

Security Target Lite
for the
PEACOS
Extended Access Control MRTD

Common Criteria version 3.1 revision 3 – ISO/IEC 15408
Assurance Level EAL 4+

Developer



Gep S.p.A.
Corso Salvatore D'Amato, 90
80022 Arzano (NA), ITALY
www.gepitalia.it

Sponsor



Istituto Poligrafico e Zecca dello Stato S.p.A.
Via Salaria, 1027
00138 Roma, ITALY
www.ipzs.it

Version 1.2
Date 02.03.2011
Reference TCLE100138
Classification PUBLIC

Version control

Version	Date	Author	Revision Description
1.0	20.12.2010	Marco EVANGELISTA	First version
1.1	11.02.2011	Marco EVANGELISTA	In section 1.5.4.2 it is now clearly stated that patches are loaded in step 1 "IC Manufacturing" of Phase 2 "Manufacturing"
1.2	02.03.2011	Marco EVANGELISTA	An application note has been added to section 1.3 "TOE Reference", regarding the product version identifier. Technical References for composition have been updated. The address of the Sponsor has been updated.

Table of Contents

Abbreviations and Notations	5
1. Introduction	6
1.1 ST Overview	6
1.2 ST reference.....	6
1.3 TOE reference.....	7
1.4 TOE overview	7
1.4.1 TOE Usage and security features	8
1.5 TOE Description	10
1.5.1 Physical scope of the TOE	10
1.5.2 Other non-TOE physical components	11
1.5.3 Logical scope of the TOE	11
1.5.4 TOE Life-cycle.....	12
2. Conformance claims	16
2.1 Conformance with the Common Criteria.....	16
2.2 Conformance with a Protection Profile	16
2.3 Conformance with an assurance package.....	16
3. Security Problem Definition.....	17
3.1 Introduction.....	17
3.1.1 Assets.....	17
3.1.2 Subjects.....	17
3.2 Threats	19
3.3 Organizational Security Policies	22
3.4 Assumptions.....	23
4. Security Objectives	25
4.1 Security Objectives for the TOE	25
4.2 Security Objectives for the environment.....	28
4.2.1 Development and Manufacturing Environment.....	28
4.2.2 Operational Environment.....	28
4.3 Rationale	30
5. Extended Components Definition.....	35
5.1 Definition of the family FAU_SAS	35
5.2 Definition of the family FCS_RND	35
5.3 Definition of the family FIA_API.....	36
5.4 Definition of the family FMT_LIM.....	37
5.5 Definition of the family FPT_EMSEC.....	39
6. Security Requirements.....	41
6.1 Security Functional Requirements for the TOE	41
6.1.1 Class FAU Security Audit	41
6.1.2 Class Cryptographic Support (FCS)	41
6.1.3 Class FIA Identification and Authentication	47
6.1.4 Class FDP User Data Protection	53
6.1.5 Class FMT Security Management	57
6.1.6 Class FPT Protection of the Security Functions	64
6.2 Security Assurance Requirements for the TOE	67
6.3 Security Requirements Rationale	67
6.3.1 Security functional requirements rationale.....	67
6.3.2 Dependency Rationale	73
6.3.3 Security Assurance Requirements Rationale	76

6.3.4	Security Requirements – Mutual Support and Internal Consistency	76
7.	TOE Summary Specification	78
7.1	Coverage of SFRs	78
7.1.1	Agents Identification & Authentication	78
7.1.2	Data exchange with Secure Messaging	79
7.1.3	Access Control of stored Data Objects	79
7.1.4	Life cycle management	80
7.1.5	Software integrity check of TOE's assets	80
7.1.6	Security features provided by the hardware	80
7.1.7	Verification of digital signatures	80
7.2	Assurance Measures	83
8.	References	85
8.1	Acronyms	85
8.2	Glossary	86
8.3	Technical References	93
Appendix A	Integrated Circuits supported by PEACOS	96
A.1	NXP P5CD080V0B Integrated Circuit	96
A.1.1	Chip Identification	96
A.1.2	IC Developer Identification	96
A.1.3	IC Manufacturer Identification	96
A.1.4	Main Features	96

