements the commands of e-passport that are available in operational phase
  - Manages access control on these commands
  - Implements authentication mechanisms:
    - Basic Access Control (BAC), including session keys generation
    - Active Authentication (AA) – if implemented (optional)
    - Extended Access control (EAC)
  - Implements Secure Messaging for incoming and outgoing commands

- **BASE CARD:** This subsystem fulfils the following functionalities:
  - Implements the commands of e-passport that are available in pre-personalization and personalization phases
  - Manages access control on these commands

- **OS :** This layer provides an interface between the Hardware and the application layer.
  - **OS_Crypto** provides cryptographic services such as
    - 3DES
    - Random Number generator
    - RSA
    - Elliptic curves cryptography (ECDSA and ECDH)
    - Message Digest Computation (SHA-1, SHA-224, SHA-256, SHA-384)
  - **OS_Mem** performs access to memory (read & write) - EEPROM
  - **OS_Security** provides security mechanism (secure comparison,..) as well as the transaction mechanism, ensuring the copy in the EEPROM is fully performed, whenever an event occurs (loss of power – tearing)
  - **OS_Tool** provides several services to the subsystem LDS & BASE CARD.
  - **OS_Com** handles the communication interface (TCL interface)

2.4.2 File structure of the TOE

The TOE distinguish between two types of files
- System files.
- Data files that store data visible from the outside.

Basically, the **system files** and **data files** are files handled by the Base Card. The Base card handles their creation and management. Both types have the following characteristics:
- Size – size reserved within the EEPROM for the content of this file
- EFID – Identifier of the file within the file structure. This identifier is coded over two bytes.
- SFI - Short File Identifier coded over five bytes. It is used for an easy file selection. It is only used for the data files
- Access conditions – it specifies under which conditions the file may be accessed (read never, read always,..)

The **system files** are dedicated to store sensitive data that are used by the application. These data are protected in integrity by means of a checksum. Theses files may be created and updated in prepersonnalization or personalization phase. They are never readable.
Once created, these files are used by the application to work properly. They have to be created before any use of the application
In particular, theses files are used to store:

- The active authentication public key needed to perform the active authentication
- The active authentication private key needed to perform the active authentication
- The keys needed to perform the BAC authentication
- The application data, needed to store the persistent internal state of the application, such as the effective date, the role ID of the CVCA key, the expiration date of the CVCA key(s), the algorithm to use for the Terminal authentication….
- The list of the application present on the card.
- The Chip authentication private key needed to perform the chip authentication
- The CVCA root public key(s) needed to initiate the certificate chain.
- The temporary public key extracted from the certificate that was previously verified.

The **data files** are dedicated to store the data that may be retrieved. These data are protected in integrity by means of a checksum. These files may be created and updated in prepersonnalization or personalization phase. They are created in such a way that

- They can only be read in used phase provided, the BAC authentication was performed, except the DG3 & DG4 that can be read only after a successful EAC (see [R7])

Usually, the files that are considered for the passport are the followings:

- EF.COM – it describes which DGs are present in the file structure
- EF.SOD – it contains a certificate computed over the whole DGs. It ensures their integrity & authenticity
- DG1 up to DG16 – it contains information about the holder (picture, name,..)
- EF.TOE_Identification – it contains data stored by the manufacturer to identify the TOE (codop version, Certification BAC or EAC)
- EF.CVCA – it contains the name of the Root CVCA key(s) the passport knows

2.4.3 Other Data structures of the TOE

The TOE handles other data structure

- The CPLC data
- The optional code
- The application locks

These data are not seen as part of the file system.

The **CPLC data,** are data enabling to identify the ROM mask, the prepersonnalization phase & the personalization phase. Theses data are stored in

- ROM for the ROM CPLC data. Theses data are set in the ROM mask by the chip manufacturer. They enable to identify the ROM mask
- EEPROM for the prepersonnalization & personalization data

The TOE is not responsible for the CPLC data it stores. Therefore:

- In pre personalisation it is up to the manufacturer to store the correct pre personalization data
- In personalisation it is up to the personnalizer to store the correct personalisation data

These data may be retrieved at any time during the pre-personnalization & the personalization. Once the TOE is fully personalized, the CPLC data can not be retrieved without a BAC authentication, to preserve the privacy of the card holder.

The **optional code,** is an executable code that is stored in the EEPROM of the chip. This code is called by the Base Card when needed. These data are loaded during the prepersonnalization phase after the authentication of the manufacturer. Once an optional code is loaded, it is not possible to load any other optional code whether the TOE is in prepersonnalization phase or personalization phase. The TOE ensures the optional code's integrity and that it can not be read from the outside.

The **application locks** are within a particular area of the EEPROM memory. It is called OTP (One Time Programmable). When the TOE is delivered, all the bits of this area are set to '0'. Theses bits may be set (to'1') in prepersonnalization phase or personalization phase after the agent authentication (Manufacturer or Personnalizer). Once a bit is set to '1' in this area, it can not be reset anymore. This area is used to select the configuration of the TOE, in particular:

- If the BAC authentication is enforced in used phase ('0' = not enforced/'1' = enforced)
- If the Active authentication is activated ('0' = not activated/'1' = activated)
- If the Extended Access control is activated ('0' = not activated/'1' = activated)
- To indicate the TOE was prepersonalized ('1' = prepersonnalized)
- To indicate the TOE was personalized ('1' = personalized)
- To block the retrieval of the data (CPLC,…) in free mode ('0' = data can be retrieved in free mode/'1' = data can only be retrieved trought a BAC session)
- To enforce the use of an integrity checksum for each command sent to the TOE during the pre-personalization and personalization phase ('0' = integrity checksum enforced/'1' = No integrity checksum)

These OTP bytes are protected in integrity as they are copied in EEPROM too.

2.5 TOE life cycle according to the PP 9911

The Smart card life-cycle considered hereby, is the one described in [R22]. This protection profile is decomposed into 7 phases, described hereafter.

This life cycle is related to the different phases the designer/manufacturer/issuer has to go through to get a smart card ready to use. It starts from the design till the end of usage of the card.

It is depicted in the figure below :

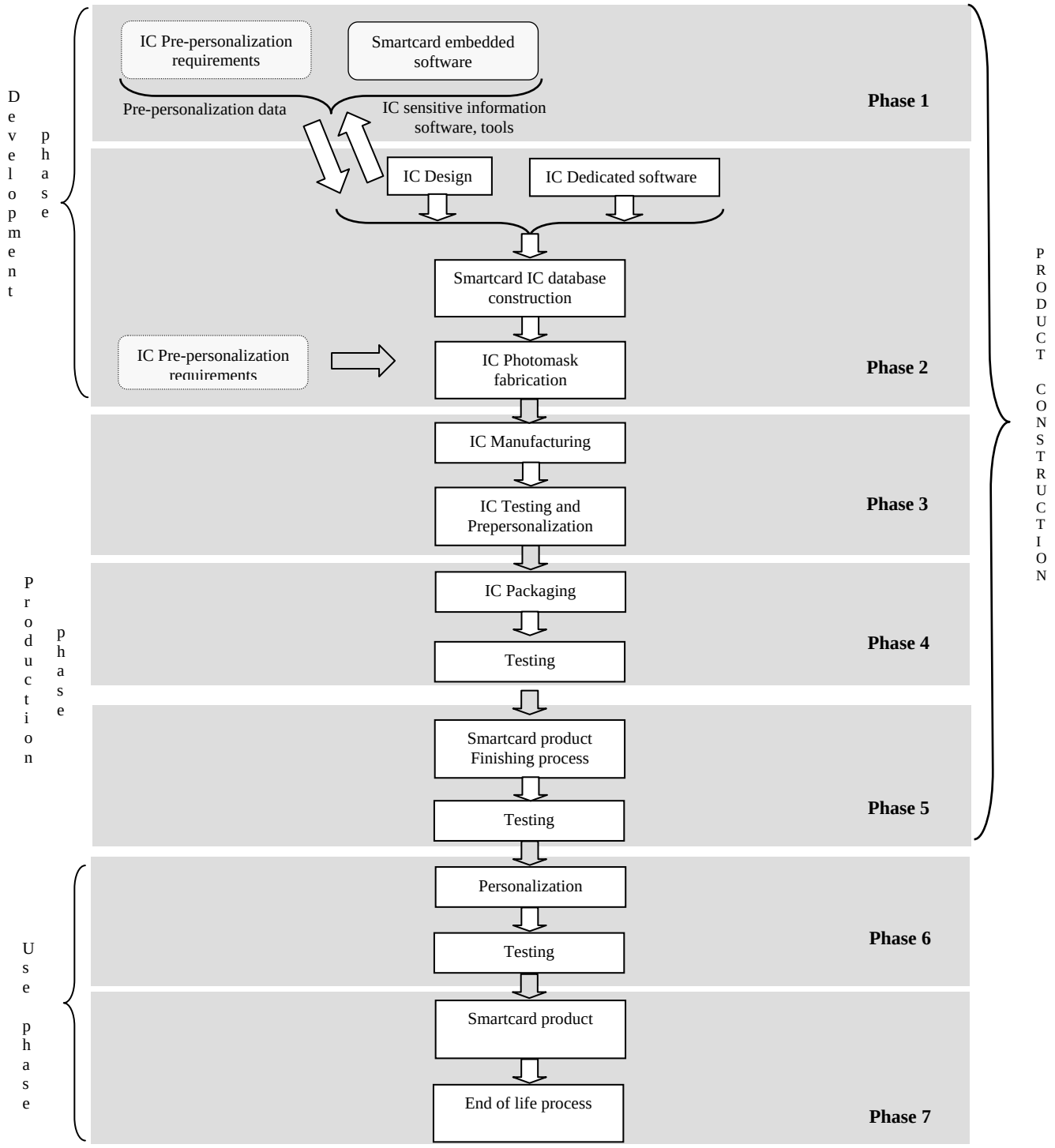


Figure 4 : Smart Card Life cycle

2.6 Description of the TOE environment

The TOE environment may be splitted into two different parts:

- The **development environment**, in which the TOE is designed, tested and manufactured. The security requirements that are applied reach the one described in [R9], [R10] and [R2].
- The **production environment** in which the TOE is tested and manufactured. The security requirements that are applied reach the one described in [R9], [R10] and [R2].
- The **User environment**, in which the TOE is used as stated in [R9], [R10] and [R2]. The security requirements that are requested and the assurance levels are met.

2.6.1 Development environment

2.6.1.1 Software development (phase 1)

This environment is limited to OBERTHUR TECHNOLOGIES' Nanterre site.
To ensure security, access to development tools and products elements (PC, emulator, card reader, documentation, source code,etc..) is protected. The protection is based on measures for prevention and detection of unauthorized access. Two levels of protection are applied:

- Access control to OBERTHUR TECHNOLOGIES Nanterre offices and sensitive areas.
- Access to developpement data through the use of a secure computer system to design, implement and test software

2.6.1.2 Hardware development (Phase 2)

The environment is limited to NXP site
The IC development environment is described in [R3]
The IC is certified EAL5+ and the IC certificate reference is BSI-DSZ-CC-0410

2.6.2 Production environment

2.7.2.1 IC manufacturing (phase 3)

The IC production environment is described in [R3]
The IC is certified EAL5+ and the IC certificate reference is BSI-DSZ-CC-0410

Depending on the choice made for the optional code loading, the optional code may be loaded during this phase

2.7.2.2 TOE manufacturing (phase 4 & 5)

Two situations may occur:

- The TOE may be manufactured by **OBERTHUR TECHNOLOGIES** in any of its manufacturing site
- The TOE may be manufactured at a **contractor's site**

The production sites present adequate security measures that fit the TOE protection during its manufacturing even if they are not in the scope of security assurance requirements for the environment.
More precisely, all the guidance for initialization, pre-personalization and personalization are applied with respect to **P.Manufact**.

If **OBERTHUR TECHNOLOGIES** is in charge of manufacturing the TOE, the following process will be applied

- Loading the optional code
- Loading the authentication key of the Personalization Agent.
- Preparing the TOE prior to delivering it to the Personalization Agent (phase 6)

If a **contractor** is in charge of manufacturing the TOE, the following process will be applied

- Loading the optional code – This step is optionnal/ It may be performed by **OBERTHUR TECHNOLOGIES**
- Loading the authentication key of the Personalization Agent.
- Preparing the TOE prior to delivering it to the Personalization Agent (phase 6)

The **OBERTHUR TECHNOLOGIES** manufacturing sites have all the needed certifications:

Note:
Even thought the optional code may be loaded in phase 5, it is important to notice the following issues:

- The optional code does not modify TSF
- The optional code can only be loaded by the manufacturer agent, having its personalization keys

Therefore, the phase 5, when an optional code is loaded may be covered by AGD_ADM.

2.7 Summary of the production environment

In this chapter, the TOE life cycle envisioned is the one of PP 9911 ([R22])

Three situations are envisioned for the production environments of the TOE.

