ID ONE™ EPASS V2.1
WITH BAC CONFIGURATION

PUBLIC SECURITY TARGET

ISSUE: 1

Verification and approval

Function	Name	Visa
Author / Security Certification Project manager	CAPEL Clément	Approbation de FQR 110 4641 Ed1 par CAPEL Clément le 30-6-2009.oft

Table of contents

FQR : 110 4641	Édition : 1	Date : 30/06/2009		2/77

FQR : 110 4641	Édition : 1	Date : 30/06/2009		3/77

List of figures

FQR : 110 4641	Édition : 1	Date : 30/06/2009		4/77

List of tables

1 Security Target identification

1.1 Identification

General identification:

Title:	ID One™ ePass v2.1 with BAC configuration
Editor:	Oberthur Technologies
CC version:	3.1 revision 2
EAL:	EAL4+

TOE technical identification[1]:

Name:	ePass v2.1 on NXP P5CDXXX
Microcontroller[2]:	P5CD040V0B, P5CD080V0B and P5CD144V0B of NXP[3]
ROM:	069591
Optional code:	070942

1.2 Target of evaluation

The TOE is a Machine readable travel document implementing the Basic Access control as defined in [R1] and [R2].

---

[1] Some TOE identification data are stored in a file located in the chip EEPROM memory (see 3.2).
[2] The software is embedded on these three chips. Nevertheless, this not impacts the security target which remains the same.
[3] These chips are certified at EAL5+ according to the BSI-0002 Protection Profile.

2 Conformance claims

2.1 Common Criteria conformance

This Security Target (ST) is CC Part 2 extended [R31] and CC Part 3 conformant [R32] and written according to the Common Criteria version 3.1 Part 1[R30].

2.2 Package conformance

This ST is conformant to the EAL4 package as defined in [R32].

The EAL4 have been augmented with the following requirements to fulfill the smartcards standard assurance level**:**

Requirement	Name	Type
ALC_DVS.2	Sufficiency of security measures	Higher hierarchical component

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 enhanced basic attack potential (AVA_VAN.3)[4].

2.3 Protection Profile conformance

The Security Target is conformant to the following PP written in CC2.3:
- Machine readable travel documents with "ICAO Application", Basic Access control [R7]

Remark:

Since this PP is not yet available in CC 3.1, requirements have been translated from CC2.1 to CC3.1 revision 2.

---

[4] AVA_VLA.2 of CC2.3 has been translated to AVA_VAN.3 in CC3.1r2. Therefore "low attack potential" has been translated to "enhanced basic attack potential".

FQR : 110 4641	*Édition : 1*	*Date : 30/06/2009*		*7/77*

3   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 overview
- TOE on-chip identification
- TOE logical structure
- TOE life-cycle,
- Limits of the TOE
- TOE environment
- TOE scope

3.1   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 [7].
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, integration of the IC with the booklet and antenna is out of the evaluation scope (see [R9]).
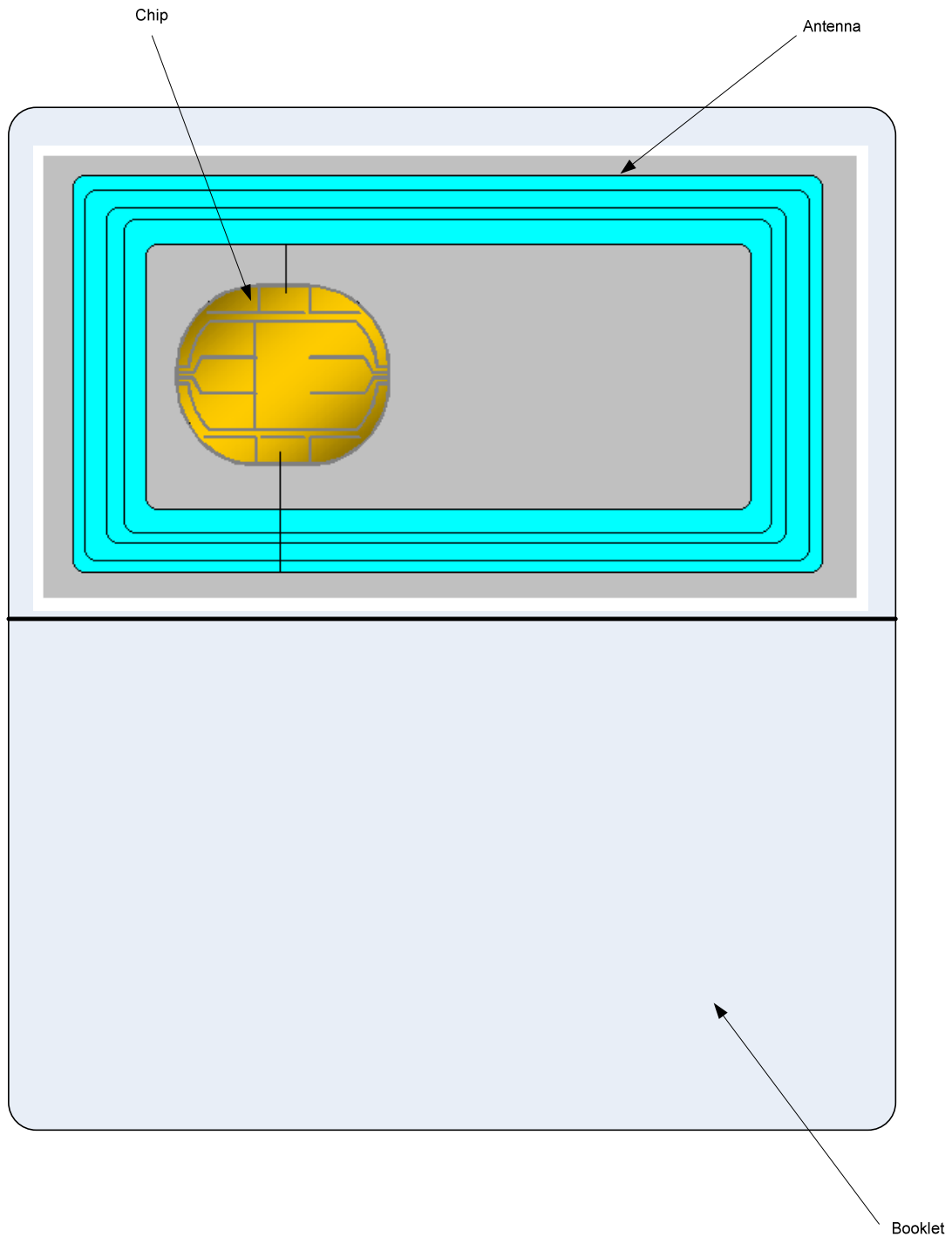
Figure 1 : Physical TOE overview

3.2 TOE on-chip Identification

At any time TOE can be identified by reading the CPLC data stored in ROM as specified in the AGD_PRE document.

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 = 069591
- OptionalCodeIdentifier = 070942

PPIdentifier and CertificateIdentifier are set according to the AGD_PRE document.

3.3 TOE usage and security features for operational use

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, personalisation 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 [R1] & [R2] 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 [R1]) 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 or ECC 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 or ECC Key pair.

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)

3.4 TOE logical structure

The TOE contains an application embedded in the chip. This application fulfils the requirements described beforehand and in [R1], [R2].
This application is made of:
- A file system compliant with [R13]
- 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 files are selected, the file structure it contains may be accessed, provided the access conditions are fulfilled.