List of Tables

Table 1 – ST Identification	6
Table 2 – TOE Identification	7
Table 3 – Security Objectives Rationale	31
Table 4 – Family FAU_SAS	35
Table 5 – Family FCS_RND	36
Table 6 – Family FIA_API	37
Table 7 – Family FMT_LIM	38
Table 8 – Family FPT_EMSEC	40
Table 9 - Object Identifiers for Terminal Authentication with RSA	46
Table 10 – FIA_AFL.1 Refinement	52
Table 11 – Assurance requirements at EAL4+	67
Table 12 – Security Objectives Coverage for the TOE by the SFR	68
Table 13 – Dependencies between the SFR for the TOE	75
Table 14 – Coverage of SFRs by security services	82
Table 15 – Assurance Requirements documentation	84

List of Figures

Figure 1 – Physical TOE	11
Figure 2 – TOE Life Cycle	13
Figure 3 – NXP P5CD080V0B internal architecture	97

Abbreviations and Notations

Numerical values

Numbers are printed in decimal or hexadecimal notation.

Hexadecimal values are indicated with a 'h' suffix as in XXh, where X is a hexadecimal digit from 0 to F.

Decimal values have no suffix.

Example: the decimal value 179 may be noted as the hexadecimal value B3h.

Denoted text

The text added to provide details on how the TOE implementation fulfils some security requirements is written in *italics* and is preceded by the numbered tag "Application Note".

Refinements to the security requirements are denoted by the tag "Refinement" and are written in **bold** text.

Selections and *assignments* made by the Protection Profile authors are written in underlined text.

Selections and *assignments* made by the authors of this ST are written in **underlined bold** text.

The original text of the selection and assignment components, as defined by the Common Criteria, is given by a footnote.

Key words

The words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" are to be interpreted as described in RFC2119 [R34].

1. Introduction

1.1 ST Overview

This Security Target (ST) document provides the information necessary to understand the security properties and the scope of the Common Criteria evaluation of the PEACOS electronic passport. The Target Of Evaluation (TOE) is the contactless integrated circuit NXP P5CD080V0B programmed with the operating system and with the passport application. The TOE adds security features to a passport booklet, providing machine-assisted identity confirmation and machine-assisted verification of document security.

The PEACOS passport was developed in full accordance with specifications for a Machine Readable Travel Document (MRTD) defined by the International Civil Aviation Organization (ICAO). ICAO's technical reports (Doc 9303 [R14], TR-BD [R15], TR-LDS [R16] and TR-PKI [R17]) detail technical properties and security features of such a travel document, as well as recommendations for the security environment in which it operates.

The TOE is meant for "global interoperability". According to ICAO the term is understood as *"the capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States"*.

The TOE is supplied with a file system, that contains all the data that is used in the context of the ICAO application as described in the Protection Profile (PP) "Machine Readable Travel Document with ICAO Application, Extended Access Control" [R5].

1.2 ST reference

Title	Security Target Lite for the PEACOS Extended Access Control MRTD
Version	1.2
Author	Marco EVANGELISTA
Reference	TCLE100138
Keywords	Security Target, Protection Profile, Common Criteria

Table 1 – ST Identification

1.3 TOE reference

Product Name	PEACOS
Product Version	1.2
Evaluation Criteria	Common Criteria version 3.1 revision 3
Protection Profile	BSI-PP-0026
Evaluation Assurance Level	EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5
Developer	Gep S.p.A.
Evaluation Sponsor	Istituto Poligrafico e Zecca dello Stato S.p.A.
Evaluation Facility	SERMA Technologies' ITSEF
Certification Body	ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information
Keywords	Electronic Passport, ICAO, Machine Readable Travel Document, Extended Access Control

Table 2 – TOE Identification

The TOE identification data is located in the non-volatile memory of the chip and can be read by following the procedure detailed in the User Guidance [R35].

Application Note 1: *The product version is composed of a major version number, indicating the ROM code version, and of a minor version number, indicating the patch version. The major version number and the minor version number are separated by the character “_” (underscore, ASCII code 5Fh). A minor version number 0 (ASCII code 30h) indicates that no patch is loaded.*

1.4 TOE overview

The TOE is the contactless integrated circuit of MRTD, programmed according to the Logical Data Structure (LDS) defined by ICAO [R16], and providing Basic Access Control (BAC) according to ICAO TR-PKI [R17] and Extended Access Control (EAC) as defined in the TR-03110 technical guideline from BSI [R6].