- Case 1 : the optional code is loaded in phase 3 by the IC manufacturer. All the procedure is covered by its certificates. In phase 4 and 5, only the prepersonalisation of the TOE is performed as described in §2.8.5.
- Case 2 : the optional code is loaded in phase 5 in a manufacturing site of **OBERTHUR TECHNOLOGIES**
- Case 3 : the optional code is loaded in phase 5 in a manufacturing site of a **contractor**

This is summarized in the following table:

TOE life cycle	Case 1		Case 2	
	Phases	Environment	Phases	Environment
3	Optional code loading	Production environment at NXP	N/A	Production environment at NXP
4	IC packaging	Production environment of a (contractor orOBERTHUR TECHNOLOGIES)	IC packaging	OBERTHUR TECHNOLOGIES manufacturing site
5	Set up of the TOE		Optional code loading Set up of the TOE	
6	Personalization of the MRTD (While the TOE is under the Personalization Agent's operation)	Production environment of the customer	Personalization of the MRTD (While the TOE is under the Personalization Agent's operation)	Production environment of the customer
7	Operational Use		Operational Use	

Table 1 : Production environments of the TOE – case 1 & 2

TOE life cycle	Case 3	
	Phases	Environment
3	N/A	Production environment at NXP
4	IC packaging	contractor manufacturing site
5	Optional code loading Set up of the TOE	
6	Personalization of the MRTD (While the TOE is under the Personalization Agent's operation)	Production environment of the customer
7	Operational Use	

Table 2 : Production environments of the TOE – case 3

2.7.1 User environment

2.7.1.1 TOE Personnalization & testing (phase 6)

At the end of the phase 5, the card manufacturer delivers the TOE to the personnalizer of the MRTD service.

The TOE delivered to the personnalizer has the following features:

- The personnalizer must authenticate itself prior to any data exchange with the TOE. This authentication is performed by a cryptographic mean based on triple DES algorithm

- The TOE can be identified by the retrieval of its CPLC data.
- All the system files are created (key files, application data,…), as well as the EF.CVCA
- The optional code is loaded and is used by the TOE.
- The file EF.TOE_Identification is created and initialized. It is up to the personnalizer that receives the TOE to perform the following steps:

The personalization agent is responsible of:

- creating the DGs it needs
- loading the data into the DGs
- Setting the lock to enable the active authentication feature (if needed), and the BAC
- loading the key(s) – Chip authentication keys, CVCA keys, BAC keys, Active authentication keys (if activated)
- Loading the CVCA certificate
- Loading the counter limit for the BAC authentication and the Terminal authentication.
- Updating the CPLC data to fill the personalization data
- Setting the lock to block the CPLC data retrieval in free mode. This feature ensure the CPLC data can not be read without any BAC authentication
- Setting the lock to indicate the TOE is personnalized : the TOE switches in used phase.

Once the personalization agent finished the electrical personalization, it TOE is switched into personalized phase. This transition is irreversible.

Note:
Even though all the key files are present in the TOE when delivered to the personalization agent, it shall be cautious when personalizing the Chip authentication key and the CVCA root keys.
First of all, only one Chip authentication key is available (RSA or Elliptic curve). Moreover, the CVCA root key(s) shall be of the same type and length as the chip authentication key.
E.g, if the chip authentication key is a private key over an elliptic curve of 256 bits, the root CVCA key(s) shall be a public key over a 256 bits curve (regardless the terminal authentication algorithm chosen, ECDSA SHA-1/SHA-224/SHA-256).

2.7.1.2 TOE Operationnal Use (phase 7)

The TOE is delivered to the holder of the passport. The TOE behaves as described in [R4], [R5], [R7].

2.8 Description of the TOE's scope

The scope of this present security target is:

- TOE development phase realized in the OBERTHUR TECHNOLOGIES environment in phase 1
- TOE manufacturing phase realized in the NXP environment in phase 2 & 3

All other phases are out of the scope of the TOE. (i.e. security assurance requirements for the corresponding environment are out of the scope.
The TOE embedded software, developed and embedded during phases 1 to 3, aims to control and protect the TOE during phases 4 to 7.

As such, this Security Target addresses all the security features put in place in phases 4 to 7 but that are developed in phase 1 while [R3] addresses the security requirements for phases 2 and 3 for the same objective.

2.8.1 The development phase : phase 1

This phase is performed at OBERTHUR TECHNOLOGIES' site in NANTERRE (France).

2.8.2 The manufacturing phase : phase 2

This phase is performed at NXP manufacture. The security of the procedures is described in [R3] and ensured by the IC certificate reference BSI-DSZ-CC-0410

2.8.3 The prepersonnalization phase : phase 3

This phase is performed at NXP manufacture. It mainly consists in changing the manufacturer's MSK to set the Live MSK.
This phase is performed at NXP manufacture. The security of the procedures is described in [R3] and ensured by the IC certificate reference BSI-DSZ-CC-0410

2.8.4 The packaging phase : phase 4

This phase is performed in any OBERTHUR TECHNOLOGIES' manufacturing site . It mainly consists in mounting the chip in a

- module
- inlay
- datapage

The chip connections are soldered with the antennae connections.

2.8.5 *Initialization of the TOE : phase 5*

The behaviour of the TOE is obtained by a relevant electrical personalization made during the phase 5. Moreover, in this phase, the chip might be as well embedded within an inlay

The TOE addresses the application EAC based on RSA (travel document compliant with [R4], [R5], [R6] and[R7] with RSA cryptography)

The Profile EAC based on RSA requires the following key files:

- The Master File (EFID = 3F00) – creation
- The symmetric keys needed to perform the authentication of the Personalization Agent (EFID = 2C12) – It is created empty
- The DF LDS (EFID = 7F50) - creation
- The active authentication public and private key needed to perform the active authentication (EFID = B917) - (if enabled). It is created empty
- The symmetric keys needed to perform the BAC authentication (EFID = 2C12) - It is created empty
- The application data, needed to store the persistent internal state of the application, such as the effective date, the role ID of the CVCA key, the expiration date of the CVCA key(s), the algorithm to use for the Terminal authentication…(EFID = C001) - It is created empty
- The Chip authentication private key needed to perform the chip authentication using the DH algorithm (EFID = B919) - It is created empty
- The first CVCA root public key needed to initiate the certificate chain using the RSA algorithm (EFID = B921) - It is created empty
- The second CVCA root public key needed to initiate the certificate chain using the RSA algorithm (EFID = B923) - It is created empty
- The temporary public key (extracted from a certificate) using the RSA algorithm (EFID = BBAA) – It is created empty
- The file containing the list of the application present on the card (EFID = 0015) – It is created and updated
- The file containing the name of the trust point (CVCA key) the TOE knows (EF.CVCA EFID = 011C SFI = 1C) - It is created empty
- The file EF.TOE_Identification (SFI = 11/ EFID = 0111) – creation and update. This file enables to identify the TOE, in particular:
  - The version of the optional code
  - The TOE evaluation : EAC
  - The profile of the TOE : EAC based on RSA

The file structure for this profile may be depicted as follows:

File structure of the TOE
– EAC RSA Profile

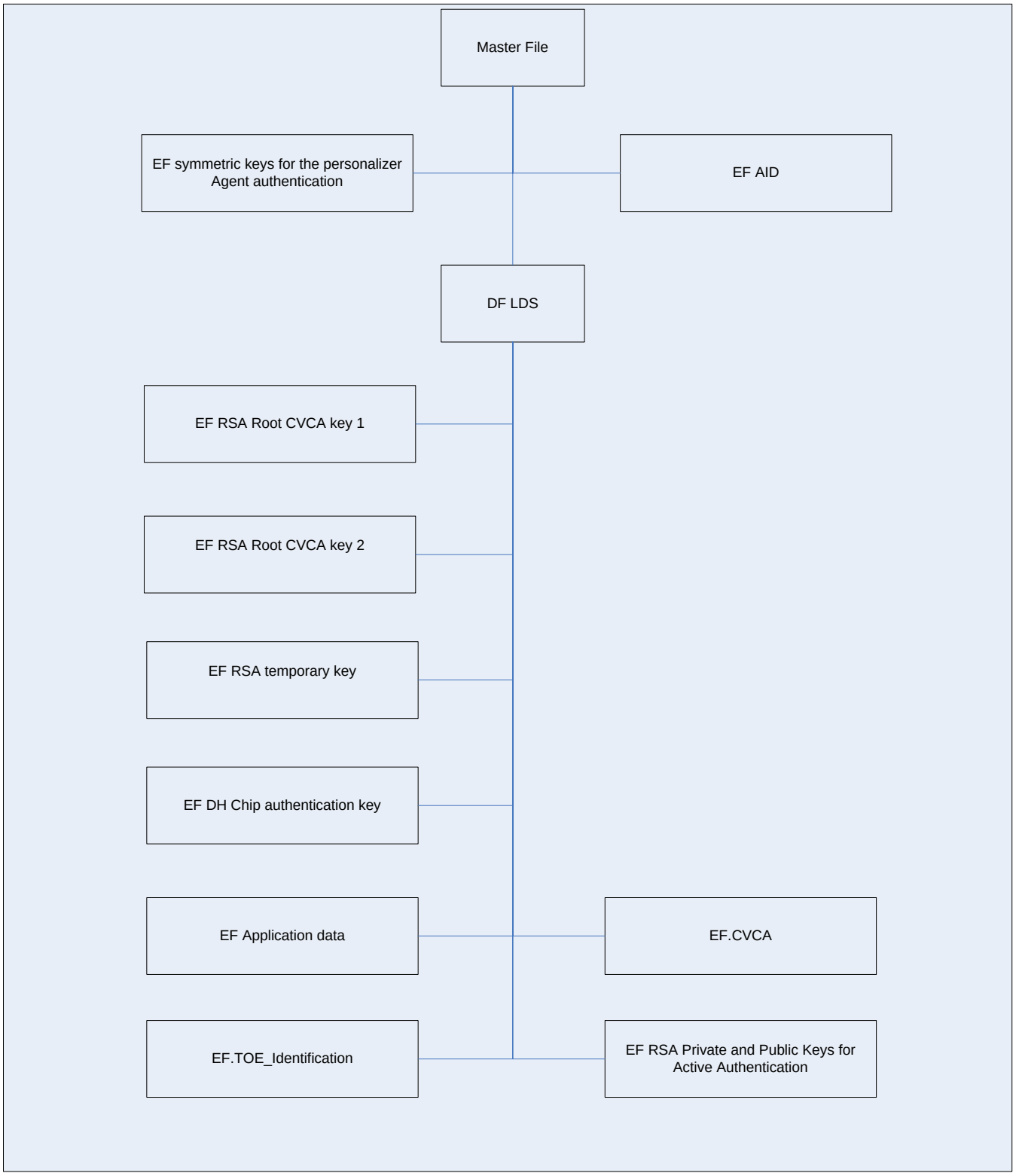


Figure 5 : File Structure of the TOE : EAC RSA Profile

2.8.5.1 Pre-personalization of the TOE

Once the TOE is received from the chip manufacturer, an authentication of the manufacturer shall be performed prior to any data exchange.
When the IC is received from the IC manufacturer, it does expects an integrity over the incoming data (a checksum – MAC - shall be added to any incoming command). It enables to ensure the data are really issued by the agent (manufacturer or personalization agent).
It is possible to bypass this constraint (checksum in any incoming command) through a dedicated mechanism (called "debrayed mode"). It is very convenient to fasten the pre-personalization & personalization phase.
As the Phase 2 and 3 (according to the life cycle described in the Protection profile we are considering) are performed in highly secured environments, this mechanism will be envisioned to speed up the electrical personalization process.
However, even though this feature is deactivated, the IC does still mandates the authentication of the actor (Manufacturer agent or personalization agent) prior to any operation.

The authentication should be performed with the Manufacturer secret key (MSK) the IC manufacturer loaded on the chip.

The following operation shall be performed:

1. Authentication of the manufacturer agent using its MSK.
2. Eventually, change the MSK of the manufacturer agent to a new one.
3. Authentication of the manufacturer agent using its MSK.
4. Configure the contactless speed.
5. Activate the "debrayed mode"
6. Activate the BAC lock : the Basic Access control at least shall be enforced in used phase prior to any data retrieval.
7. Activate the EAC lock : the Extended Access control shall be enforced in used phase prior to granting access to DG3 & DG4.
8. Load the optional code in the EEPROM
9. Activate the optional code
10. Create and update the file system, depending on the profile considered.
    - EAC based on RSA Profile
    - EAC based on Elliptic curves Profile
11. Load the authentication keys of the personalization agent (PK.ENC & PK.MAC). Theses keys are loaded enciphered with the session key for encipherment.
12. Write the CPLC data to update the bytes related to the pre-personalization phase
13. Set the lock to indicate the TOE is pre-personalized : the TOE switches in personalization phase

2.8.5.2 Configuration of the TOE software

The TOE software configuration may be depicted as follows :