Structure of the File system

```
┌─────────────────────────────────────────────────────┐
│                                                       │
│    ┌──────────────┐                                   │
│    │              │          Application              │
│    │ Master File  │                                   │
│    │              │                                   │
│    └──────┬───────┘                                   │
│           │              ┌──────────────────┐         │
│           │              │                  │         │
│    ┌──────┴───────┐      │ Other data       │         │
│    │              │      │ structure        │         │
│    │ Dedicated    │      │                  │         │
│    │ File LDS     │      └──────────────────┘         │
│    └──────┬───────┘                                   │
│           │        ┌──────────────────┐               │
│           ├────────│ Elementary File 1│               │
│           │        └──────────────────┘               │
│           │        ┌──────────────────┐               │
│           ├────────│ Elementary File 2│               │
│           │        └──────────────────┘               │
│           │        ┌──────────────────┐               │
│           ├────────│ Elementary File 3│               │
│           │        └─────────┬────────┘               │
│           │        ┌─────────┴────────┐               │
│           └────────│ Elementary File n│               │
│                    └──────────────────┘               │
│                                                       │
└─────────────────────────────────────────────────────┘
```
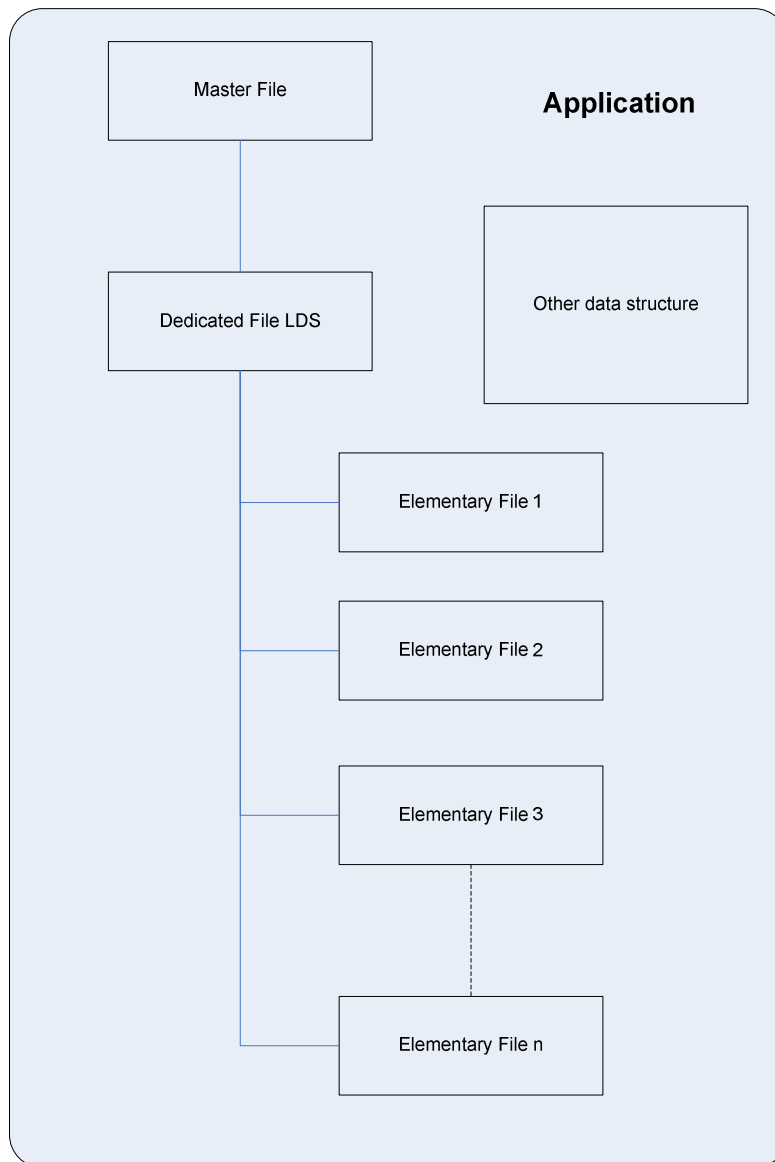
Figure 2 : Structure of the File system

3.4.1   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 describe below:
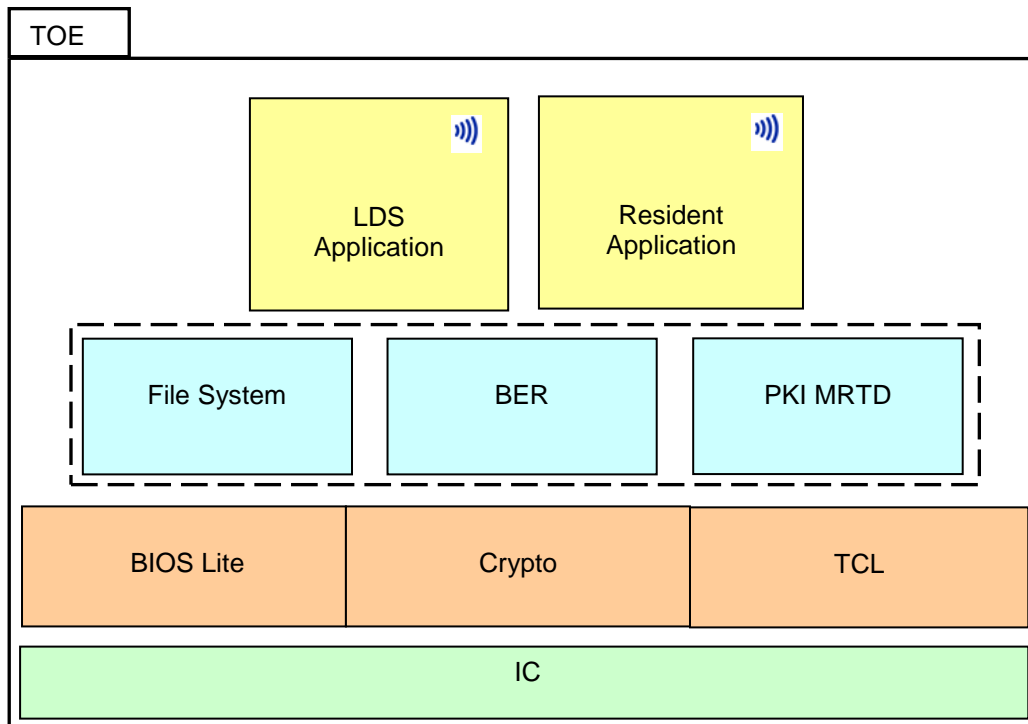
This layer is permeable. This means that upper layers can also directly access to lower layer for a defined set of services.

Figure 3 : Logical structure of the TOE

- **LDS application***:* This "application" fulfils the following functionalities*:*
    - o Implements the commands of e-passport that are available in operational phase
    - o Manages access control on these commands
    - o Implements authentication mechanisms:
        - ▪ Basic Access Control (BAC), including session keys generation ,
        - ▪ Active Authentication (AA),

- **Resident application:** This "application" fulfils the following functionalities,
    - o Implements the commands of e-passport that are available in pre-personalisation and personalisation phases,
    - o Manages access control on these commands.

- **API layer (blue):** This layer provide generic APIs used by applications,
    - o **File System** implements the secure management of application data for the applications,
    - o **BER** provides a toolbox to manage APDU format,
    - o **PKI MRTD** Implements generic functions for Activation Authentication and Secure Messaging of incoming and outgoing commands.

- **Low level layer (orange):** This layer provides an interface between the Hardware and upper layer.