On account of its composite nature, the TOE evaluation builds on the evaluation of the integrated circuit.

The chip is equipped with an operating system and with a software application providing the passport features. Cryptographic techniques are applied to confirm the identity of the holder and to verify the authenticity of the passport.

The TOE is embedded between two sheets, which also embed an antenna for wireless communication. The resulting sandwich, called “inlay”, is intended to be attached to a passport booklet (see section 1.5.4).

Once personalized with the data of the legitimate holder and with security data, the e-Passport can be inspected by authorized agents.

The product provides a number of security features to prevent forgery, tampering and data leakage. Such features include:

- User authentication based on symmetric key cryptography to protect the overall content of the passport
- Additional user authentication based on asymmetric key cryptography to protect sensitive biometric data, such as fingerprints and iris image
- Sophisticated on-chip sensors to detect all known types of attack
- Memory management unit to prevent improper usage of memory and unauthorized code execution
- Encrypted communications between the passport and the Inspection System

The product also provides the following security mechanisms:

- Basic Access Control (BAC) mechanism according to the ICAO TR-PKI technical report [R17]
- Extended Access Control (EAC) mechanism, implemented combining the Chip Authentication mechanism with the Terminal Authentication protocol, as defined in the BSI TR-03110 technical guideline [R6]

The TOE is comprised of:

- the circuitry of the MRTD's chip (see Appendix A)
- the IC Embedded Software (PEACOS Operating System)
- the passport application as defined in the ICAO TR-LDS technical report [R16]
- the associated guidance documentation.

1.4.1 TOE Usage and security features

States or organizations issue MRTDs to be used by the holder for international travel. The traveler presents an MRTD to the Inspection System to prove his or her identity.

The MRTD in the context of this ST contains:

- i. visual (eye readable) biographical data and portrait of the holder,
- ii. a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ), and
- iii. data elements on the MRTD's chip according to LDS for contactless machine reading.

The authentication of the traveler is based on:

- the possession of a valid MRTD personalized for the traveler with the claimed identity as given on the biographical data page, and
- biometrics using the reference data stored in the MRTD chip.

The Issuing State or Organization ensures the authenticity of the data of genuine MRTDs, while the receiving State trusts a genuine MRTD of an Issuing State or Organization.

For this ST the MRTD is viewed as the union of:

- the *physical MRTD* as travel document in the form of paper, plastic and chip. It presents visually readable data including (but not limited to) personal data of the MRTD holder:
 - i. the biographical data on the biographical data page of the passport booklet,
 - ii. the printed data in the Machine Readable Zone (MRZ),
 - iii. the printed portrait.

- the *logical MRTD* as data of the MRTD holder stored according to the Logical Data Structure [R12] as specified by ICAO on the contactless integrated circuit. It presents machine readable data including (but not limited to) personal data of the MRTD holder:
 - i. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
 - ii. the digitized portraits (EF.DG2),
 - iii. the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,
 - iv. the other LDS DGs (EF.DG5 to EF.DG14, EF.DG16),
 - v. the document security object (EF.SOD),
 - vi. security data objects required for product management.

The Issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and its data. The printed MRTD and the MRTD's chip are uniquely identified by the document number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [R14]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD delivered by the IC Manufacturer is protected by a mutual authentication mechanism based on symmetric cryptography until completion of the initialization and pre-personalization processes. After completion the authentication keys are disabled.

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 as well as the security features of the MRTD's chip.

The ICAO [R17] defines this baseline required security method, Passive Authentication, and the following optional advanced security methods:

- Basic Access Control (BAC),
- Active Authentication,
- Extended Access Control (EAC),
- data encryption of sensitive biometrics as an optional security measure.

Passive Authentication and data encryption are wholly performed independently on the TOE by the TOE environment.

This ST addresses the protection of data integrity and confidentiality of the logical MRTD by the following means:

- in integrity by write-once access control enforced by logical and physical means,
- in confidentiality on less sensitive data (e.g. the MRZ, the facial image and other data that can easily be acquired elsewhere) by the BAC Mechanism
- in confidentiality on more sensitive data, such as finger and iris biometric data, by the EAC Mechanism.

Furthermore, this ST addresses the Chip Authentication described in [R6] as an alternative to the Active Authentication stated in [R17].

The BAC mechanism cannot be disabled by the Issuing State or Organization.