Initialization of the TOE software

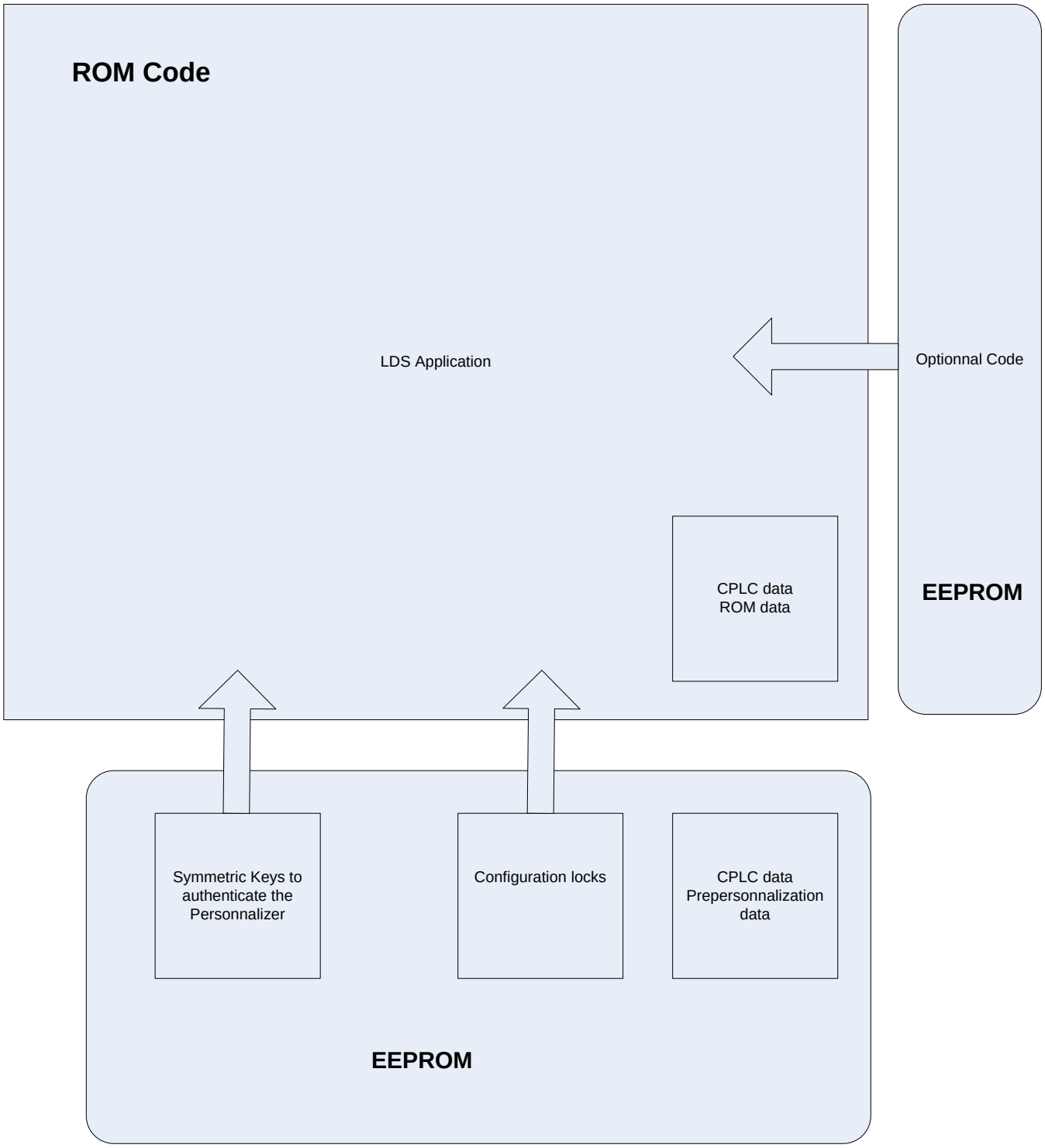


Figure 6 : Initialization of the TOE software

2.9 Mapping of the TOE life cycle with the life cycle described in the Protection profile

The protection profile considered considers a life cycle slightly different from the one depicted above. Here we provide a mapping between the PP we are considering and [R22]

TOE life cycle	Matching life cycle as described in the PP
1	Phase 1 : development
2	
3	Phase 2 : Manufacturing
4	
5	
6	Phase 3 : Personalization of the MRTD (While the TOE is under the Personalization Agent's operation)
7	Phase 4 :Operational Use

Table 3 : Mapping of life cycle states

For more details about this mapping, see [R23]

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 [R6]. 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 Active Authentication Public Key Info in DG 15 is used by the inspection system for Active Authentication of the chip. The Document security object is used by the inspection system for Passive Authentication of the logical MRTD.

The TOE, contains two sets of identification data

- A set uniquely identifying the chip, usually called the CPLC data.
- A set enabling to identify the TOE, in particular, its PP evaluation

The behaviour of the TOE securely handles its internal state, so that it can

- distinguish between the "Phase 3 - Personalization of the MRTD" and the "Phase 4 – Operational Phase". It is ensured by its life cycle state.
- Ensure no tearing can arises
- The configuration chosen (BAC, AA, EAC, Get Data is forbidden)

While a session is established with an inspection system, the TOE handles the two session keys used to ensure the confidentiality and integrity of the communications.

To ensure the TOE is protected against brute force attacks, both the BAC protocol and the Terminal authentication are protected by a counter error, distinct for each authentication, increased at each wrong consecutive authentication. When the limit is exceeded, the TOE performs the authentication within a period of time constantly increasing. Theses counters are reset when the matching authentication is successfully performed

All these data may be sorted out in two different categories.

- If they are specific to the user, they are User data
- If they ensures the correct behaviour of the application, they are TOS Security Data

User Data	
CPLC Data	Data uniquely identifying the chip. They are considered as user data as they enable to track the holder.
Personnal Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 – EF.DG13,EF.DG16)	Contains identification data of the holder
Sensitive biometric reference data (EF.DG3, EF.DG4)	Contain the fingerprint a the iris picture
Document Security Object (SOD) in EF.SOD	Contain a certicate ensuring the integrity of the file stored within the MRTD and their authenticity. It ensures the data are issued by a genuine country
Common data in EF.COM	Declare the data the travel document contains
Active Authentication Public Key in EF.DG15	Contain public data enabling to authenticate the chip thanks to an active authentication
Chip Authentication Public Key in EF.DG14	Contain public data enabling to authenticate the chip thanks to a chip authentication

Table 4 : User Data

TSF Data	
TOE_ID	Data enabling to identify the TOE
Personalisation Agent reference authentication Data	Private key enabling to authenticate the Personalisation agent
Basic Access Control (AC) Key	Master keys used to established a trusted channel between the Basic Inspection Terminal and the travel document
Active Authentication private key	Private key the chip uses to perform an active authentication
Session keys for the secure channel	Session keys used to protect the communication in confidentiality and in integrity
Life Cycle State	Life Cycle state of the TOE
Error counter for BAC protocol	Counter increased at each wrong consecutive authentication number of wrong consecutive authentication for BAC protocol
Public Key CVCA	Trust point of the travel document stored in persistent memory
CVCA Certificate	All the data related to the CVCA key (expiration date, name, ..) stored in persistent memory
Current Date	Current date of the travel document
Chip Authentication private Key	Private key the chip uses to perform a chip authentication
Error counter for Terminal protocol	Counter increased at each wrong consecutive authentication number of wrong consecutive authentication for terminal authentication protocol

Table 5 : TSF Data

An additional 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's holder is used by the traveller to authenticate himself as possessing a genuine MRTD.

3.2 Subjects

This security target considers the following subjects:

Subject	Definition
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
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalised the MRTD
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder
Personalization Agent	The agent is acting on the behalf of the issuing State or Organisation to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity the holder for the biographic data in the MRTD, (iii) 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) (iv) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability and (v) signing the Document Security Object defined in [R6].
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.
Inspection system	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder. The **Basic Inspection System** (**BIS**) (i) contains a terminal for the contact less 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 printed data in the MRZ 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 (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates. (iii) implements the Active Authentication Mechanism
Terminal	A terminal is any technical system communicating with the TOE through the contact less interface
Attacker	A threat agent trying (i) to identify and to trace the movement the MRTD's chip remotely (i.e. without knowing or reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD

Table 6 : Subjects

Application note 6 on Inspection system
According to [R6] the support of

(i) the Passive Authentication mechanism is mandatory, and

(ii) the Basic Access Control is optional.

In the context of this protection profile 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 protection profile will not consider the use of **Primary Inspection System** by the receiving State or Organization. The TOE of the current protection profile does not allow the Personalization agent to disable the Basic Access Control

for use with **Primary Inspection Systems** as described in the BSI-PP-0017 Machine Readable Travel Document with „ICAO Application", Basic Access Control.

Application note 7 on Attacker
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 itself 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 Active Authentication Public Key Info (DG15) if stored on the MRTD's chip,
- (iv) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip,and
- (v) the Document Signer Public Key Certificate (if stored on the MRTD's chip).

The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

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

The Inspection System is used by the border control officer of the receiving State
- (i) examining an MRTD presented by the traveller and verifying its authenticity and
- (ii) verifying the traveller 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 [R4]

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.

The Active authentication is also optional and can be enabled or disabled by the Personalization agent.

A.Signature_PKI	PKI for Passive Authentication

The issuing and receiving States or Organisations 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 over the Document Signer Public Key to the CA for certification,

(iii) keeps the Document Signer Private Key secret and

(iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs.

The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and organizations.

A.Auth_PKI	PKI for Inspection Systems

The issuing and receiving States or Organisations 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 Organisations 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 Organisations. The issuing States or Organizations distributes the public key 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 IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE.

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

T.Chip_ID	Identification of MRTD's chip

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contact less communication interface. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.*

T.Skimming	**Skimming the logical MRTD**

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contact less communication channel of the TOE. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

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 the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are 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 an other identity of the traveller. The attacker may alter the printed portrait and the digitised 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 MRTD's to create a new forged MRTD, e.g. the attacker write the digitised portrait and optional biometric reference data of finger read from the logical MRTD of a traveller 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 an other contact less chip.

The TOE shall avert the threat 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 initialisation and the personalization in the operational state after delivery to MRTD holder.

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

An attacker may exploit information that 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 contact less interface (emanation) or direct measurements (by contact to the chip still available even for a contact less chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

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) to modify User Data or (iv) to modify TSF data.

The physical tampering may be focused directly on the discloser 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 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
(ii) circumvent or 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 misuse of administration function. To exploit this an attacker needs information about the functional operation.

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 traveller 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.

3.5 Organisational Security Policies

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

P.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 Initialisation 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 digitised 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 authorized agents of the issuing State or Organization only.

P.Personal_Data	**Personal data protection policy**

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitised 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 [R4] 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 8:
The organisational security policy **P.Personal_Data** is drawn from the ICAO Technical Report [R4]. Note, that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE 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 of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate.

3.6 Specific Organisational Security Policies

P.Plat-Appl	**Development according to the IC recommandations**

The development of the Composite TOE was lead in accordance with the recommendations issued by the IC manufacturer. For More details see the "Design Compliance evidences".

P.Sensitive_Data_Protection	**Protection of sensitive data**

All the sensitive data are at least protected in integrity. The keys are protected in both integrity and confidentiality.

P.Key_Function	**Design of the cryptographic routines in order to protect the keys**

All the cryptographic routines are designed in such a way that they are protected against probing and do not cause any information leakage that may be used by an attacker.

4 Security Objectives

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

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 organisational security policies to be met by the TOE.

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

The TOE must ensure that the logical MRTD data groups DG1 to DG16, the Document security object according to LDS [R6] and the TSF data can be written by authorized Personalization Agents. The logical MRTD data groups DG1 to DG16 and the TSF data can be written only once and can not be changed after personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups DG 3 to DG16 are added.
Only the Personalization Agent shall be allowed to enable or to disable the TSF Basic Access Control.

Application note 9:
The **OT.AC_Pers** implies that:

1. The data of the LDS groups written during personalization for MRTD holder (at least DG1 and DG2) can not be changed by write access after personalization,
2. The Personalization Agents may
   (i) add (fill) data into the LDS data groups not written yet, and
   (ii) update and sign the Document Security Object accordantly.

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 [R4] and enforce **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 10:

The traveller grants the authorization for reading the personal data in EF.DG1 to EF.DG16 to theinspection 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 Technical Report [R6] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective **OT.Data_Conf**

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 an unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". If the TOE is configured for use with Basic Inspection Terminals only in Phase 4 "Operational Use" the TOE shall identify themselves only to a successful authenticated Basic Inspection System or Personalization Agent.

Application note 11:

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 Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [R7] The authenticity prove provided by MRTD's chip shall be protected against attacks with high attack potential.

Application note 12:
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 [R6] and
(ii) the hash value of the Authentication Public Key in the Document Security Object signed by the Document Signer.

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 Smart card Embedded Software,
(iii) to manipulate Soft-coded Smart card 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.

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

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:

(i) 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
(ii) Forcing a malfunction of the TOE and/or
(iii) A physical manipulation of the TOE.

Application note 13:
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 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

(i) Measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
(ii) 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)
(iii) Manipulation of the hardware and its security features, as well as
(iv) Controlled manipulation of memory contents (User Data, TSF Data) with a prior
(v) Reverse-engineering to understand the design and its properties and functions.

Application note 14:
In order to meet the security objectives **OT.Prot_Phys-Tamper** the TOE must be designed and fabricated so that it requires a high 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 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 15:
A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective **OT.Prot_Phys-Tamper**) provided that detailed knowledge about the TOE´s internals.

OT.Chip_Authenticity	**Protection against forgery**

The TOE must support the Inspection Systems to verify the authenticity of the MRTD's chip. The TOE stores a RSA private key to prove its identity, and that is used in chip authentication. This mechanism is described in [R4] as "Active Authentication".

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 so 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 the Initialisation 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 fulfils its security objectives and is resistant against obvious penetration attacks with low attack potential and against direct attacks with high attack potential against security function that uses probabilistic or permutation mechanisms.

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, to initialise, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.

4.3 Security Objectives for the Operational Environment

Issuing State or Organization

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

OE.Personalization	**Personalization of logical MRTD**

The issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the issuing State or Organisation

(i) establish the correct identity of the holder and create biographic 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 (including the digital signature in the Document Security Object) to protect the integrity and confidentiality 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 Key Pair,

(ii) ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment, and

(iii) distribute the Certificate of the Country Signing 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 include all data in the data groups DG1 to DG16 if stored in the LDS according to [R6].