FQR : 110 4641	Édition : 1	Date : 30/06/2009		15/77

- o **BIOS Lite** performs access to memory (read & write) – EEPROM - and other basic manipulation of the hardware,
- o **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)
- o **TCL** handles the communication interface (i.e. conctaless interface).

- **IC layer:** it corresponds to the chip features.

3.5 TOE life cycle according to the PP 9911

The Smart card life-cycle considered hereby, is the one described in [R28]. 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:

FQR : 110 4641	*Édition : 1*	*Date : 30/06/2009*	**16/77**
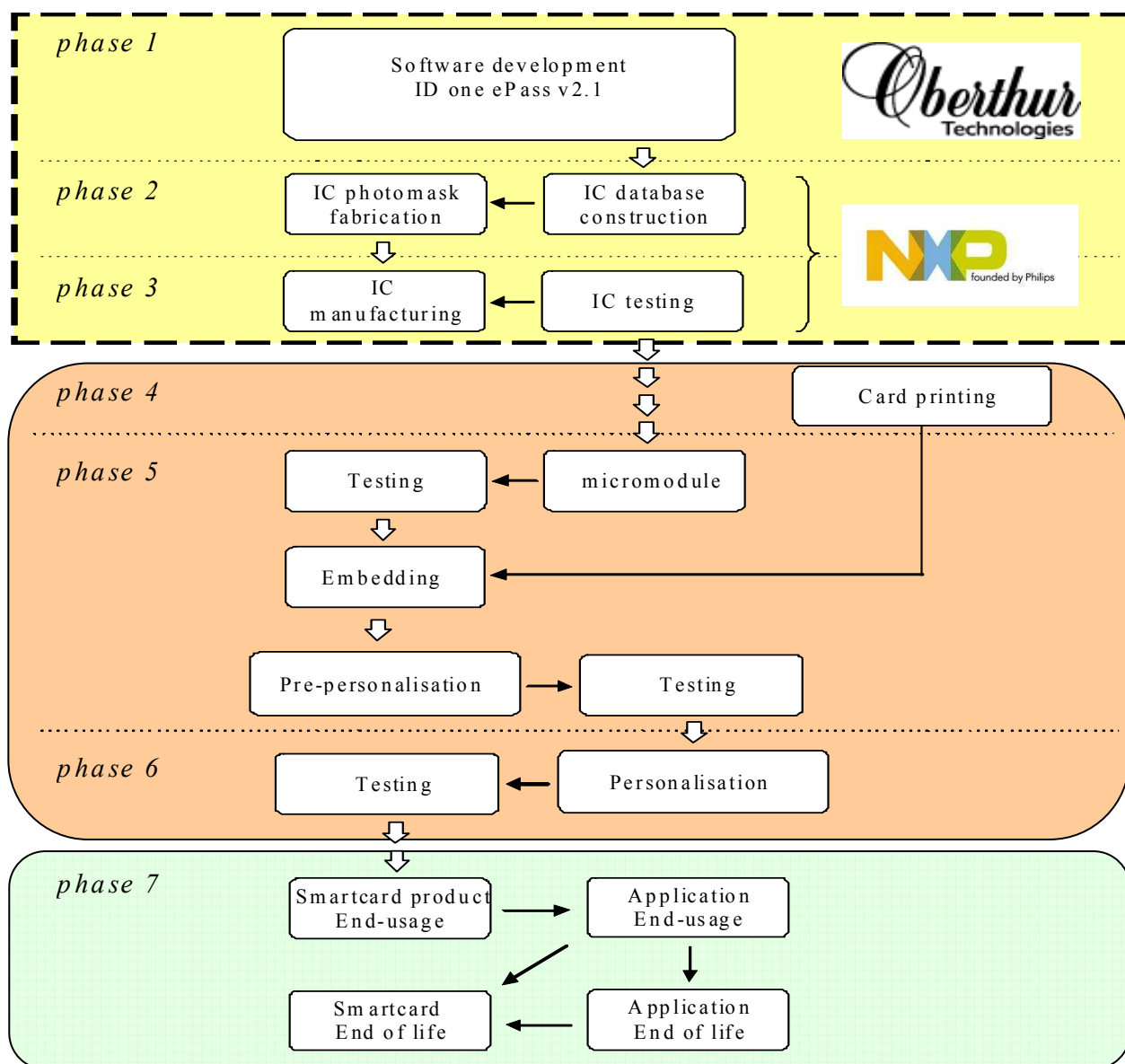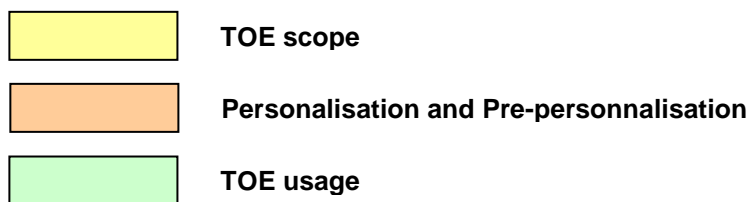
Figure 4 *Smartcard product life-cycle for the TOE*

3.6 Description of the TOE environment

The TOE environment may be spitted 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 [R7] and [R6].
- The **production environment** in which the TOE is tested and manufactured. The security requirements that are applied reach the one described in [R7] and [R6].
- The **User environment**, in which the TOE is used as stated in [R7] and [R6]. The security requirements that are requested and the assurance levels are met.

3.6.1 Development environment

3.6.1.1 Software development (phase 1)

This environment is enforced by OBERTHUR TECHNOLOGIES.
To ensure security, access to development tools and products elements (PC, emulator, card reader, documentation, source code...) 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 development data through the use of a secure computer system to design, implement and test software

3.6.1.2 Hardware development (Phase 2)

The environment is enforce by NXP site
The IC development environment is described in [R10], [R11] and [R12].
The ICs are certified EAL5+ and the IC certificate reference are:
- BSI-DSZ-CC0404-2007 for the NXP P5CD0040V0B
- BSI-DSZ-CC0417-2008 for the NXP P5CD0080V0B
- BSI-DSZ-CC0411-2007 for the NXP P5CD0144V0B

3.6.2 Production environment

3.6.2.1 IC manufacturing (phase 3)

The environment is equivalent to the one of the phase 2.
Depending on the choice made for the optional code loading, the optional code may be loaded during this phase.

3.6.2.2 *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-personalisation and personalisation 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 Personalisation Agent.
- Preparing the TOE prior to delivering it to the Personalisation 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 optional; it may be performed by **OBERTHUR TECHNOLOGIES**
- Loading the authentication key of the personalisation Agent.
- Preparing the TOE prior to delivering it to the Personalisation Agent (phase 6)

The **OBERTHUR TECHNOLOGIES** manufacturing sites have all the needed certifications.
The same level of security will be required for the contractor's site.