The Inspection System:

1. reads the printed data in the MRZ,
2. authenticates itself, using the BAC mechanism, by means of the keys derived from MRZ data. After a successful BAC authentication, the MRTD chip provides read access to the logical MRTD, except for the EF.DG3 and EF.DG4 data group files, by means of private communication (secure messaging) with this Inspection System [R17], [R16].

This ST does not address Active Authentication because, as an alternative, the TOE provides evidence of the MRTD's chip authenticity by means of the Chip Authentication mechanism described in [R6]. The Chip Authentication prevents data traces described in [R14], normative appendix 7, A7.3.3. The Chip Authentication is provided throughout the following steps:

1. The Inspection System communicates by means of the Secure Messaging established by Basic Access Control,
2. The Inspection System reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object,
3. The Inspection System generates an ephemeral key pair,
4. The TOE and the Inspection System agree on two session keys for Secure Messaging in ENC_MAC mode according to the Diffie-Hellman Primitive, and
5. The Inspection System verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. whether it could apply the Chip Authentication Private Key corresponding to Chip Authentication Public Key for derivation of the session keys).

Access to sensitive data stored in EF.DG3 and EF.DG4 is given only on successful completion of an EAC authentication.

The EAC mechanism requires the proof of chip authenticity, obtained by means of Chip Authentication, and a subsequent proof of Inspection System's entitlement as an entity authorized by the Issuing State or Organization through the receiving State. The latter proof is obtained executing the Terminal Authentication Protocol. Sensitive data exchange is protected by the Secure Messaging session established by the Chip Authentication. The Terminal Authentication shall be preceded by a successful Chip Authentication.

The issuing State or Organization authorizes the receiving State by means of a certification chain: a Country Verifying Certification Authority (CVCA) issues certificates for the Document Verifier (DV) which in turn creates the Inspection System Certificates. Further details on the Public Key Infrastructure (PKI) required by EAC can be found in the BSI TR-03110 technical guideline [R6].

1.5 TOE Description

1.5.1 Physical scope of the TOE

The physical structure of the PEACOS product is comprised of an integrated circuit chip (microcontroller) programmed with the operating system and with the passport application.

The microcontrollers supported by the PEACOS operating system are described in Appendix A.

1.5.2 Other non-TOE physical components

The inlay embedding the TOE is comprised of the following:

- a contactless interface (antenna),
- a substrate containing the antenna and the chip.

Wireless communication protocol is ISO 14443 compliant [R26][R27][R28][R29], carrier frequency is 13.56 MHz and the antenna is compliant with the ISO 14443-1 standard [R26].

The integrated circuit is powered by the electromagnetic field radiated by the passport reader that equips the user workstations.

Figure 1 shows the hardware components inlay with an internal view of the microcontroller.