OE.Auth_Key_MRTD	MRTD Authentication Key

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

(i) generate the MRTD's Chip Authentication Key Pair,

(ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and

(iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data	Authorization for Use of Sensitive Biometric Reference Data

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

OE.AA_Key_MRTD	Active Authentication Key

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

(i) generate the MRTD's Active Authentication Key Pair,

(ii) sign and store the Active Authentication Public Key in the Chip Authentication Public Key data in EF.DG15

OE.AA_Personalization	Active Authentication Personalization

The Personalization Agents enable or disable the Active Authentication function of the TOE according to the decision of the issuing State or Organization. If the Active Authentication function is enabled the Personalization Agents generate the Active authentication keys and store them in the MRTD's chip.

Receiving State or organization

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

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

The inspection system of the Receiving State must examine the MRTD presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD.

OE.Passive_Auth_Verif	**Verification by Passive Authentication**

The border control officer of the Receiving State uses the inspection system to verify the traveller 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 Organisation ensures the confidentiality and integrity of the data read from the logical MRTD. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

Application note 16:
The figure 2.1 in [R7] 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.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 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 the Document Security Object.

OE.Ext_Insp_Systems	**Authorisation of Extended Inspection Systems**

The Document Verifier of receiving States or Organizations authorize 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 Requirements

5.1 Extended Components Definition

This security target uses components defined as extensions to CC part 2. These components are defined in this security target.
They are the following:

- Family **FAU_SAS**
- Family **FCS_RND**
- Family **PIA_API**
- Family **FMT_LIM**
- Family **FPT_EMSEC**

5.2 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.

5.2.1 Class FAU Security Audit

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

FAU_SAS.1 Audit storage

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

Dependencies: No dependencies.

Application note 20:
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 Initialisation 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 fulfil the security objective **OD.Assurance**.

5.2.2 Class Cryptographic Support (FCS)

5.2.2.1 Cryptographic key generation (FCS_CKM.1)

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

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

FCS_CKM.1.1/ BAC_MRTD The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***[Document Basic Access Key Derivation Algorithm]*** and specified cryptographic key sizes ***[112 bits]*** that meet the following: ***[[R4], Annex E]***.

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

Application note 21:
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 [R4], 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 [R4], 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 TSF as required by **FCS_RND.1/MRTD**.

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

FCS_CKM.1/DH_MRTD Cryptographic key generation – Diffie-Hellman Keys by the MRTD

FCS_CKM.1.1/ The TSF shall generate cryptographic keys in accordance with a specified DH_MRTD cryptographic key generation algorithm ***[Diffie Hellmann]*** and specified cryptographic key sizes ***[112 bits]*** that meet the following: ***[[R7], Annex A.1.]***

Refinements
The size of DH Domain parameters the TOE handles is 1024 and 1536 bits

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

Application note 22:
The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [R7], 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. [R16]) or on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [R7], Annex A.1, [R12] and [R15] 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 [R4], annex E.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/ MRTD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[zeroisation]*** that meets the following: ***[no standard]***.

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

Application note 23:
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.

5.2.2.2 Cryptographic operation (FCS_COP.1)

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/RSA_MRTD Cryptographic operation – RSA signature by MRTD

The TSF shall perform ***[digital signature creation]*** in accordance with a specified cryptographic algorithm ***[RSA with SHA-1]*** and cryptographic key sizes ***[1024 bits]*** that meet the following: ***[scheme 1 of ISO/IEC 9796-2:2002]***.

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

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

FCS_COP.1.1/SHA_MRTD The TSF shall perform ***[hashing]*** in accordance with a specified cryptographic algorithm ***[SHA-1]*** and cryptographic key sizes ***[none]*** that meet the following: ***[FIPS 180-2]***.

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

Application note 24:
This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Session key derivation used by the Basic Access Control Authentication Mechanism and the chip authentication mechanism.

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

FCS_COP.1.1/TDES_MRTD The TSF shall perform ***[secure messaging – encryption and decryption]*** in accordance with a specified cryptographic algorithm ***[Triple-DES in CBC mode]*** and cryptographic key sizes ***[112 bits]*** that meet the following: ***[FIPS 46-3 [R17] and [R8]; Annex E]***.

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

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

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

Application note 26:
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_RSA
The TSF shall perform ***[digital signature verification]*** in accordance with a specified cryptographic algorithm ***[RSASSA-PKCS1-v1_5 and RSASSA-PSS with SHA-1 or SHA-256]*** and cryptographic key sizes ***[1024 bits and 1536 bits]*** that meet the following: ***[[R19] and [R20]]***

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

Random Number Generation (FCS_RND.1)

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

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 ***[the requirement to provide an entropy of at least 7.976 bit in each byte, following AIS 31 [R21]].***

Dependencies: No dependencies.

Application note 28:
This SFR requires the TOE to generate random numbers used for the authentication protocols as required by **FIA_UAU.4/MRTD**.

5.2.3 Class FIA Identification and Authentication

Application note 29:
The Table 1 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [R4], Annex E, and [R7]
Basic Access Control Authentication Mechanism	**FIA_UAU.4/MRTD** and **FIA_UAU.6/MRTD** **FIA_AFL.1**	**FIA_UAU.4/BT** and **FIA_UAU.6/T**	Triple-DES, 112 bits keys and Retail-MAC, 112 bit keys
Symmetric Authentication Mechanism for Personalization Agents	**FIA_UAU.4/MRTD**	**FIA_API.1/PT**	Triple-DES with 112 bits keys
Active Authentication Mechanism (if enabled)	**FIA_API.1/AA**	**FIA_UAU.4/BT**	RSA with 1024 bits. Algorithm according to [R4], Annex D.
Chip authentication protocol	**FIA_API.1/MRTD**, **FIA_UAU.5/MRTD**, **FIA_UAU.6/MRTD**	**FIA_UAU.4/GIS**, **FIA_UAU.5/GIS**, **FIA_UAU.6/GIS**	DH and Retail-MAC, 112 bit keys
Terminal authentication protocol	**FIA_UAU.5/MRTD**	**FIA_API.1/EIS**	RSASSA-PKCS1-v1_5 and RSASSA-PSS

Table 1: Overview on authentication SFR

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

(1) to establish the communication channel

(2) to read the initialization data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS

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

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

Dependencies: No dependencies.

Application note 30:
The MRTD's chip and the terminal establish the communication channel through the contactless. The Protocol Type A defines an "Answer to Select" (ATS) and 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 then one RFID. If the historical bytes are used to identify the product as usual for example with hard-mask version and component code (specific to the manufacturer), in particular context this could lead to an exploitation of the threat **T.Chip_Id** (e.g. in the case a MRTD holder has a chip manufactured by a local manufacturer, he could be traced in a foreign country where few holders could have the same ATS content). Therefore the ATS has to be set in such a manner, that it will not lead to a vulnerability by the means of identifying the chip (e.g. randomly using random number generator as required by **FCS_RND.1**).

Application note 31:
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 then one RFID. If this identifier is randomly selected it will not violate the **OT.Identification**. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by **T.Chip_ID**.
In the TOE, the chip identifier cannot be read in the operational phase, and the UID is randomized at each session

Application note 32:
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 themselves as

(i) 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.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

(1) to establish the communication channel

(2) to read the initialization data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS

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

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

Dependencies: FIA_UID.1 Timing of identification.

FIA_API.1/AA Authentication Proof of Identity - MRTD

FIA_API.1.1/AA The TSF shall provide an ***[Active Authentication Protocol]*** to prove the identity of the TOE.

Dependencies: No dependencies.

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

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

1. Basic Access Control Authentication Mechanism,

2. Authentication Mechanism based on Triple-DES,

3. Terminal Authentication protocol

Dependencies: No dependencies.

Application note 33:
All listed authentication mechanisms uses 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 [R7].

Application note 34:

The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [R4]. 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 fulfil the security objective **OT.Identification** and to prevent **T.Chip_ID**.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide:

1. Basic Access Control Authentication Mechanism

2. Symmetric Authentication Mechanism based on Triple-DES

3. Terminal Authentication protocol

4. Secure messaging in MAC-ENC mode,

to support user authentication.

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

1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms

Basic Access Control Authentication Mechanism with the Personalization Agent Keys,

Symmetric Authentication Mechanism with the Personalization Agent Key

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.

<u>Refinement:</u>

The TOE authenticates the Personnalization agent by a Symmetric Authentication Mechanism with Personnalizer Agent Key

Dependencies: No dependencies.

Application note 35:
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 [R4], 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.
For the TOE, the option (a) of the SFR is not available: Personalisation agent can only be authenticated using the Symmetric Authentication Mechanism with the Personalization Agent Key.

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:

1.Each command sent to 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.

Dependencies: No dependencies.

Application note 36:
The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [R4] 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.

FIA_AFL.1/Authentication failure handling – BAC Authentication

FIA_AFL.1.1/BAC The TSF shall detect when ***[an administrator configurable positive integer within range of acceptable value 1 to 255 consecutive]*** unsuccessful authentication attempts occur related to ***[BAC Authentication protocol]***.

Application note : This positive integer is set in personalisation phase by **the Personalization Agent**

FIA_AFL.1.2/BAC When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall ***[increase the period of time needed to perform the BAC Authentication protocol].***

FIA_AFL.1/Authentication failure handling – Terminal Authentication

FIA_AFL.1.1/TA The TSF shall detect when ***[an administrator configurable positive integer within range of acceptable value 1 to 255 consecutive]*** unsuccessful authentication attempts occur related to ***[Terminal authentication]***.

Application note : This positive integer is set in personalisation phase by **the Personalization Agent**

FIA_AFL.1.2/ TA When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall ***[increase the period of time needed to perform the Terminal authentication].***

Dependencies: FIA_UAU.1 Timing of authentication

FIA_API.1/CAP Authentication Proof of Identity - MRTD

FIA_API.1.1/CAP The TSF shall provide a ***[Chip Authentication Protocol according to [R7]]*** to prove the identity of the ***[TOE]*** .

Dependencies: No dependencies.

Application note 38:
This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [R7]. 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 [R4], Annex E.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).

5.2.4 Class FDP User Data Protection

Subset access control (FDP_ACC.1)

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 ***[Access Control SFP]*** on ***[terminals gaining write, read and modification access to data groups DG1 to DG16 and Active Authentication Private Key of the logical MRTD]***.

Dependencies: FDP_ACF.1 Security attribute based access control

Application note 39:
The Basic Access Control SFP addresses the configuration of the TOE for usage with Basic Inspection Systems only.

Security attribute based access control (FDP_ACF.1)

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 ***[Access Control SFP]*** to objects based on the following: ***1. Subjects:*** ***a. Personalization Agent,*** ***b. Basic Inspection System,*** ***c. Extended Inspection System*** ***c. Terminal,*** ***2. Objects:***

a. data in the data groups DG1 to DG16 of the logical MRTD
b. data in EF.COM
c. data in EF.SOD
d. Active Authentication Private Key

3. Security attributes
a. Authentication status of terminals,
b. Terminal Authorization.

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

1.The successfully authenticated Personalization Agent is allowed to write and to read the data of the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD, including the Active Authenticate Public Key

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 additional rules: ***[none]***.

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

1.A terminal authenticated as CVCA is not allowed to read to read data in the EF.DG3,
2.A terminal authenticated as CVCA is not allowed to read to read data in the EF.DG4,
3.A terminal authenticated as DV is not allowed to read to read data in the EF.DG3,
4.A terminal authenticated as DV is not allowed to read 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.

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

Application note 40:
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.

Inter-TSF-Transfer

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 ***[Access Control SFP]*** to be able to ***[transmit and receive]*** objects in a manner protected from unauthorised disclosure ***[after Chip Authentication]***.

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

FDP_UIT.1/MRTD Data exchange integrity - MRTD

FDP_UIT.1.1/MRTD The TSF shall enforce the ***[Access Control SFP]*** to be able to ***[transmit and receive]*** user data in a manner protected from ***[modification, deletion, insertion and replay]*** errors after Chip Authentication.

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

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

FDP_ITC.1/AA Import of user data without security attributes

This requirement deals with the import of Active Authentication private RSA key, when it is not generated on card. It is applicable for TOE with or without BAC.

FDP_ITC.1.1/AA The TSF shall enforce the ***[Access Control SFP]*** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/AA The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: ***[none]***.

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

5.2.5 Class FMT Security Management

FMT_MOF.1/AA Management of functions in TSF

.
FMT_MOF.1.1 The TSF shall restrict the ability to ***[enable and disable]*** the functions ***[TSF Active Authentication]*** to ***[Personalization Agent]***.

Refinement:
Once the TOE is delivered to the Personalization agent, the TSF Active Authentication is not enabled. It can either let it disabled, or enable it by writing a lock. Once enabled, the TSF Active Authentication can not be disabled.

Dependencies: No Dependencies

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:
1.Initialization,
2.Personalization,
3.Configuration

Dependencies: No Dependencies

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles
1.Manufacturer,
2.Personalization Agent,

5.Country Verifier Certification Authority,
6.Document Verifier,
7.Basic Inspection System,
8.Domestic Extended Inspection System
9.Foreign Extended Inspection System

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

Application note 43:
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.

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:
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

Dependencies: FMT_LIM.2 Limited availability.

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 capabilities (FMT_LIM.1)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow
1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated
3. Software to be reconstructed and
4. Substantial information about construction of TSF to be gathered which may enable other attacks.

Dependencies: FMT_LIM.1 Limited capabilities.

Application note 44:

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.