*Remark***:**

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 personalisation keys

Therefore, the phase 5, when an optional code is loaded may be covered by AGD_PRE.
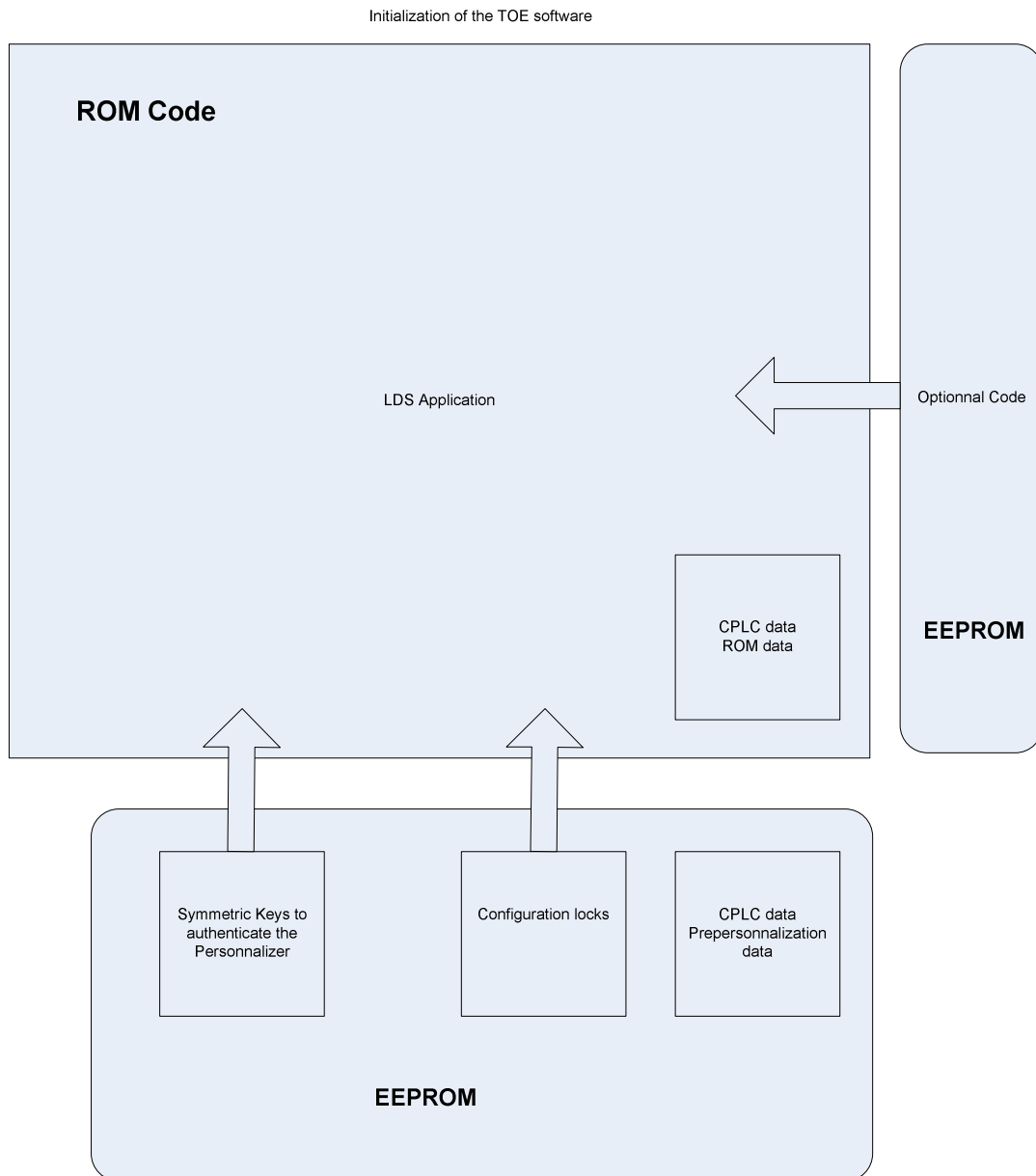
Figure 5 : Initialization of the TOE software

3.7 Summary of the production environment

In this chapter, the TOE life cycle envisioned is the one of PP 9911 ([R28])

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 pre-personalisation of the TOE is performed as described in §3.6.2.2

FQR : 110 4641	Édition : 1	Date : 30/06/2009		20/77

- 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 or OBERTHUR TECHNOLOGIES)	IC packaging	OBERTHUR TECHNOLOGIES manufacturing site
5	Set up of the TOE		Optional code loading Set up of the TOE	
6	Personalisation of the MRTD (While the TOE is under the Personalisation Agent's operation)	Production environment of the customer	Personalisation of the MRTD (While the TOE is under the Personalisation 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	Personalisation of the MRTD (While the TOE is under the Personalisation Agent's operation)	Production environment of the customer
7	Operational Use	

Table 2 : Production environments of the TOE – case 3

3.7.1   User environment

3.7.1.1   TOE Personalisation and testing (phase 6)

At the end of the phase 5, the card manufacturer delivers the TOE to the personaliser of the MRTD device.

The TOE delivered to the personalizer has the following features:
- The personalizer 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 personaliser that receives the TOE to perform the following steps:

The personalisation 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) – BAC keys, Active authentication keys (if activated)
- Optionally generating the key for Active Authentication if not loaded
- Loading the counter limit for the BAC authentication
- Updating the CPLC data to fill the personalisation 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 personalisation agent finished the electrical personalisation, it TOE is switched into personalized phase. This transition is irreversible.

3.7.1.2 TOE Operationnal Use (phase 7)

The TOE is delivered to the holder of the passport. The TOE behaves as described in [R1], [R2] and [R4].

3.8 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 [R10], [R11] and [R12] addresses the security requirements for phases 2 and 3 for the same objective.

***Remark*:**
   According to [R9] the phase 4 related to the embedding of the chip in a booklet and the connection of the antenna has been removed from the TOE scope.

3.9 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 [R28]

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 : Personalisation of the MRTD (While the TOE is under the Personalisation Agent's operation)
7	Phase 4 :Operational Use

Table 3 : Mapping of life cycle states

For more details about this mapping, see [R29].

4   TOE Security Environment

4.1   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, the data groups DG1 to DG16 and the Document security object according to LDS [R3]. These data are user data of the TOE. The data groups DG1 to DG14 and DG 16 contain personal data of the MRTD holder.
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 the TOE can not be erased
- Ensure no tearing can arises
- The configuration chosen (BAC, AA, Get Data 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, the BAC protocol is protected by a counter error, increased at each wrong consecutive authentication. When the limit is exceeded, the TOE performs the authentication within a period of time constantly increasing. This counter is 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.DGx – except EF.DG15)	Contains identification data of the holder
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

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

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.

4.2 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 [R3].
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 **Primary Inspection System (PIS)** (i) contains a terminal for the contact less communication with the MRTD's chip and (ii) does not implement the terminals part of the Basic Access Control Mechanism. The Primary Inspection System can read the logical MRTD only if the Basic Access Control is disabled. 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 **Extended Inspection System (EIS)** in addition to the Basic Inspection System (i) implements the Active Authentication Mechanism, (ii) supports the terminals part of the Extended Access Control Authentication Mechanism and

	(iii) is authorized by the issuing State or Organization to read the optional biometric reference data.
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 4 on Inspection system
This security target does distinguish between the **BIS** and **EIS** because the Active Authentication is in the scope.

Application note 5 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.

4.3 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 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 Primary Inspection System for global interoperability contains the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization [R1].

The Primary Inspection System performs the Passive Authentication to verify the logical MRTD if the logical MRTD is not protected by Basic Access Control. The Basic Inspection System in addition to the Primary Inspection System implements the terminal part of the Basic Access Control and reads the logical MRTD being under Basic access Control.

Application note 6: According to [R1] the support of
- (i) the Passive Authentication mechanism is mandatory, and
- (ii) the Basic Access Control is optional. In the context of this security target the Primary Inspection System does not implement the terminal part of the Basic Access Control. It is therefore not able to read the logical MRTD if the logical MRTD is protected by Basic Access Control.