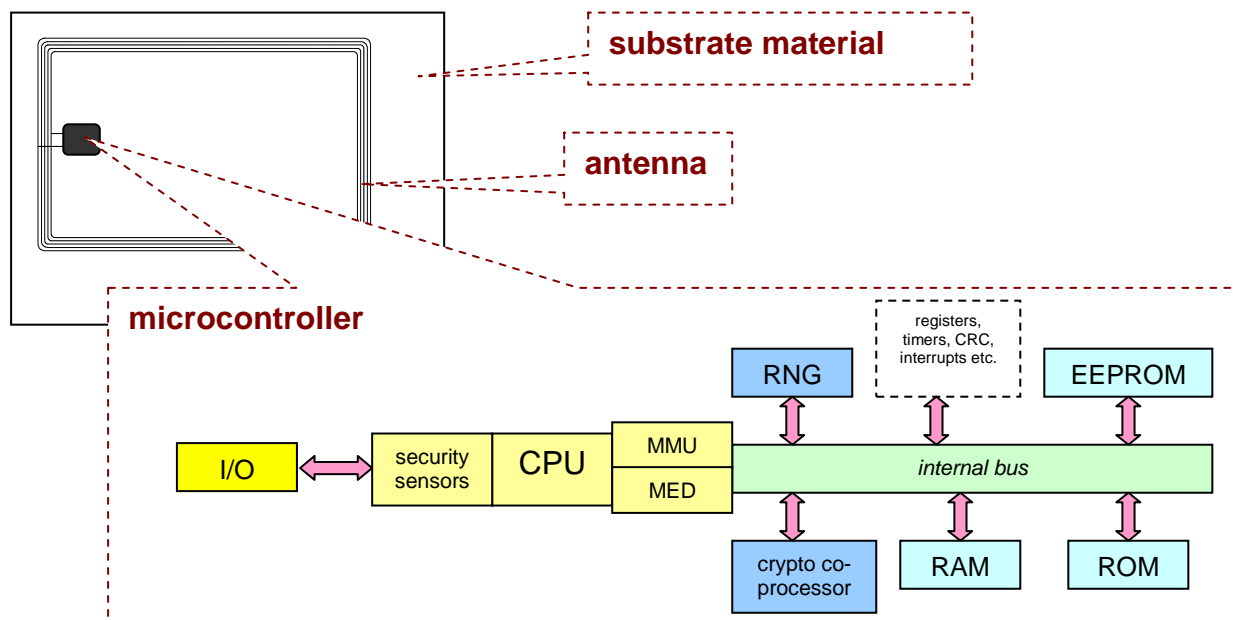


Figure 1 – Physical TOE

1.5.3 Logical scope of the TOE

The logical part of the TOE comprises the following software components stored in the non-volatile memory units of the microcontroller:

- operating system
- file system
- passport application
- security data objects

The PEACOS operating system manages all the resources of the integrated circuit that equips the passport, providing secure access to data and functions. Major tasks performed by the operating system are:

- Communication between internal objects
- Communication with external devices

- Data storage in the file system
- Execution of commands
- Cryptographic operations

The operating system has a flexible modular structure and a layered architecture providing:

- full support of the ICAO LDS passport application
- Basic Access Control
- Extended Access Control
- secure support of various types of applications
- secure management of functions and data

The file system contains security data objects and the LDS passport application.

1.5.4 TOE Life-cycle

The TOE life cycle is described in terms of four life cycle phases (shown in Figure 2):

1. Development, composed of (i) the development of the operating system software by the Embedded Software Developer and (ii) the development of the integrated circuit by the IC Manufacturer
2. Manufacturing, composed of (i) the fabrication of the integrated circuit by the IC Manufacturer, (ii) the completion of the operating system, (iii) the embedding of the chip in an inlay with an antenna, (iv) the initialization and pre-personalization of the MRTD
3. Personalization
4. Operational Use

Application Note 2: *The entire Development phase, as well as step (i) “fabrication of the integrated circuit” of the Manufacturing phase are the only phases covered by assurance as during these phases the TOE is under construction in a protected environment.*