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialisation Data and Prepersonalisation Data

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to ***[write]*** the ***[Initialisation Data and Prepersonalisation Data]*** to ***[the Manufacturer]***.

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

Application note 45:
The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent that is the symmetric cryptographic Personalization Agent Authentication Key.

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

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

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

Application note 46:
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 Pre-personalization 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 – Initialisation of CVCA Certificate and Current Date

FMT_MTD.1.1/ CVCA_INI The TSF shall restrict the ability to ***[write]*** the
1. Initial Country Verifying Certification Authority Public Key,
2. Initial Country Verifier Certification Authority Certificate,
3. Initial Current Date

to ***[The Personalization Agent].***

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

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 ***[update]*** the
1. Country Verifier Certification Authority Public Key,
2. Country Verifier Certification Authority Certificate

to ***[Country Verifier Certification Authority]***.

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

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

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

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

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

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to ***[write]*** the ***[Document Basic Access Keys and the Active Authentication RSA private key]*** to ***[the Personalization Agent.]***

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

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

FMT_MTD.1.1/CAPK creation The TSF shall restrict the ability to ***[create]*** the Chip Authentication Private Key to ***[The manufacturer Agent]***.

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

Refinement:

The Manufacturer agent creates the chip authentication key needed by the TOE during the initialisation phase (phase 6). Once it was successfully done, the Personalization agent can not create Chip authentication private key(s), as they will not be used by the TOE. Therefore, by construction, only the manufacturer agent can create the chip authentication key.

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

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

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to ***[read]*** the

1. ***Document Basic Access Keys,***
2. ***the Active Authentication RSA private key***
3. ***the Chip authentication private key***
4. ***Personalization Agent Keys***

to ***[none]***.

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

FMT_MTD.3 Secure TSF data

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

Dependencies: ADV_SPM.1 Informal TOE security policy model
FMT_MTD.1 Management of TSF data

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 52:
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**

5.2.6 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-bypass ability 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.

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit ***[power variations, timing variations during command execution]*** in excess of ***[non useful information]*** enabling access to ***[personalization agent Authentication Key and Chip Authentication Private Key] and [Active Authentication RSA private key]***

FPT_EMSEC.1.2 The TSF shall ensure ***[any unauthorized users]*** are unable to use the following interface ***[smart card circuit contacts]*** to gain access to ***[Personalization Agent Authentication Key and Chip Authentication Private Key]*** and ***[Active Authentication RSA private key]***

Dependencies: No other components.

Application note 53
The ST writer shall perform the operation in **FPT_EMSEC.1.1** and **FPT_EMSEC.1.2**. 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 origin from internal operation of the TOE or may origin 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. The MRTD's chip has to provide a smart card contact less interface but may have also (not used by the terminal but maybe by an attacker) additional contacts according to ISO/IEC 7816-2 as well. 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.

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:
(1) Exposure to operating conditions where therefore a malfunction could occur,
(2) failure detected by TSF according to FPT_TST.1.

Refinement:
In particular, (1) means the TOE handles the tearing, or loss of field.

Refinement for FPT_FLS.1.1:

Type of failure	Secure state
Exposure to operating conditions where therefore a malfunction could occur	The transaction that was performed is ignored. No internal data are updated
failure detected by TSF according to FPT_TST.1.	During a session, while the card is powered, when a failure is detected, the TOE becomes mute. At next reset, the card is killed

Dependencies: ADV_SPM.1 Informal TOE security policy model

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 authorised user, at the conditions] [assignment : conditions under which the self test should occur]*** to demonstrate the correct operation of the TSF.

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

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

Dependencies: FPT_AMT.1 Abstract machine testing.

Application note 54:

The ST writer shall perform the operation in **FPR_TST.1.1**. If the MRTD's chip uses state of the art smart card technology it will run the some self tests at the request of the authorised user and some self tests automatically. e.g. a self test for the verification of the integrity of stored TSF executable code required by **FPT_TST.1.3** may be executed during initial start-up by the "authorised user" Manufacturer in the Phase 2 Manufacturing. Other self tests may run automatically to detect failure and to preserve of secure state according to **FPT_FLS.1** in the Phase 4 Operational Use, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist ***[physical manipulation and physical probing]*** to the TSF by responding automatically such that the ***[TSP]*** is not violated.

Dependencies: No dependencies.

Application note 55:
The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here

(i) assuming that there might be an attack at any time and
(ii) countermeasures are provided at any time.

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

FPT_RVM.1 Non-bypass ability 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.

Dependencies: No dependencies.

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 entrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC

Dependencies: No dependencies.

Application note 56:
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.

5.3 Security Requirements for the IT environment

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

5.3.1 Passive Authentication

The ICAO, the Issuing States or Organizations and the Receiving States or Organization 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 (DG1 to DG16) by means of the Document Security Object. The Technical Report [7] 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 guarantee of the validity of ***[logical the MRTD (DG1 to DG16) and the Document Security Object]***.

FDP_DAU.1.2/DS The ***[Document Signer]*** shall provide ***[Inspection Systems of Receiving States or Organization]*** with the ability to verify evidence of the validity of the indicated information.

Dependencies: No dependencies

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 the TOE may verify. 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 ***[RSA]*** and specified cryptographic key sizes ***[RSA 1024 or 1536 bits]*** that meet the following: [R7], Annex A.

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

FCS_COP.1/CERT_SIGN Cryptographic operation – Certificate Signing

FCS_COP.1.1/CERT_SIGN The PKI shall perform digital signature creation in accordance with a specified cryptographic algorithm ***[RSASSA-PKCS1-v1_5 and RSASSA-PSS with SHA-1 or SHA-256]*** and cryptographic key sizes ***[RSA 1024 or 1536 bits]*** that meet the following: ***[[R19] and [R20]]***.

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

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 ***[Document Basic Access Key Derivation Algorithm]*** and specified cryptographic key sizes ***[112 bits]*** that meet the following: ***[[R4], Annex E.]***

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 60:
The ST writer shall perform the open operation in the element **FCS_CKM.1.1/KDF_BT**. The assigned standard shall ensure 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**. The [R4], Annex E.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

FCS_CKM.4/BT Cryptographic key destruction - BT

FCS_CKM.4.1/BT The ***[Basic Terminal]*** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[irreversible erasing]*** that meets the following: ***[no standard]***.

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

Application note 61:
The ST writer shall perform the operation in **FCS_CKM.4.1/BT**. 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.

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

FCS_COP.1.1/SHA_BT The ***[Basic Terminal]*** shall perform ***[hashing]*** in accordance with a specified cryptographic algorithm ***[SHA-1]*** and cryptographic key sizes ***[none]*** that meet the following: ***[FIPS 180-2]***.

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

Application note 62:

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 ***[secure messaging – encryption and decryption]*** in accordance with a specified cryptographic algorithm ***[Triple-DES in CBC mode]*** and cryptographic key sizes ***[112 bits]*** that meet the following: ***[FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)]***.

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

Application note 63:
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 bit 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 ***[secure messaging – message authentication code]*** in accordance with a specified cryptographic algorithm ***[Retail-MAC]*** and cryptographic key sizes ***[112 bits]*** that meet the following: ***[FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)]***.

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

Application note 64:
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 bit 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 meets ***[the requirement to provide an entropy of at least 7.976 bit in each byte, following AIS 31 [R21]]***

Dependencies: No dependencies.

Application note 65:
The ST writer shall perform the operation in **FCS_RND.1.1/BT**. 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
1.Basic Access Control Authentication Mechanism.
2.Active Authentication Mechanism

Dependencies: No dependencies.

Application note 66:
The Basic Access Control Authentication Mechanism [R4] 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-authentication - Basic Terminal

FIA_UAU.6.1/BT The ***[Basic Terminal]*** shall re-authenticate the user under the conditions ***each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism***.

Dependencies: No dependencies.

Application note 67:
The Basic Access Control Mechanism specified in [R4] 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 fulfil 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 ***[Diffie Hellmann]*** and specified cryptographic key sizes ***[DH 1024 or 1536 bit]*** that meet the following: ***[[R7], Annex A.1].***

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

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 hashing in accordance with a specified cryptographic algorithm ***[SHA-1]*** and cryptographic key sizes ***[none]*** that meet the following: ***[FIPS 180-2 98].***

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

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

FIA_UAU.4.1/GIS The ***[General Inspection System]*** shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication Protocol.

Dependencies: No dependencies.

FIA_UAU.5/GIS Multiple authentication mechanisms – General Inspection System

FIA_UAU.5.1/GIS The ***[General Inspection System]*** shall provide

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication to support user authentication.

FIA_UAU.5.2/GIS The ***[General Inspection System]*** shall authenticate any user's claimed identity according to the 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 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

Dependencies: No dependencies.

FIA_UAU.6/GIS Re-authenticating – Re-authenticating of Terminal by the General Inspection System

FIA_UAU.6.1/ The ***[General Inspection System]*** shall re-authenticate the user under the GIS conditions

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.

Dependencies: No dependencies.

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

FDP_UCT.1.1/GIS The ***[General Inspection System]*** shall enforce the ***[Access Control SFP]*** to be able to ***[transmit and receive]*** objects in a manner protected from unauthorised disclosure after Chip Authentication.

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

FDP_UIT.1/GIS Data exchange integrity -General Inspection System

FDP_UIT.1.1/GIS The ***[General Inspection System]*** shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from ***[modification, deletion, insertion and replay]*** errors ***[after Chip Authentication]***.

FDP_UIT.1.2/GIS The ***[General Inspection System]*** shall be able to determine on receipt of user data, whether ***[modification, deletion, insertion and replay]*** has occurred ***[after Chip Authentication]***.

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

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.

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 ***[signature creation]*** in accordance with a specified cryptographic algorithm ***[RSASSA-PKCS1-v1_5 and RSASSA-PSS with SHA-1 or SHA-256]*** and cryptographic key sizes ***[RSA 1024, 1536]*** that meet the following: ***[[R19] and [R20]].***

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

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

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

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

FIA_API.1.1/EIS The ***[Extended Inspection System]*** shall provide a ***[Terminal Authentication Protocol]*** according to ***[[R7]]*** to prove the identity of the ***[Extended Inspection System]***.

Dependencies: No dependencies.

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:

(i) The Basic Access Control Mechanism which may be used by the Personalization Agent 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.

(ii) 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 protocol as requested by the **SFR FIA_UAU.4/MRTD** and **FIA_API.1/SYM_PT**.

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 an ***[Authentication Mechanism based on Triple-DES]*** to prove the identity of the ***[Personalization Agent].***

Dependencies: No dependencies.

Application note 75: 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 [R11] 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).

FCS_CKM.1/PERSO Cryptographic key generation – Generation of Active Authenticate Keys

This SFR deals with RSA key generation for Active Authentication when they are generated off card and imported into the card.

FCS_CKM.1.1/AA_MRTD The TSF shall generate ***[cryptographic keys]*** in accordance with a specified cryptographic key generation algorithm ***[RSA key generation]*** and specified cryptographic key sizes ***[1024 bits]*** that meet the following: ***[ANSI X9.31 [R18]].***

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

5.3.7 Terminals with Active Authentication feature

FCS_RND.1/AA Quality metric for random numbers

FCS_RND.1.1/AA The ***[Basic Terminal]*** shall provide a mechanism to generate random numbers that meets ***[the requirement to provide an entropy of at least 7.976 bit in each byte, following AIS 31 [R21]].***

Dependencies: No dependencies.

FCS_COP.1/RSA_AA Cryptographic operation – RSA signature

FCS_COP.1.1/RSA The TSF shall perform ***[digital signature verification]*** in accordance with a specified cryptographic algorithm ***[Public RSA with SHA-1]*** and cryptographic key sizes ***[1024 bits]*** that meet the following: ***[scheme 1 of ISO/IEC 9796-2:2002]***.

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

6 TOE SUMMARY SPECIFICATION

This part covers the IT security functions and specifies how these functions satisfy the TOE security functional requirement

6.1 Security function list of the composite TOE

Identification	Name
F.ACC_READ	Access control in reading

F.ACC_WRITE	Access control in writing
F.BAC	BAC mechanism
F.SM	Secure messaging mechanism
F.AUTH_PERSO	Personalization agent authentication
F.AA	Active Authentication
F.EAC	EAC mechanism
F.SELFTESTs	Self tests
F.ROLLBACK	Safe state management
F.PHYS	Physical protection
IC security functions	
F.RNG	Random number generator
F.HW_DES	Triple DES coprocessor
F.HW_AES	AES coprocessor
F.OPC	Control of operating conditions
F.PHY	Protection against physical manipulation
F.LOG	Logical protection
F.COMP	Protection of mode control
F.MEM_ACC	Memory access control
F.SFR_ACC	Special function register access Control

Table 7 : List of the security functions of the composite TOE

6.2 Security functions provided by the IC

The description of the security functions of the IC is provide in [R3]

6.3 Security functions provided by the TOE

F.ACC_READ - Access Control in reading
This function controls access to read functions (in EEPROM) and enforces the security policy for data retrieval.
Prior to any data retrieval, it authenticates the actor trying to access the data, and checks the access conditions are fulfilled as well as the life cycle state.