The TOE allows the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems
The Active authentication is also optional and can be enabled or disabled by the Personalization agent.

4.4 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 digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by 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 (DG1), the printed portrait and the digitized portrait (DG2), the biometric reference data of finger(s) (DG3), the biometric reference data of iris image(s) (DG4) and data according to LDS (DG5 to DG14, DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [R1].

The issuing State or Organization decides

- (i) to enable the Basic Access Control for the protection of the MRTD holder personal data or
- (ii) to disable the Basic Access Control to allow Primary Inspection Systems of the receiving States and all other terminals to read the logical MRTD.

Application note 7:

The organisational security policy **P.Personal_Data** is drawn from the ICAO Technical Report [R1]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

4.5 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.

4.6 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.Eavesdropping	Eavesdropping to the communication between TOE and inspection system

An attacker is listening to the communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know this data in advance. Note in case of T.Skimming the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data printed on the MRTD data page and without a help of the inspection system which knows these data. In case of T.Eavesdropping the attacker uses the communication of the inspection system.

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 digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker write the digitized 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 contactless chip.

T.Counterfeit MRTD's chip

An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a 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.

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

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 functionalities of the MRTD's chip Embedded Software,
- (iii)   to modify User Data or
- (iv)   (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 functionalities 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.

5 Security Objectives

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

5.1 Security Objectives for the TOE

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

OT.AC_Pers	Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data groups DG1 to DG16, the Document security object according to LDS [R3] 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 8:
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. If the TOE is configured for the use with Basic Inspection Terminals only the TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

OT.Data_Conf	Confidentiality of personal data

If the TOE is configured for the use with Basic Inspection Systems the TOE must ensure the confidentiality of the logical MRTD data groups DG1 to DG16 by granting read access to terminals successfully authenticated by
   (i) as Personalization Agent or as
   (ii) **Basic Inspection System**. The **Basic Inspection System** shall authenticate themselves by means of the Basic Access Control based on knowledge of the Document Basic Access Key.
The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System. If the TOE is configured for the use with **Primary Inspection Systems** no protection in confidentiality of the logical MRTD is required.

Application note 9:
The traveller grants the authorization for reading the personal data in DG1 to DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective **OT.Data_Conf** requires the TOE to ensure the strength of the security functionality Basic Access Control Authentication independent on the quality of the Document Basic Access Keys that 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 [R1] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective **OT.Data_Conf**.

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 10:
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 tractability 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. If the TOE allows a Primary Inspection System (i.e. Every terminal) to read these data every terminal may identify the TOE. If the TOE is configured to allow a Basic Inspection System only to read these data the **OT.Identification** forbids the output of any other IC (e.g. integrated circuit serial number ICCSN) or a MRTD identifier through the contact less interface before successful authentication as Basic Inspection System or as Personalization Agent.

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 11:
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

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

with a prior

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

Application note 12:
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 13:
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 or ECC private key to prove its identity, and that is used in chip authentication. This mechanism is described in [R1] as "Active Authentication".

5.2 Security Objectives for the environment

5.2.1 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 functionality 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.

5.2.2 Security Objectives for the Operational Environment

Issuing State or Organization

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

OE.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) enrol 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).

The Personalization Agents enable or disable the Basic Access Control function of the TOE according to the decision of the issuing State or Organization. If the Basic Access Control function is enabled the Personalization Agents generate the Document Basic Access Keys and store them in the MRTD's chip.

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 includes all data in the data groups DG1 to DG16 if stored in the LDS according to [R3].

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 ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems that implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems). The receiving State examining the logical MRTD with Primary Inspection Systems will prevent eavesdropping to the communication between TOE and inspection system.

Application note 14:
The Primary Inspection System may prevent unauthorized listening to or manipulation of the communication with the MRTD's chip e.g. by a Faraday cage.

MRTD Holder

OE.Secure_Handling   Secure handling of the MRTD by MRTD holder

The holder of a MRTD configured for use with Primary Inspection Systems (i.e. MTRD with disabled Basic Access Control) will prevent unauthorized communication of the MRTD's chip with terminals through the contact less interface.

Application note 15:
The MRTD holder may prevent unauthorized communication of the MRTD's chip with terminals e.g. by carrying the MRTD in a metal box working as Faraday cage.

6　Security requirements

6.1　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 **FIA_API**
- Family **FMT_LIM**
- Family **FPT_EMSEC**

Definition of these families and related requirements is provided in the Protection Profile [R7].

6.2　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.

6.2.1　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 18:
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**.

6.2.2　Class FCS Cryptographic Support

6.2.2.1 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: *[[R1], normative appendix 5]*.

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 19:
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 [R1], Annex E.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [R1], Annex E.1. The algorithm uses the random number RND.ICC generated by TSF as required by **FCS_RND.1/MRTD**.

FCS_CKM.1/ASYM Cryptographic key generation – Assymetric keys for AA

FCS_CKM.1.1/ The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[for RSA and ECC]* and specified cryptographic key sizes *[*
- 1024, 1536 and 2048 for RSA,
- 192bits, 224bits, 256 bits, 384 bits and 512 bits over characteristic p curves for ECC
] that meet the following: *[R23], [R24], [R25], [R26]*.

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

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]*.

FQR : 110 4641	*Édition : 1*	*Date : 30/06/2009*		**41/77**

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 20:
The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys
for secure messaging.

6.2.2.2   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/SIG_MRTD Cryptographic operation – signature by MRTD

The TSF shall perform *[digital signature creation]* in accordance with a specified cryptographic
algorithm *[RSA CRT or ECDSA with SHA1, SHA-224, SHA-256 or SHA-384]* and cryptographic key
sizes *[*
- 1024, 1536 and 2048 bits for RSA CRT,
- 192, 256 384 and 512 bits for ECDSA,
] that meet the following: *[*
- scheme 1 of ISO/IEC 9796-2:2002 for RSA CRT,
- [R15], [R16], [R14] for ECC,
].

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, 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

FQR : 110 4641	Édition : 1	Date : 30/06/2009		42/77

FMT_MSA.2 Secure security attributes

Application note 21:
This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also **FIA_UAU.4/BAC_MRTD**) according to [7].

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 [R19] and [R5]; 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 22:
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 the Basic Access Control Authentication Mechanism according to the **FCS_CKM.1/BAC_MRTD** and **FIA_UAU.4/BAC_BT**. 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 23:
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 according to the **FCS_CKM.1/BAC_MRTD** and **FIA_UAU.4/BAC_MRTD**.

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 [R27]].*

Dependencies: No dependencies.

Application note 24:
This SFR requires the TOE to generate random numbers used for the authentication protocols as required by **FIA_UAU.4/MRTD**.

6.2.3   Class FIA Identification and Authentication

Application note 25:
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 [R1], Annex E
Basic Access Control Authentication Mechanism	**FIA_UAU.4/MRTD** and **FIA_UAU.6/MRTD**	**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, 1536, 2048 bits and ECC with 192, 256, 384, 512 bits according to [R1], Annex D.

Table 1: Overview on authentication SFR

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow
    (1) to read the Initialisation Data in Phase 2 "Manufacturing",
    (2) to read the ATS in Phase 3 "Personalization of the MRTD",
    (3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 "Operational Use",

---

> **(4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 "Operational Use"**
> on behalf of the user to be performed before the user is identified.
>
> FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

Application note 26:
The IC manufacturer and the MRTD manufacturer write the Initialisation Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 "Manufacturing". The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. 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 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. If the TOE is configured for use with Primary Inspection System s any terminal is assumed as Primary Inspection System and is allowed to read the logical MRTD. If the TOE is configured for use with Basic Inspection Systems only 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 according to the **SFR FIA_UAU.4/T**.