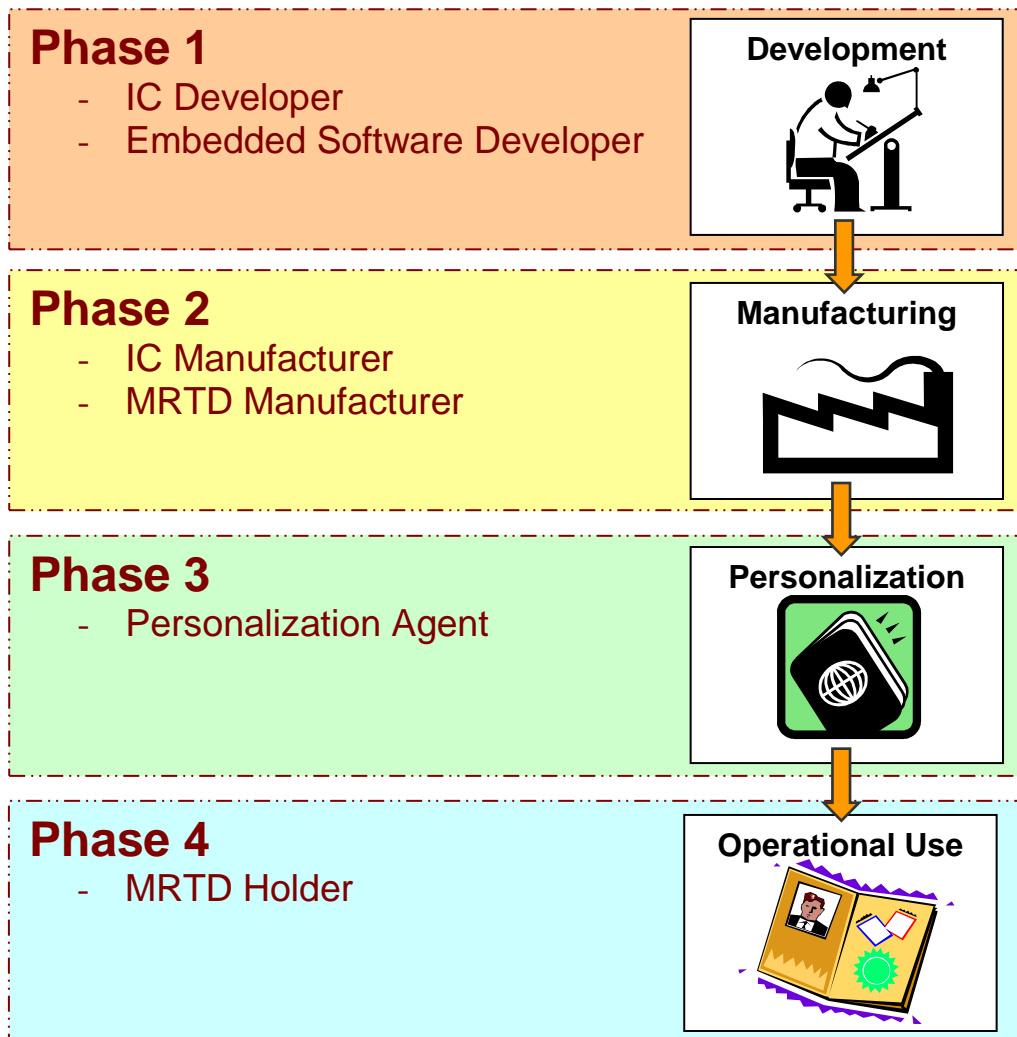


Figure 2 – TOE Life Cycle

1.5.4.1 Development

The TOE is developed in phase 1. The IC Developer develops the IC, the IC dedicated software and the technical documentation associated with these TOE components. The Embedded Software Developer uses the IC’s technical documentation (datasheet and relevant parts of the IC dedicated software) and develops the IC embedded software (operating system and MRTD LDS application) as well as the technical documentation associated with these TOE components. The IC embedded software in the non-volatile memories, the MRTD application and the technical documentation are securely delivered to the MRTD Manufacturer.

1.5.4.2 Manufacturing

The Manufacturing phase is carried out in two steps.

Fist step: IC manufacturing

In a first step, the TOE IC is produced by the IC Manufacturer. The MRTD embedded software is stored in the non-volatile memories of the chip; the operating system is held in ROM, while EEPROM contains patches and initialization data.

In this step the IC Manufacturer writes:

- patches to the IC Embedded Software, if any, and
- the initialization data.

The finished ICs are delivered from the IC Manufacturer to the MRTD Manufacturer. During delivery the ICs are protected by a symmetric cryptographic mechanism.

Second step: MRTD manufacturing

In the second step, the MRTD Manufacturer:

- produces the inlay. The chip is bound to a substrate, then an antenna is electrically connected to the chip
- binds the inlay to the passport booklet
- equips MRTD's chip with pre-personalization data.

The pre-personalized inlay and the related technical documentation are securely delivered from the MRTD Manufacturer to the Personalization Agent.

Application Note 3: *In the contexts where no distinction is made between the subjects participating in the manufacturing, the IC Manufacturer and the MRTD Manufacturer are both referred to as “the Manufacturer”.*

1.5.4.3 Personalization of the MRTD

The personalization of the MRTD, performed by the Personalization Agent, includes:

- survey of the MRTD holder biographical data,
- enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- printing of the Visual Inspection Zone (VIZ) data onto the physical MRTD,
- writing of the TOE User Data into the LDS of the logical MRTD,
- writing of the TOE Security Functionality (TSF) data into the LDS of the logical MRTD,
- configuration of the TSF, if necessary.

The step “writing the TOE User Data” includes (but is not limited to) the creation of:

- the digital MRZ data (EF.DG1),
- the digitized portrait (EF.DG2),
- the EF.COM elementary file
- the document security object (EF.SOD).

The signing of the SO_D by the Document Signer [R17] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate documentation specifying TOE use if necessary) is handed over to the MRTD holder for operational use.