It ensures that at any time, the keys are never readable,i.e.:

- BAC keys
- Chip authentication keys
- CVCA keys
- Active Authentication private key
- Personalisation agent keys

It controls access to the CPLC data as well:

- It ensures the CPLC data can be read during the personalization phase
- It ensures it can not be readable in free mode at the end of the personalization step

Regarding the file structure:

In the operational use:

- The terminal can read user data (except DG3 & 4), the Document Security Object, the EF.CVCA, EF.COM only after BAC authentication and throught a valid secure channel.
- When the EAC was successfully performed, The terminal can only read the DG3 & 4 provided the access rights are sufficient throught a valid secure channel

In the personalisation phase

- The personalisation agent can read all the data stored in the TOE after it is authenticated by the TOE (using its authentication keys).
- The TOE is uniquely identified by a random number, generated at each reset. This unique identifier is called (U.I.D)

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

F.ACC_WRITE - Access Control in writing

This function controls access to write functions (in EEPROM) and enforces the security policy for data writing.
Prior to any data update, it authenticates the actor, and checks the access conditions are fulfilled as well as the life cycle state.

This security function ensures the **application locks** can only be written once in personalization phase to be set to '1'.

It ensures as well the **CPLC data** can not be written anymore once the TOE is personalized and that it is not possible to load an **optional code** or change the **personnalizer authentication keys** in personalization phase.

Regarding the file structure

In the operational use:

It is not possible to create any files (system or data files). Furthermore, it is not possible to update any system files.
However

- the application data is still accessed **internally** by the application for its own needs

- the Root CVCA key files and temporary key files are updated internally by the application according to the authentication mechanism described in [R7]

In the personalisation phase

- The personalisation agent can create and write throught a valid secure channel all the data files it needs after it is authenticated by the TOE (using its authentication keys.

F.BAC - BAC mechanism

This security function ensures the BAC is correctly performed. It can only be performed once the TOE is personalized with the symmetric BAC keys the Personalization Agent loaded beforehand during the personalization phase.
Furthermore, this security functions ensures the session keys are destroyed at the beginning of each BAC session.
A self-test on TDES and random generator is performed when a BAC session is requested.

It handles an error counter: after several failure in attempting to establish a BAC session (the error limit is reached), the TOE implements countermeasures to protect the TOE : it takes more and more time for the TOE to reply to subsequent wrong BAC attempts.

F.SM - Secure Messaging

This security function ensures the confidentiality & integrity of the channel the TOE and the IFD are using to communicate.
After a successful BAC authentication and successful Chip authentication, a secure channel is (re)established based on Triple DES algorithms.
This security function ensures

- No commands were inserted nor deleted within the data flow
- No commands were modified
- The data exchanged remain confidential
- The issuer of the incoming commands and the destinatory of the outgoing data is the one that was authenticated (through BAC or EAC)

If an error occurs in the secure messaging layer, the session keys are destroyed

F.AUTH_PERSO - Personalisation Agent Authentication

This security function ensures the TOE, when delivered to the Personnalization Agent, demands an authentication prior to any data exchange.

This authentication is based on a symmetric Authentication mechanism based on a Triple DES algorithm.

F.AA - Active Authentication

This security function ensures the Active Authentication is performed as described in [R4] & [R5]. (if it is activated by the personnalizer).

A self-test on the random generator is performed priori to any Active authentication. Moreover, this security function is protected against the DFA.

F.EAC - EAC mechanism

This security function ensures the EAC is correctly performed. In particular,

- it handles the certificate verification
- the management of access rights to DG3 & DG4
- the management of the current date (update and control towards the expiration date of the incoming certificate)
- the signature verification (in the certificate or in the challenge/response mechanism)

It can only be performed once the TOE is personalized with the chip authentication keys & Root CVCA key(s) the Personnalization Agent loaded during the personalization phase.

Furthermore, this security functions ensures the authentication is performed as described in [R7].

This security functions ensures the session keys for secure messaging are destroyed at each successful Chip Authentication step.

It handles an error counter: after several failure in attempting to strongly authenticate the GIS (the error limit is reached), the TOE implements countermeasures to protect the TOE : it takes more and more time for the TOE to reply to subsequent wrong GIS authentication attempts.

F.SELFTESTS - Self tests

The TOE performs self tests on the TSF data it stores to protect the TOE. In particular, it is in charge of the:

- DFA detection for the Active authentication
- Self tests of the random generator before the BAC and Active Authentication
- Self tests of the DES before the BAC
- Monitoring of the integrity of keys, files and TSF data
- Monitoring the integrity of the optional code (at start up)
- Protecting the cryptographic operation
- …….

The integrity of the files are monitored each time they are accessed and the integrity of the optional code is checked each time the TOE is powered on.
The integrity of keys and sensitive data is checked each time they are used/accessed.

F.ROLLBACK - Safe state management
This security functions ensures that the TOE gets bask to a secure state when

- an integrity error is detected by F.SELFTESTS
- a tearing occurs (during a copy of data in EEPROM)

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

F.PHYS – Physical protection
This security function protects the TOE against physical attacks

6.4 Coverage of the security functions of the TOE by the security functions of the IC

Security function of the TOE	Description	Covered by
F.ACC_READ	Access control in reading	F.MEM_ACC
F.ACC_WRITE	Access control in writing	F.MEM_ACC
F.BAC	BAC mechanism	F.RNG F.HW_DES F.COMP F.MEM_ACC F.SFR_ACC
F.SM	Secure messaging mechanism	F.HW_DES F.COMP F.MEM_ACC F.SFR_ACC
F.AUTH_PERSO	Personalization agent authentication	F.RNG F.HW_DES F.COMP F.MEM_ACC F.SFR_ACC
F.AA	Active Authentication	F.RNG F.COMP F.MEM_ACC F.SFR_ACC
F.EAC	EAC mechanism	F.RNG F.COMP F.MEM_ACC F.SFR_ACC
F.SELFTESTS	Self tests	F.OPC

F.ROLLBACK	Safe state management	F.MEM_ACC
F.PHYS	Physical protection	F.PHY F.LOG F.OPC

Table 8 : TOE security function vs chip security functions

6.5 Assurance measures

This chapter defines the list of the assurance measures required for the TOE security assurance requirements. The EAL4+ is claimed

6.5.1 Assurance measure list

Measure	Name
AM_ACM	Configuration management
AM_ADO	Delivery and operation
AM_ADV	Development
AM_AGD	Guidance documents
AM_ALC	Life cycle
AM_ATE	Tests
AM_AVA	Vulnerability assessment

Table 9 : Assurance measures list

6.5.2 AM_ACM: Configuration management

This assurance measure ensures the configuration management. The CM responsible is in charge to write the CM plan, use the CM system and validate the CM system in order to confirm that ACM_XXX.Y components are completed

6.5.3 AM_ADO: Delivery and Operation

This assurance measure ensures the delivery and operation. The delivery responsible is in charge to write delivery documentation and validate it in order to confirm that the procedure is applied.

6.5.4 AM_ADV: Development

This assurance measure ensures the development. The development responsible is in charge to design the TOE, write development documentation and validate it in order to confirm that the related security functional requirements are completed by security functions.

6.5.5 AM_AGD: Guidance documents

This assurance measure ensures the guidance documents. The guidance responsible is in charge to write administrator and user guidance. The documentation provides the rules to use and administrate the TOE in a secured manner.

6.5.6 *AM_ALC: Life cycle*

This assurance measure ensures the life cycle. The life cycle responsible is in charge to confirm that the life cycle process is applied.

6.5.7 *AM_ATE: Tests*

This assurance measure ensures the tests. The test responsible is in charge to write tests and execute it in order to confirm that the security functions are tested.

6.5.8 *AM_AVA: Vulnerability assessment*

This assurance measure ensures the vulnerability assessment. The security responsible is in charge to confirm that the security measures are suitable to meet the TOE security objectives conducing a vulnerability analysis.

7 PP CLAIMS

7.1 PP reference

The PP EAC [R10] is claimed

7.2 PP refinements

Non applicable

7.3 PP additions

The additional functionality is the Active Authentication (AA) based on the ICAO PKI V1.1. It implies some addition to the standard PP.

The following SFRs are added to the standard PP for the TOE:

- FCS_COP.1 / RSA
- FIA_API.1 / AA
- FDP_ITC / AA
- FMT_MOF.1 / AA

The following SFRs are added to the standard PP for the IT environment:

- FCS_CKM.1 / PERSO
- FCS_RND.1/AA
- FCS_COP.1/RSA_AA

The following Objective for the TOE is added to the standard PP:

- OT.Chip_authenticity "Protection against forgery"

The following Objectives for the IT environment are added to the standard PP:

- OE.AA_Key_MRTD "Active Authentication key"
- OE.AA_Personalization 'Active Authentication Personalization"

Moreover, the composition with the IC mandates to introduce complementary OSPs:

- P.Plat_Appl "Development according to the IC recommendations"
- P.Sensitive_Data_Protection "Protection of sensitive data"
- P.Key_Function "Design of the cryptographic routines in order to protect the keys"

8 Rationale

This section presents the evidence to be used for the ST evaluation. This evidence supports the claim that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

This rational shows the composition with the IC that is evaluated EAL4+.

8.1 Composition with the IC Security target features

8.1.1 Coverage of the assumptions of the IC (A.IC vs TOE)

The assumptions defined in the Security target of the IC are covered by the following TOE features:

IC Assumption	Covered by	Justification
A.Process-Card Protection during Packaging, Finishing and Personalisation	**P.Manufact**	Security procedures are used during TOE packaging, finishing and prepersonnalization (During Phase 2)
A.Plat-Appl Usage of Hardware Platform The Smartcard Embedded Software is designed so that the requirements from the following documents are met: • TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and • (ii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.	**P.Plat-Appl**	The development of the Smart Card embedded Software was lead in accordance with the recommendations issued by the IC manufacturer. For more details see the "Design Compliance Evidence"

A.Resp-Appl Treatment of User Data "All User Data are owned by Smartcard Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context."	**P.Sensitive_Data_Protection**	The Composite TOE ensure the confidentiality of the cryptographic keys it stores
A.Check-Init Check of initialization data by the Smartcard Embedded Software « The Smartcard Embedded Software must provide a function to check Initialisation data. The data is defined by the customer and injected by the TOE Manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability"	**P.Manufact**	Security procedures and manufacturing guidance are used during IC development and production phase (Phase 2)
A.Key-Function Usage of Key-dependent Functions « Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address • the cryptographic routines which are part of the TOE and • the processing of User Data including cryptographic keys »	**P.Key_Function**	The Cryptographic routines are designed in such a way that they do not compromise key by any leak of information

8.1.2 *Coverage of the environment objectives of the IC (OE.IC vs TOE)*

The environment objectives defined in the Security target of the IC are covered by the following TOE features:

Objectives for the IT environment required by the IC	Covered by	Justification
OE.Plat-Appl Usage of Hardware Platform The Smartcard Embedded Software is designed so that the requirements from the following documents are met: • TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and • (ii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.	**P.Plat-Appl**	The development of the Smart Card embedded Software was lead in accordance with the recommendations issued by the IC manufacturer. For more details see the "Design Compliance Evidence"
OE.Resp-Appl Treatment of User Data "All User Data are owned by Smartcard Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context."	**P.Sensitive_Data_Protection**	The Composite TOE ensure the confidentiality of the cryptographic keys it stores as well as the integrity of all the sensitive data.
OE.Process-TOE Protection during TOE Development and Production (Phase 2 & 3 of the PP 9911 [R22])	**P.Manufact**	This objective is ensured by the security procedures and manufacturing guidelines of NXP manufacturing site
OE.Process-Card Protection during Packaging, Finishing and Personalisation	**P.Manufact**	Security procedures are used during TOE packaging, finishing and prepersonnalization (During Phase 2 of this PP)

OE.Check-Init Check of initialization data by the Smartcard Embedded Software « The Smartcard Embedded Software must provide a function to check Initialisation data. The data is defined by the customer and injected by the TOE Manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability"	**P.Manufact**	Security procedures and manufacturing guidance are used during IC development and production phase (Phase 2 of this PP)

8.1.3 Coverage of the organizational security policies of the IC by the TOE (P.IC vs TOE)

The organizational security policies defined in the Security target of the IC are covered by the following TOE features:

IC Organizational Security Policy	Covered by	Justification
P.Add-Components Additional Specific Security Components	**P.Plat-Appl**	The development of the Smart Card embedded Software was lead in accordance with the recommendations issued by the IC manufacturer. For more details see the "Design Compliance Evidence"

8.1.4 Coverage of the Objectives of the TOE by the objectives of the IC (O.IC vs O.TOE)

IC Objectives	Ensures	Covers
O.Leak-Inherent	Protection against Inherent Information Leakage	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper
O.Phys-Probing	Protection against Physical Probing	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper
O.Malfunction	Protection against Malfunctions	OT.Prot_Malfunction
O.Phys-Manipulation	Protection against Physical Manipulation	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper
O.Leak-Forced	Protection against Forced Information Leakage	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper
O.Abuse-Func	Protection against Abuse of Functionality	OT.Prot_Abuse-Func

O.Identification	TOE Identification	OT.Identification
O.RND	Random Numbers	OT.Data_Conf OT.Sens_Data_Conf
O.HW_DES3	Triple DES Functionality	OT.AC_Pers OT.Data_Int OT_Data_Conf OT.Sens_Data_Conf
O.HW_AES	AES Functionality	N/A
O.MF_FW	MIFARE Firewall	N/A
O.MEM_ACCESS	Area based Memory Access Control	OT.Prot_Abuse-Fonc OT.Data_Conf OT.Sens_Data_Conf OT.AC_Perso OT.Chip_Auth_Proof
O.SFR_ACCESS	Special Function Register Access Control	OT.Prot_Abuse-Fonc OT.Data_Conf OT.Sens_Data_Conf OT.AC_Perso OT.Chip_Auth_Proof
O.CONFIG	Protection of configuration data	OT.Prot_.Malfunction OT.Prot_Abuse-Fonc