Application note 27:
In the operation phase the MRTD must not allow anybody to read the ICCSN or any other unique identification before the user is authenticated as Basic Inspection System (cf. **T.Chip_ID**). Note that the terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal for communication with more than one RFID. 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

> **FIA_UAU.1 Timing of authentication**
>
> FIA_UAU.1.1 The TSF shall allow
> **(1) to read the Initialisation Data in Phase 2 "Manufacturing",**
> **(2) to read the ATS in Phase 3 "Personalization of the MRTD",**
> **(3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 "Operational Use",**
> **(4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 "Operational Use"**
>
> On behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification.

Application note 28:
The **Primary Inspection System** does not authenticate themselves. Only the **Basic Inspection System** and the Personalization Agent authenticate themselves.

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,

Dependencies: No dependencies.

Application note 29:
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 uses RND.ICC [R1], and the Authentication Mechanism based on Triple-DES shall use a Challenge as well.

Application note 30:
The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [R1]. 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 this second step the MRTD's chip provides the terminal with a challenge-response-pair that allows 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

---

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
(a) the Basic Access Control Authentication Mechanism with the Personalization Agent Keys,
(b) the Symmetric Authentication Mechanism with the Personalization Agent Key

2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

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

Dependencies: No dependencies.

Application note 31:
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 [R1], or
   (ii)   a Triple-DES key for the Symmetric Authentication Mechanism.
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 may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Note, the successful authenticated Personalization Agent may disable the Basic Access Control 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

Dependencies: No dependencies.

Application note 32:
The Basic Access Control Mechanism specified in [R1] includes the 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-

authenticate the user for each received command and accept only those commands received from the initially authenticated by means of BAC user.

6.2.4   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). The instantiations of FDP_ACC.1 are caused by the TSF management according to FMT_MOF.1.

FDP_ACC.1 Subset access control – Primary Access Control FDP_ACC.1.1/PRIM The TSF shall enforce the *[Primary 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 33:
The data groups DG1 to DG16 of the logical MRTD as defined in [R1]are the only TOE User data. The Primary Access Control SFP addresses the TOE usage with Primary Inspection Systems and Basic Inspection Systems independent on the configuration of the TOE.

FDP_ACC.1 Subset access control – Basic Access control FDP_ACC.1.1/BASIC The TSF shall enforce *[the Basic 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 34:
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). The instantiations of FDP_ACC.1 address different SFP.

FDP_ACF.1/Security attribute based access control – Primary Access Control FDP_ACF.1.1/PRIM The TSF shall enforce *[the Primary Access Control SFP]* to objects based on the following: *1. Subjects:*

FQR : 110 4641	Édition : 1	Date : 30/06/2009		48/77

a. Personalization Agent,
b. Terminals,
2. Objects: data in the data groups DG1 to DG16 of the logical MRTD, and Active Authentication Private Key
3. Security attributes
a. Configuration of the TOE according to FMT_MOF.1,
b. Authentication status of terminals.

FDP_ACF.1.2/PRIM
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: i*n the TOE configuration for use with Primary Inspection Systems*
1. The successfully authenticated Personalization Agent is allowed to write the data of the data groups DG1 to DG16 of the logical MRTD, including the Active Authenticate Public Key
2. The Terminals are allowed to read the data of the groups DG1 to DG16 of the logical MRTD, including the Active Authenticate Public Key.

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

FDP_ACF.1.4/PRIM
The TSF shall explicitly deny access of subjects to objects based on the rule: *the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD*.

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

Application note 35:
The MRTD access control prevents changes of data groups by write access to the logical MRTD after their creation by the Personalization Agent (i.e. no update of successful written data in the data groups DG1 to DG16). The Passive Authentication Mechanism detects any unauthorised changes.

FDP_ACF.1/Basic Security attribute based access control – Basic Access Control

FDP_ACF.1.1/BASIC The TSF shall enforce the *[the Basic Access Control SFP]* to objects based on the following:
1. Subjects:
a. Personalization Agent,
b. Basic Inspection System,
c. Terminal,
2. Objects: data in the data groups DG1 to DG16 of the logical MRTD and Active Authentication Private Key
3. Security attributes
a. Configuration of the TOE according to FMT_MOF.1,
b. Authentication status of terminals.

FDP_ACF.1.2/BASIC The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *in the TOE configuration for use with Basic Inspection Systems only*
 1.The successfully authenticated Personalization Agent is allowed to write and to read the data of the data groups DG1 to DG16 of the logical MRTD, including the Active Authenticate Public Key
 2.The successfully authenticated Basic Inspection System is allowed to read data of the groups DG1 to DG16 of the logical MRT,D including the Active Authenticate Public Key.

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

FDP_ACF.1.4/BASIC The TSF shall explicitly deny access of subjects to objects based on the rule: *the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD*.

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

Inter-TSF-Transfer

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

Application note 36:
FDP_UCT.1/MRTD and **FDP_UIT.1/MRTD** require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

FDP_UCT.1.1/MRTD The TSF shall enforce the *[Basic Access Control SFP]* to be able to *[transmit and receive]* user data in a manner protected from unauthorised disclosure.

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 *[Basic Access Control SFP]* to be able to *[transmit and receive]* user data in a manner protected from *[modification, deletion, insertion and replay]* errors.

FQR : 110 4641	Édition : 1	Date : 30/06/2009		50/77

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.

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 or ECC 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 *[Primary Access Control SFP or Basic 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

6.2.5   Class FMT Security Management

FMT_MOF.1 Management of functions in TSF
.
FMT_MOF.1.1 The TSF shall restrict the ability to *[enable and disable]* the functions *[TSF Basic Access Control]* to *[Personalization Agent]*.

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

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

Application note 37:
The enabling and disabling the TSF Basic Access Control defines the configuration of the TOE in Phase 3 "Personalization of the MRTD" before use in the phase 4 "Operational Use":
  1. The TOE is configured with Primary Inspection systems when the TSF Basic Access Control is disabled. In this configuration the TOE enforces the Primary Access Control SFP according to

---

FDP_ACC.1/PRIM and **FDP_ACF.1/PRIM**. In this case the logical MRTD may be read without successful authentication as **Basic Inspection System** or **Personalization Agent**.

2. The TOE is configured with Basic Inspection Systems only when the TSF Basic Access Control is enabled. In this configuration the TOE enforces the Basic Access Control SFP according to **FDP_ACC.1/BASIC** and **FDP_ACF.1/BASIC**. In this case the reading of the logical MRTD requires successful authentication as Basic Inspection System or Personalization Agent.

It is up to the security target writer to decide whether the disabling of the TSF Basic Access Control is accompanied with the disabling of the Basic Access Control Authentication Mechanism. Even if the TOE will be configured for use in the phase 4 "Operational Use" with Primary Inspection systems the Personalization Agent may use this mechanism with the Personalization Agent Authentication Keys or a Basic Inspection System may use this mechanism together with secure messaging to protect the logical MRTD against eavesdropping to the communication between TOE and inspection system.

In this Security Target, when the BAC mechanism is disabled the Basic Access Control Authentication Mechanism cannot be used with the Personalization Agent keys or any other keys.

Moreover the Active Authentication mechanism can be enabled or disabled by the Personalization Agent.