8.1.5 Coverage of the threats of the TOE (T.TOE vs IC.O)

The threats of the TOE are covered by the following IC objectives & assumptions:

Threats of the TOE	Covered by	Justification
T.Chip_ID	O.Leak-Inherent O.Phys-Probing O.Phys-Manipulation O.Leak-Forced O.Abuse-Func O.Malfunction O.RND	Theses IC objectives ensures • the MRZ keys used by the TOE can not be disclosed by a physical way (probing, leakage, physical manipulation,..). It ensures the attacker can not read the logical MRTD • the authentication can not be replayed by means of a random number.
T.Skimming	O.Leak-Inherent O.Phys-Probing O.Phys-Manipulation O.Leak-Forced O.Abuse-Func O.Malfunction	These IC objectives ensures the MRZ keys can not be disclosed by a physical way (probing, leaking, physical manipulation,…)
T.Read_Sensitive_Data	O.RND O.HW_DES3	O.RND ensures the authentication between the Inspection system and the TOE is unpredictable. O.HW_DES3 ensures the communication are protected in confidentiality and integrity

T.Forgery	O.Phys-Manipulation O.Abuse-Func O.Malfunction	O.Phys-Manipulation, O.Abuse-Func and O.Malfunction provide protection against forgery of the Logical MRTD stored in the TOE..
T.Counterfeit	O.Leak-Inherent O.Phys-Probing O.Phys-Manipulation O.Leak-Forced O.Abuse-Func O.Malfunction	These objectives ensure that no data may be copied from the TOE
T.Abuse-Func	O.Mem_Access O.SFR_Access O.Abuse-Func O.Malfunction	These objectives ensure the functions for personalization and initialization can not be used in operational state.
T.Information_Leakage	O.Leak-Inherent O.Phys-Probing O.Phys-Manipulation O.Leak-Forced O.Abuse-Func O.Malfunction	These objectives ensure there is no information leakage
T.Phys_Tamper	O.Leak-Inherent O.Phys-Probing O.Phys-Manipulation O.Leak-Forced O.Abuse-Func O.Malfunction	These objectives ensure there is no physical tampering
T.Malfunction	O.Abuse-Func O.Malfunction	

8.2 Security function rationale

The following section demonstrates that the Security Functions supplied by the TOE fulfill [R9]/[R10] Security Functional Requirements.

.

8.2.1 Security function coverage

In this chapter, an explanation for each SFR is given, as well as the security functions to which it is linked.

FAU_SAS.1 /Audit Storage

This SFR requires the TOE to permanently store an identifier of the Manufacturer Agent. This identifier shall be readable by the personalization Agent for traceability purposes.

This requirement is fulfilled by the CPLC data the Manufacturer agent stores in phase 5. It is readable by the Personalization Agent. Once the TOE is personalized (in phase 7), this field can not be read anymore.

This requirement is fulfilled by F.ACC_READ and F.ACC_WRITE

FCS_CKM.1 /BAC MRTD

This SFR requires the TOE to generate the session keys according to the given description after BAC establishment.
This requirement is fulfilled by F.BAC.

FCS_CKM.1 /DH MRTD Cryptographic key generation

This SFR requires the TOE to generate the session keys according to the given description after the Chip Authentication establishment.
This requirement is fulfilled by F.EAC.

FCS_CKM.4 /Cryptographic key destruction

This SFR requires the TOE to destroy the session keys according to the given method.
This requirement is fulfilled by

- F.EAC : this security function destroys the session keys generated by the BAC establishment when they are regenerated by the chip authentication establishment
- F.SM : this security function destroys the session keys when an error occurs in the secure channel (wrong checksum, wrong encipherment, wrong structure of the incoming command, sequence broken)
- F.BAC : this security function destroys the session keys when the BAC is (re) established

FCS_COP.1 / RSA MRTD Cryptographic Operation

This SFR requires the TOE to compute the signature performed for the Active Authentication step as described.
This requirement is fulfilled by F.AA.

FCS_COP.1 / SHA MRTD Cryptographic Operation

This SFR requires the TOE to generate the session keys with the hashing algorithm specified.
This requirement is fulfilled by

- F.EAC for the session keys regenerated by the Chip authentication establishment
- F.BAC for the session keys regenerated by the BAC establishment

FCS_COP.1 / TDES MRTD Cryptographic Operation

This SFR requires the TOE to compute the encipherment/decipherment used to ensure the confidentiality of the data exchanged as described.
This requirement is fulfilled by F.SM.

FCS_COP.1 / MAC MRTD Cryptographic Operation

This SFR requires the TOE to compute the MAC used to ensure the integrity of the data exchanged as described.
This requirement is fulfilled by F.SM.

FCS_COP.1 / SIG VER Cryptographic Operation

This SFR requires the TOE to verify the signature used for:

- The certificate used in the terminal authentication steps
- The terminal authentication (verification of the signature computed by the Extended GIS)

As described
This requirement is fulfilled by F.EAC.

FCS_RND.1 / MRTD quality metric for random numbers

This SFR requires the TOE to ensure sufficient entropy for the random numbers it generates.
This requirement is fulfilled by

- F.BAC for the BAC establishment
- F.EAC for the Terminal authentication.
- F.ACC_READ for the UID number generation
- F.AA for the Active authentication (random used for the padding)

FIA_UID.1 / Timing of authentication

This SFR requires to be able to retrieve from the TOE:

- during the phase 2, the CPLC data set by the manufacturer Agent for tracability/identification purposes.
- during the phase 2 & 3, the ATS.
- during the phase 4, to read the logical MRTD, if the TOE is configured to be read without any BAC establishment.

These data shall be retrievable without any identification of the user. This requirement is fulfilled by F.ACC_READ.

Furthermore, this SFR requires that no other operations can be performed without a preceding identification of the user. This requirement is fulfilled by:

- F.AUTH_PERSO in phase 3
- F.BAC in phase 4

FIA_UAU.1 / Timing of authentication

This SFR requires to be able to retrieve from the TOE:

- during the phase 2, the CPLC data set by the manufacturer Agent for tracability/identification purposes.
- during the phase 2 & 3, the ATS.
- during the phase 4, to read the logical MRTD, if the TOE is configured to be read without any BAC establishment.

These data shall be retrievable without any authentication of the user. This requirement is fulfilled by F.ACC_READ.

Furthermore, this SFR requires that no other operations can be performed without a preceding authentication of the user. This requirement is fulfilled by:

- F.AUTH_PERSO in phase 3
- F.BAC in phase 4

FIA_API.1 / AA Authentication proof of identity

This SFR is fulfilled by F.AA.

FIA_UAU.4 / MRTD Single use authentication mechanisms

This SFR is fulfilled by

- F.BAC for the BAC establishment. It is ensured by the use of a eight bytes random number.
- F.AUTH_PERSO for the authentication of the Personalization Agent. It is ensured by the use of a counter, which always has a unique value.

- F.EAC for the Terminal authentication step. is ensured by the use of a eight bytes random number.

FIA_UAU.5 / Multiple authentication mechanisms

This SFR is fulfilled by

- F.BAC for the BAC establishment : The BAC can only successfully performed with the Document basic access keys
- F.AUTH_PERSO for the authentication of the Personalization Agent. This mechanism is based on a Triple DES mechanism. The authentication can only be performed with the Personalization Agent keys.
- F.EAC . It ensures the secure messaging sessions keys are correctly used before and after the chip authentication step (in particular that the Terminal authentication step is performed with the new session messaging keys)
- F.SM : it ensures the communication are protected in confidentiality and integrity after successful BAC and Chip Authentication

FIA_UAU.6 / MRTD re authenticating

This SFR requires each data sent to the TOE are identified as being sent by the authenticated GIS. This is fulfilled by the MAC attached to each incoming command.

Ths SFR is fulfilled by F.SM that

- enforces the secure messaging once the BAC step and the Chip authentication step are performed
- Verifies the MAC of the incoming command with the valid session key (session key generated at BAC establishment before the Chip authentication step, session key generated at Chip Authentication step afterwards)

FIA_AFL.1 / Authentication failure handling

This SFR requires the TOE to take actions when several consecutive failure in the BAC establishment step and Terminal authentication steps arise.

This requirement is fulfilled by

- F.BAC for the BAC establishment step
- F.EAC for the terminal authentication step

FIA_API.1 / CAP Authentication proof of authenticity

This SFR is fulfilled by F.EAC

FDP_ACC.1 / Subset Access Control

This SFR is fulfilled by

- F.ACC_READ for the access control for data retrieval
- F.ACC_WRITE for the access control on data writing
- F.AA for the Access Control on Active authentication

FDP_ACF.1 / Subset Attribute based Access Control

This SFR is fulfilled by

- F.ACC_READ for the access control for data retrieval
- F.ACC_WRITE for the access control on data writing
- F.AA for the Access Coqntrol on Active authentication

FDP_UCT.1 / MRTD basic data exchange confidentiality

This SFR requires each data sent to and by the TOE to be protected in confidentiality. This is fulfilled by an encipherment of all the data exchanged.
This SFR is fulfilled by F.SM that

- enforces the secure messaging once the BAC step and the Chip authentication step are performed
- Ciphers and deciphers the data exchanged with the valid session key (session key generated at BAC establishment before the Chip authentication step, session key generated at Chip Authentication step afterwards)

FDP_UIT.1 / MRTD data exchange integrity

This SFR requires each data sent to and by the TOE are protected in integrity. This is fulfilled by a MAC over all the data exchanged.
This SFR is fulfilled by F.SM that

- enforces the secure messaging once the BAC step and the Chip authentication step are performed
- Verifies/computes the MAC of all data exchanged with the valid session key (session key generated at BAC establishment before the Chip authentication step, session key generated at Chip Authentication step afterwards)

FDP_ITC.1 / AA import of user data without security attributes

This SFR is fulfilled by F.ACC_WRITE.

FMT_MOF.1 / AA Management of function in TSF

It is achieved by writing the relevant lock in the TOE. This SFR is fulfilled by F.ACC_WRITE.

FMT_SMF.1 / Specification of Management function

This SFR is fulfilled by F.ACC_WRITE & F.AUTH_PERSO

FMT_SMR.1 / Security Roles

This SFR requires the TOE to authenticate several roles. It is fulfilled by :

- F.AUTH_PERSO for the authentication of the Role Manufacturer & personalization Agent
- F.BAC for the authentication of the Basic inspection System
- F.EAC for the authentication of the CVCA, DV, foreign and extended inspection system

FMT_LIM.1 / Limited capabilities

This SFR is fulfilled by F.ACC_READ, F.SELFTESTS and F.PHYS

FMT_LIM.2 / Limited availibility

This SFR is fulfilled by F.ACC_READ, F.SELFTESTS and F.PHYS

FMT_MTD.1 / INI_ENA Management of TSF Data

This SFR requires that only the Manufacturer can write the Personalization keys and the Initialization data used to authenticate the manufacturer agent. This SFR is fulfilled by F.ACC_WRITE

FMT_MTD.1 / INI_DIS Management of TSF Data

This SFR requires that only the Personalization Agent can block the retrieval of the Initialization data. It is achieved by writing the relevant lock in the TOE. This SFR is fulfilled by F.ACC_WRITE

FMT_MTD.1 / CVCA_INI Management of TSF Data
This SFR is fulfilled by F.ACC_WRITE

FMT_MTD.1 / CVCA_UPD Management of TSF Data
This SFR is fulfilled by F.EAC

FMT_MTD.1 / DATE Management of TSF Data
This SFR is fulfilled by F.EAC

FMT_MTD.1 / KEY_WRITE Management of TSF Data
This SFR is fulfilled by F.ACC_WRITE

FMT_MTD.1 / CAPK Management of TSF Data
This SFR is fulfilled by F.ACC_WRITE

FMT_MTD.1 / KEY_READ Management of TSF Data
This SFR is fulfilled by F.ACC_READ

FMT_MTD.3 Secure TSF Data
This SFR ensures that only values for the certificate chain are accepted. The SFR is fulfilled by F.EAC

FPT_EMSEC.1 / TOE Emanation
This SFR is fulfilled by

- F.ACC_WRITE that ensures the writing operations in EEPROM do not provoke any power leaks that may be use to reconstruct the information
- F.ACC_READ that ensures the reading operations in EEPROM do not provoke any power leaks that may be use to reconstruct the information
- F.BAC, F.EAC,F.AA,F.AUTH_PERSO, F.SM that ensures all the cryptographic operations are performed in a way that do not provoke any power leaks that may be use to reconstruct information about the key
- F.PHYS that protects the TOE from any physical attack

FPT_FLS.1 Failure with preservation of secure state
This SFR is fulfilled by F.ROLLBACK

FPT_TST.1 TSF Testing
This SFR is fulfilled by F.SELTESTS

FPT_PHP.3 Resistance to physical attack
This SFR is fulfilled by F.PHYS

FPT_RVM.1 Non By Passability of the TSF
This SFR is fulfilled by F.ACC_READ and F.ACC_WRITE

FPT_SEP.1 TSF Domain separation
This SFR is fulfilled by F.ACC_READ and F.ACC_WRITE that ensures that all the TSF data are separated.