Application note 38:
The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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: FMT_SMF.1 Specification of management Functions
                     FMT_SMR.1 Security roles

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,*
> *3.Primary Inspection System,*
> *4.Basic Inspection System.*

FMT_SMR.1.2 The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

Application note 39:
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 40:
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

FQR : 110 4641	*Édition : 1*	*Date : 30/06/2009*	**53/77**

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 41:
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 42:
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/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 or ECC private key]* to *[the Personalization Agent.]*

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 *[Document Basic Access Keys and Personalization Agent Keys and Active Authentication RSA or ECC private key]* to *[none]*.

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

Application note 43:
The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys if the Basic Access Control is enabled. Note the Document Basic Access Keys may be used for the Basic Access Control Authentication Mechanism and secure messaging even if the Basic Access Control is disabled (cf. Application note 37).

6.2.6   Class FPT Protection of the Security functionalities

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 [Active Authentication RSA or ECC 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 *[Active Authentication RSA or ECC private key]*

Dependencies: No other components.

Application note 44
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.

Dependencies: No dependencies

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.

Note:
        The instantiation of this requirement is provided in the following table:

Refinement for FPT_TST.1.1:

Selection and assignments : conditions under which self test should occur
At reset
Before the first execution of the optional code
After the Active Authentication is computed
Before any cryptographic operation
When accessing a DG or EF.TOE_Identification
Prior to any use of TSF data
Before execution of any command
When performing a BAC authentication

Table 7 : TSF Testing

Dependencies: FPT_AMT.1 Abstract machine testing.

Application note 45:
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 46:
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.

6.3   Security Functional Requirements for the TOE

The security assurance requirement level is EAL4 augmented with ALC_DVS.2.

7   TOE SUMMARY SPECIFICATION

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

7.1   Security functionalities 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.SELFTESTs	Self tests
F.ROLLBACK	Safe state management
F.PHYS	Physical protection
IC security functionalities (Security functionalities)	
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 8 : List of the security functionalities of the composite TOE

7.2   Security functionalities provided by the IC

The description of the security functionalities of the IC is provided in [R10], [R11] and [R12].

7.3   Security functionalities 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 following keys are never readable:
- BAC 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, the Document Security Object, EF.COM only after BAC authentication and through 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 functionality 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 personnaliser 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

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

F.BAC - BAC mechanism

This security functionality 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 functionalities 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.

F.SM - Secure Messaging

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

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

F.AUTH_PERSO - Personalisation Agent Authentication

This security functionality 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 functionality ensures the Active Authentication is performed as described in [R1] & [R2]. (if it is activated by the personnalizer).
A self-test on the random generator is performed priori to any Active authentication. Moreover, this security functionality is protected against the DFA.

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 functionalities 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 functionality 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 functionality protects the TOE against physical attacks

8 PP CLAIMS

8.1 PP reference

The PP BAC [R7] is claimed.

8.2 PP refinements

Those refinements (i.e. tailoring) are performed in order to ensure conformance with CC3.1r2.

Some parts of the documents have been removed especially those related to SOF and IT Environment requirements.

FMT_SEM.1 and FPT_SEP.1 do not exist any more in CC3.1r2 and have therefore been removed. Nevertheless, they are implicitly required by the ADV_ARC.1 assurance requirement.

In FPT_PHP.3, CC3.1r2 have rewrite "The TSP is not violated" by "SFRs are always enforced". These two sentences are actually equivalent. The SFR has therefore been rewritten to fulfil CC3.1r2.

FMT_MOF.1 now requires dependencies with FMT_SMF.1 and FMT_SMR.1. These dependencies have been added.

FMT_SMR.1 now requires dependency with FIA_UID.1. This dependency has been added.

8.3 PP additions

The additional functionalities are the Active Authentication (AA) based on the ICAO PKI V1.1 and the related on-card generation of RSA and ECC keys. It implies some addition to the standard PP.

The following SFRs are added to the standard PP for the TOE:
- FCS_COP.1 / SIG_MRTD
- FIA_API.1 / AA
- FDP_ITC / AA
- FMT_MOF.1 / AA
- FCS_CKM.1 / ASYM

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"

The following Threat is added to the standard PP:
- T.counterfeit

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"

9 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 rationale shows the composition with the IC that is evaluated EAL4+.

9.1 Composition with the IC Security target features

9.1.1 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 OSP and are therefore merged with them:

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 pre-personalisation (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 • finding 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

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

Objectives for the 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 [R28])	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)

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

The following IC objectives ensure part of the TOE objectives specified in this table. Therefore these TOE objectives are also covered by requirements covering the related IC objectives.

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	OT.Prot_Inf_Leak

		Manipulation	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
O.HW_DES3		Triple DES Functionality	OT.AC_Pers OT.Data_Int OT_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.AC_Perso
O.SFR_ACCESS		Special Function Register Access Control	OT.Prot_Abuse-Fonc OT.Data_Conf OT.AC_Perso
O.CONFIG		Protection of configuration data	OT.Prot_.Malfunction OT.Prot_Abuse-Fonc

9.1.4 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.Eavesdropping	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	These objectives ensure that no data may be copied from the TOE

T.Abuse-Func	O.Abuse-Func O.Malfunction	
T.Abuse-Func	O.Mem_Access O.SFR_Access O.Abuse-Func O.Malfunction	These objectives ensure the functions for personnalisation 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	These objectives ensure protection against environmental stress that would lead to a malfunction

9.2 Security Objective rationale of the TOE

9.2.1 Standard "Basic Access Control" features

The rationale is identical to the one indicated in [R7]

9.2.2 Addition for the "Active Authentication" feature

	OT.Chip_authenticity	OE.AA_Personalization	OE.AA_=Key_MRTD
T.Chip-ID			
T.Skimming			
T.Counterfeit	x		x
T.Eavesdropping			
T.Forgery			
T.Abuse-Func			
T.Information_Leakage			
T.Phys-tamper			
T.Malfunction			
P.Manufact			

P.Personalization			
P.Personal_Data			
A.Pers_Agent		x	x
A.Insp_Sys			

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.

9.3 Security functional requirements rationale of the TOE

9.3.1 Standard "Basic Access Control" features

The security functional requirements rationale, as well as their justifications is identical to the ones indicated in [R7]

9.3.2 Addition for the "Active Authentication" feature

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

	OT.Chip_Authenticity
FAU_SAS.1	
FCS_CKM.1 / BAC_MRTD	
FCS_CKM.1 / ASYM	x
FCS_CKM.4	
FCS_COP.1 / SHA_MRTD	x
FCS_COP.1 /	x

	OT.Chip_Authenticity
SIG_MRTD	
FCS_COP.1 / TDES_MRTD	
FCS_COP.1 / MAC_MRTD	
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	
FDP_ACC.1 / PRIM	x
FDP_ACF.1 / PRIM	x
FDP_ACC.1 / BASIC	x
FDP_ACF.1 / BASIC	x
FDP_UCT.1 / MRTD	
FDP_UIT.1 / MRTD	
FDP_ITC / AA	x
FMT_MOF.1	
FMT_MOF.1 / AA	
FMT_SMF.1	
FMT_SMR.1	
FMT_LIM.1	
FMT_LIM.2	
FMT_MTD.1 / INI_ENA	
FMT_MTD.1 / INI_DIS	
FMT_MTD.1 /KEY_WRITE	x
FMT_MTD.1 / KEY_READ	x
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 / PRIM**, **FDP_ACF.1 / PRIM**, **FDP_ACC.1 / BASIC**, and **FDP_ACF.1 / BASIC** proving the identity and authenticity of the TOE. The Active Authentication relies on **FCS_COP.1/SIG_MRTD**, **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** or generated on-card by **FCS_CKM.1/ASYM**.