8.2.2 *Link between the SFRs and the Security functions*

	Security functions of the TOE										Security functions of the IC								
	F.ACC_READ	F;ACC_WRITE	F.BAC	F.SM	F.AUTH_PERSO	F.AA	F.EAC	F.SELFTESTS	F.ROLLBACK	F.PHYS	F.RNG	F.HW_DES	F.HW_AES	F.OPC	F.PHY	F.LOG	F.COMP	F.MEM_ACC	F.SFR_ACC
FAU_SAS.1	x	x																	
FCS_CKM.1 / KDF_MRTD			x								x	X							
FCS_CKM.1 / DH_MRTD							X												
FCS_CKM.4 /MRTD			x	x			X												
FCS_COP.1 / RSA						x													
FCS_COP.1 / SHA_MRTD			x				X												
FCS_COP.1 / TDES_MRTD				x								X							
FCS_COP.1 / MAC_MRTD				x								X							
FCS_COP.1 / SIG_VER							X												
FCS_RND.1 / MRTD	x		x			x	X				X								
FIA_UID.1			x		x						X	X							
FIA_UAU.1			x		x						X	X							
FIA_API.1 / AA						x					x								
FIA_UAU.4 / MRTD			x		x		X				X	X							
FIA_UAU.5 / MRTD			x	x	x		X				x	X							
FIA_UAU.6 / MRTD				x								X							
FIA_AFL.1			x				X												
FIA_API.1 / CAP							x												
FDP_ACC.1	x	x																X	
FDP_ACF.1	x	x																X	
FDP_UCT.1 /MRTD				X								X							
FDP_UIT.1 /MRTD				X								X							

	Security functions of the TOE										Security functions of the IC								
	F.ACC_READ	F;ACC_WRITE	F.BAC	F.SM	F.AUTH_PERSO	F.AA	F.EAC	F.SELFTESTS	F.ROLLBACK	F.PHYS	F.RNG	F.HW_DES	F.HW_AES	F.OPC	F.PHY	F.LOG	F.COMP	F.MEM_ACC	F.SFR_ACC
FDP_ITC / AA		X																X	
FMT_MOF.1 / AA		x																X	
FMT_SMF.1		x																X	
FMT_SMR.1			x		x		X				X	x							
FMT_LIM.1	X							X		X					X				
FMT_LIM.2	x							X		X					X				
FMT_MTD.1 / INI_ENA		X																X	
FMT_MTD.1 / INI_DIS		X																X	
FMT_MTD.1 / CVCA_INI		X																X	
FMT_MTD.1 / CVCA_UPD		X																X	
FMT_MTD.1 / DATE		x																x	
FMT_MTD.1 / KEY_WRITE		X																X	
FMT_MTD.1 / CAPK		X																x	
FMT_MTD.1 / KEY_READ	X																	X	
FMT_MTD.3							x												
FPT_EMSEC.1	x	X	x	x	x	x	x			X				X	x				
FPT_TST.1								X											
FPT_RVM.1	x	x																X	
FPT_FLS.1									x					x					
FPT_PHP.3										x				X	X				
FPT_SEP.1	x	x																X	

Table 10 : Rationale of the security functions of the TOE vs the SFRs

8.2.3 Security functions dependencies

This section shows that the security functions are complete and internally consistent by showing that they are mutually supportive and provide and 'integrated effective whole' also with the IC, on which it is built

#	Security function	Dependencies	#
1	F.ACC_READ	F.MEM_ACC F.SELFTESTS F.PHYS	18 8 10
2	F.ACC_WRITE	F.MEM_ACC F;ROLLBACK F.SELFTESTS F.PHYS	18 9 8 10
3	F.BAC	F.RNG F.HW_DES F.COMP F.MEM_ACC F.SFR_ACC F.SELFTESTS F.PHYS	11 12 17 18 19 8 10
4	F.SM	F.HW_DES F.COMP F.MEM_ACC F.SFR_ACC F.PHYS	12 17 18 19 10
5	F.AUTH_PERSO	F.RNG F.HW_DES F.COMP F.MEM_ACC F.SFR_ACC F.SELFTESTS F.PHYS	11 12 17 18 19 8 10
6	F.AA	F.RNG F.COMP F.MEM_ACC F.SFR_ACC F.SELFTESTS F.PHYS	11 17 18 19 8 10
7	F.EAC	F.RNG F.COMP F.MEM_ACC F.SFR_ACC F.SELFTESTS F.PHYS	11 17 18 19 8 10
8	F.SELFTESTS	F.OPC F.PHYS	14 10
9	F.ROLLBACK	F.MEM_ACC	18
10	F.PHYS	F.PHY F.LOG F.OPC	15 16 14

Security functions of the IC			
11	F.RNG	N/A	N/A
12	F.HW_DES	N/A	N/A
13	F.HW_AES	N/A	N/A
14	F.OPC	N/A	N/A
15	F.PHY	N/A	N/A
16	F.LOG	N/A	N/A
17	F.COMP	N/A	N/A
18	F.MEM_ACC	N/A	N/A
19	F.SFR_ACC	N/A	N/A

Table 11 : Security functions dependencies

This section shows that the security functions are complete and internally consistent by showing that they are mutually supportive and provide and 'integrated effective whole' also with the IC, on which it is built

8.2.4 SOF level rationale

The strength level for the TOE security functions is SOF-high. According to [CC2] section 424, the strength of cryptographic algorithms is outside the scope of the Common Criteria evaluation.

"Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function)"

The following security functions do not use probabilistic nor permutational mechanism:

- F.ACC_READ
- F.ACC_WRITE
- F.SM
- F.AUTH_PERSO
- F.ROLLBACK
- F.PHYS

The following security functions do use probalistic or permutational mechanism but for non security features

- F.SELFTESTS - uses a permutational mechanism (for the self tests of the SHA-1)
- F.ACC_READ - uses a probabilistic mechanism to generate a random UID at each reset.

The strength of the other security function is SOF-high:

- F.BAC uses a probabilistic mechanism to perform a mutual authentication (BAC) and a permutational mechanism to get the session keys used for the secure messaging (SHA-1 computation)
- F.AA uses a probabilistic mechanism to compute the signature (for the padding) and a permutational mechanism to prepare the data to sign.
- F.EAC uses

- a probabilistic mechanism to perform an external authentication (Terminal authentication step)
- a permutational mechanism to generate the session keys used for the secure messaging (SHA-1 computation) after the chip authentication
- a permutational mechanism for the terminal authentication step (SHA-1/SHA-224/SHA-2/SHA-384)

The SOF-high for these security functions is achieved with the combination of the relevant SFR.

8.2.5 Rationale for Strength of Function High

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the security objectives stated in the protection profile. The protection against attacks with a high attack potential dictates a strength of function high rating for functions in the TOE that are realized by probabilistic or permutational mechanisms.

8.3 Security Objective rationale of the TOE

8.3.1 Standard "Extended Access Control" features

The rationale is identical to the one indicated in [R10]

8.3.2 Addition for the"Active Authentication" feature

	OT.Chip_authenticity	OE.AA_Personalization
T.Chip-ID		
T.Skimming		
T.Read_Sensitive_Data		
T.Forgery		
T.Counterfeit	x	
T.Abuse-Func		
T.Information_Leakage		
T.Phys-tamper		
T.Malfunction		
P.Manufact		
P.Personalization		
P.Personal_Data		

P.Sensitive_Data		
A.Pers_Agent		x
A.Insp_Sys		
A.Signature_PKI		
A.Auth_PKI		

The assumption **A.Pers_Agent** "Personalization of the MRTD's chip" is covered by the security objective for the TOE environment **OE.AA_Personalization** "Active Authentication Personalization" including the enrolment, the protection with digital signature and the storage of the MRTD holder active authentication data (DG15) and the enabling of this security features of the TOE according to the decision of the Issuing State or Organization concerning the Basic Access Control.

The threat **T.Counterfeit** "MRTD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by active authentication proving the authenticity of the chip as required by **OT.Chip_Authenticity** "Protection against forgery" using a authentication key pair to be generated by the issuing State or Organization. The Public active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.AA_Key_MRTD** "Active Authentication Key". MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs targeted on by OD.Material.

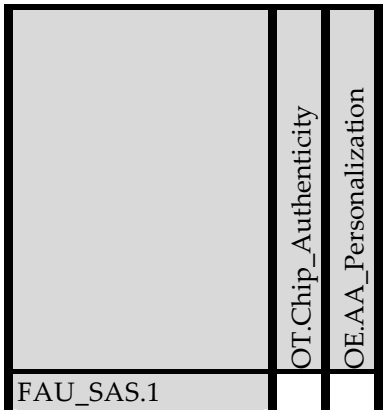
8.4 Security functionnal requirments rationale of the TOE

8.4.1 Standard "Extended Access Control" features

The security functional requirments rationale, as well as their justifications are identical to the ones indicated in [R10]

8.4.2 Addition for the"Active Authentication" feature

The rational binding the SFRs and the TOE objective is described hereafter :



	OT.Chip_Authenticity	OE.AA_Personalization
FCS_CKM.1 / KDF_MRTD		
FCS_CKM.1 / DH_MRTD		
FCS_CKM.4 /MRTD		
FCS_COP.1 / RSA	X	
FCS_COP.1 / SHA_MRTD	X	
FCS_COP.1 / TDES_MRTD		
FCS_COP.1 / MAC_MRTD		
FCS_COP.1 / SIG_VER		
FCS_RND.1 / MRTD	X	
FIA_UID.1		
FIA_UAU.1		
FIA_API.1 / AA	x	
FIA_UAU.4 / MRTD		
FIA_UAU.5 / MRTD		
FIA_UAU.6 / MRTD		
FIA_AFL.1		
FIA_API.1 / CAP		
FDP_ACC.1	x	
FDP_ACF.1	x	
FDP_UCT.1 /MRTD		
FDP_UIT.1 /MRTD		
FDP_ITC / AA	x	
FMT_MOF.1 / AA		x
FMT_SMF.1		
FMT_SMR.1		
FMT_LIM.1		
FMT_LIM.2		
FMT_MTD.1 /		

	OT.Chip_Authenticity	OE.AA_Personalization
INI_ENA		
FMT_MTD.1 / INI_DIS		
FMT_MTD.1 / CVCA_INI		
FMT_MTD.1 / CVCA_UPD		
FMT_MTD.1 / DATE		
FMT_MTD.1 / KEY_WRITE	x	
FMT_MTD.1 / CAPK		
FMT_MTD.1 / KEY_READ	x	
FMT_MTD.3		
FPT_EMSEC.1		
FPT_TST.1		
FPT_RVM.1		
FPT_FLS.1		
FPT_PHP.3		
FPT_SEP.1		

The security objective **OT.Chip_Authenticity** "Protection against forgery" is ensured by the Active Authentication Protocol provided by **FIA_API.1/AA, FDP_ACC.1** and **FDP_ACF.1** proving the identity and authenticity of the TOE. The Active Authentication relies on **FCS_COP.1/RSA**, **FCS_COP.1/ SHA_MRTD** and **FCS_RND.1/MRTD**. It is performed using a TOE internally stored confidential private key as required by **FMT_MTD.1/KEY_WRITE** and **FMT_MTD.1/KEY_READ**, this key being loaded during personalization phase as required by **FDP_ITC/AA**.

The security objective **OE.AA_Personalization** "Active Authentication Personalization" is covered by **FMT_MOF.1/AA**.

8.5 Security functionnal requirments rationale of the IT environment

8.5.1 Standard "Extended Access Control" features

The security functional requirments rationale, as well as their justifications are identical to the ones indicated in [R10]

8.5.2 Addition for the"Active Authentication" feature

The rational binding the SFRs and the TOE objective is described hereafter :

	OE.AA_Key_MRTD
Document Signer	
FDP_DAU.1/DS	x
Personalization Agent	
FCS_CKM.1/PERSO	x
Active Authentication terminal	
FCS_RND.1/AA	x
FCS_COP.1/RSA_AA	x

The **OE.AA_Key_MRTD** "Active Authentication Key" is covered by **FDP_DAU.1/DS** which requires the Document Signer to provide a capability to generate evidence for the validity and authenticity of active authentication public key in DG 15. **FCS_CKM.1/PERSO** covers the key generation required by a personalization agent in charge of issuing MRTD chips. The Active authentication control is covered by **FCS_RND.1/AA** and **FCS_COP.1/RSA_AA**.

8.6 Security Assurance requirements rationale

A security assurance requirments rationale for the EAL4+ level is provided in [R10]. Moreover, as the underlying IC is certified according to [R2] with level EAL5+, the compositon is straight forward.

9 ACRONYMS

AA	Active Authentication
BAC	Basic Access Control
CA	Chip authentication
CC	Common Criteria Version 2.3
CPLC	Card personalization life cycle
CVCA	Country Verifying Certification Authority
DF	Dedicated File
DFA	Differential Fault Analysis
DG	Data Group
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic curve cryptography
ECDH	Elliptic curve Diffie Hellmann
ECDSA	Elliptic curve Digital signature Algorithm
EF	Elementary File
EFID	File Identifier
DES	Digital encryption standard
DH	Diffie Hellmann
I/0	Input/Output
IC	Integrated Circuit
ICAO	International Civil Aviation organization
ICC	Integrated Circuit Card
IFD	Interface device
LDS	Logical Data structure
MF	Master File
MRTD	Machine readable Travel Document
MRZ	Machine readable Zone
MSK	Manufacturer Secret Key
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
SFI	Short File identifier
SHA	Secure hashing Algorithm
SOD	Security object Data
SOF	Strength of Function
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE Security function