9.3.3 Added dependencies

This table supersedes the PP dependency table:

Requirements	Dependencies	Support of the dependencies
FCS_COP.1 / SIG_MRTD	FDP_ITC.1/AA, FCS_CKM.1/ASYM, FCS_CKM.4/MRTD	Fulfilled
FIA_API.1 / AA	None	Fulfilled
FDP_ITC.1 / AA	FDP_ACF.1	See Justification 1
FMT_SMR.1	FIA_UID.1	Fulfilled
FMT_MOF.1 / AA	FMT_SMF.1, FMT_SMR.1	Fulfilled
FCS_CKM.1 / ASYM	FCS_COP.1/SIG_MRTD, FCS_CKM.4/MRTD	Fulfilled

Justification 1:
FMT_MSA.3 dependency is not required since this import does not involve any specific security attributes.

9.4 Security functionalities/SFRs mapping

The following section maps Security Functionalities supplied by the TOE [R7] to Security Functional Requirements.
.

	Security functionalities of the TOE									Security functionalities of the IC								
	F.ACC_READ	F;ACC_WRITE	F.BAC	F.SM	F.AUTH_PERSO	F.AA	F.SELFTESTS	F.ROLLBACK	F.PHYS	F.RNG	F.HW_DES	F.HW_AES / not used	F.OPC	F.PHY	F.LOG	F.COMP	F.MEM_ACC	F.SFR_ACC / not used
FAU_SAS.1	X	X														X		

	Security functionalities of the TOE									Security functionalities of the IC								
	F.ACC_READ	F;ACC_WRITE	F.BAC	F.SM	F.AUTH_PERSO	F.AA	F.SELFTESTS	F.ROLLBACK	F.PHYS	F.RNG	F.HW_DES	F.HW_AES / not used	F.OPC	F.PHY	F.LOG	F.COMP	F.MEM_ACC	F.SFR_ACC / not used
FCS_CKM.1 / BAC_MRTD			X							X	X							
FCS_CKM.1 / ASYM						X												
FCS_CKM.4			X	X														
FCS_COP.1 / SHA_MRTD			X															
FCS_COP.1 / SIG_MRTD						X												
FCS_COP.1 / TDES_MRTD				X							X							
FCS_COP.1 / MAC_MRTD				X							X							
FCS_RND.1 / MRTD	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							
FIA_UAU.5 / MRTD			X	X	X					X	X					X		
FIA_UAU.6 / MRTD				X							X							
FDP_ACC.1 / PRIM	X	X															X	
FDP_ACF.1 / PRIM	X	X															X	
FDP_ACC.1 / BASIC	X	X															X	
FDP_ACF.1 / BASIC	X	X															X	
FDP_UCT.1 / MRTD				X							X							
FDP_UIT.1 / MRTD				X							X							
FDP_ITC / AA			X			X											X	
FMT_MOF.1			X	X													X	
FMT_MOF.1 / AA			X			X										X	X	
FMT_SMF.1			X													X	X	
FMT_SMR.1			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	X	
FMT_MTD.1			X														X	

	Security functionalities of the TOE									Security functionalities of the IC								
	F.ACC_READ	F;ACC_WRITE	F.BAC	F.SM	F.AUTH_PERSO	F.AA	F.SELFTESTS	F.ROLLBACK	F.PHYS	F.RNG	F.HW_DES	F.HW_AES / not used	F.OPC	F.PHY	F.LOG	F.COMP	F.MEM_ACC	F.SFR_ACC / not used
/KEY_WRITE FMT_MTD.1 / KEY_READ	X																X	
FPT_EMSEC.1	X	X	X	X	X	X			X				X	X	X			
FPT_TST.1							X											
FPT_FLS.1								X					X					
FPT_PHP.3									X				X	X	X			

Table 9 : Mapping of the security functionalities of the TOE vs the SFRs

9.5 Security Assurance requirements rationale

A security assurance requirement rationale for the EAL4+ level is provided in [R8]. This rationale is still relevant for CC3.1r2 considering:
- EAL4 levels are equivalent,
- ALC_DVS.2 augmentations are equivalent,

Moreover, as the underlying IC is certified according to [R6] with level EAL5+, the composition is straight forward.

10 References

MRTD specifications

[R1] 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

[R2] Machine readable Travel Documents – Supplements 9303

[R3] 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

[R4] Advanced Security Mechanisms for Machine readable travel documents – Extended Access control (EAC) – TR03110 – v1.11

[R5] 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

[R6] Smartcard IC Platform Protection Profile v 1.0 - BSI-PP-0002-2001 Jul 2001

[R7] Machine readable travel documents with "ICAO Application", Basic Access control – BSI-PP-0017 v1.0

[R8] Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0026 v1.2

[R9] E-passport: adaptation and interpretation of e-passport Protection Profiles, SGDN/DCSSI/SDR, ref. 10.0.1, February 2007

Security Targets

[R10] Security Target Lite, Evaluation of the P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B Secure Smart Card Controllers, v1.0, March 21st 2007

[R11] Security Target Lite, Evaluation of the NXP P5CD080V0B, P5CN080V0B, P5CC080V0Bn P5CC073V0B Security Target Lite v1.1 -May 9th 2007

[R12] Security Target Lite, Evaluation of the NXP P5CD144V0B, P5CC144V0B, P5CN144V0B Secure Smart Card Controllers, v1.0, March 21st 2007

Standards

[R13] ISO7816-4 – Organization, security and commands for interchange

[R14] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006

[R15] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[R16] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[R17] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[R18] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993

[R19] 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

[R20] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 septembre 1998

[R21] Jakob Jonsson and Burt Kaliski. Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1. RFC 3447, 2003

[R22] RSA Laboratories. PKCS#1 v2.1: RSA cryptography standard. RSA Laboratories Technical Note, 2002

[R23] ANSI X9.31 - Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.

[R24] FIPS 140-2 - Derived Test Requirements for FIPS PUB 140-2

[R25] FIPS 186-3 DRAFT : Digital Signature Standard – March 2006

[R26] ECC Brainpool Standard Curves and Curve Generation draft-lochter-pkix-brainpool-ecc-01

Misc

[R27] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[R28] Smart Card Integrated Circuit With Embedded Software Protection Profile, version 2.0, June 1999. Certified under the reference PP/9911, DCSSI

[R29] NOTE-10 - Interpretation with e-passport PP_courtesy translation-draft v0.1

CC

[R30] Common Criteria for Information Technology security Evaluation Part 1 : Introduction and general model, CCMB-2006-09-001, version 3.1 Revision 1, September 2006

[R31] Common Criteria for Information Technology security Evaluation Part 2 : Security Functional Components, CCMB-2007-09-002, version 3.1 Revision 2, September 2007

[R32] Common Criteria for Information Technology security Evaluation Part 3 : Security Assurance Components, CCMB-2007-09-003, version 3.1 Revision 2, September 2007

11 ACRONYMS

AA	Active Authentication
BAC	Basic Access Control
CC	Common Criteria Version 3.1 revision
CPLC	Card personalisation life cycle
DF	Dedicated File
DFA	Differential Fault Analysis
DG	Data Group
EAL	Evaluation Assurance Level
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
TOE	Target of Evaluation
TSF	TOE Security function