1.5.4.4 Operational Use

The TOE is used as MRTD chip by the traveler and the Inspection Systems in the “Operational Use” phase. The User Data can be read according to the security policy of the Issuing State or Organization and used according to the security policy of the Issuing State, but they can never be modified.

2. Conformance claims

2.1 Conformance with the Common Criteria

This ST claims conformance to:

- Common Criteria version 3.1 revision 3, International English Version [R7][R8][R9], as follows:
 - Part 2 (security functional requirements) extended
 - Part 3 (security assurance requirements) conformant

The software part of the TOE runs on the chips reported in Appendix A. All the supported chips are certified against the Common Criteria.

2.2 Conformance with a Protection Profile

This ST claims demonstrable conformance to:

- BSI-PP-0026 Protection Profile for Machine Readable Travel Document with “ICAO Application” Extended Access Control version 1.2 November 2007 [R5].

This Protection Profile defines some Extended Security Functional Requirements (see section 4).

2.3 Conformance with an assurance package

This ST claims conformance to:

- EAL4 assurance package augmented with ALC_DVS.2 and AVA_VAN.5

Application Note 4: *For interoperability reasons, it is assumed the receiving State cares for sufficient measures against eavesdropping within the operating environment of the Inspection Systems. Otherwise the MRTD may protect the confidentiality of some less sensitive assets (e.g. the personal data of the MRTD holder which are also printed on the physical MRTD) for some specific attacks only against low attack potential (AVA_VAN.3).*

3. Security Problem Definition

3.1 Introduction

3.1.1 Assets

The assets to be protected by the TOE are comprised of the data stored in the chip internal memory. These data can be divided into two groups: the data available to users (User Data) and the data which can only be accessed by the operating system (TSF Data).

Even if all assets could be protected with a high security level (with the EAC mechanism), some of them, hereafter indicated as “standard data”, have to be accessible through a mechanism with a lower security level (BAC mechanism). This is due to interoperability reasons as the ICAO Doc 9303 [R14] specifies only the BAC mechanism.

Standard data

User Data protected by BAC mechanism, consisting of:

- Less sensitive personal data of the MRTD holder contained in the EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16 elementary files
- The EF.DG14 elementary file containing the public key required by the Chip Authentication Protocol
- The EF.COM elementary file that contains a list of the existing data groups (only data groups EF.DG1 and EF.DG2 are mandatory)
- The EF.SOD elementary file, that is used by the Inspection System for Passive Authentication of the logical MRTD
- The EF.CVCA elementary file containing references of trusted CVCA public keys

Sensitive data

User Data protected by the EAC mechanism, consisting of sensitive biometric data of the MRTD holder such as fingerprints and iris image, contained in the EF.DG3 and EF.DG4 elementary files

A further asset to be protected is the authenticity of the MRTD chip. The authenticity of the MRTD chip personalized by the Issuing State or Organization for the MRTD's holder is used by the traveler to authenticate himself as possessing a genuine MRTD.

3.1.2 Subjects

This Security Target considers the following subjects:

- **Manufacturer:** The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer producing the inlay. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.
- **Personalization Agent:** The agent who is acting on the behalf of the Issuing State or Organization to personalize the MRTD for the holder by some or all the following activities:
 - I. establishing the identity of the holder for the biographic data in the MRTD,

- II. enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s),
 - III. writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability,
 - IV. writing the initial TSF Data and
 - V. signing the Document Security Object (SO_D) as defined in the TR-LDS technical report [R16].
- **Country Verifying Certification Authority:** The Certification Authority enforcing the privacy policy of the issuing Country or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.
 - **Document Verifier:** The Certification Authority enforcing the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.
 - **Terminal:** A terminal is any technical system communicating with the TOE through the contactless interface.
 - **Inspection System (IS):** A technical system used by the border control officer of the receiving state (i) in examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
 - I. The **Basic Inspection System (BIS)**
 - contains a terminal for the contactless communication with the MRTD's chip,
 - implements the terminals part of the BAC Mechanism,
 - gets the authorization to read the logical MRTD under the BAC by optically reading the printed data in the MRZ or other parts of the passport book providing this information.
 - II. The **General Inspection System (GIS)** is a Basic Inspection System which additionally implements the Chip Authentication Mechanism.
 - III. The **Extended Inspection System (EIS)** in addition to the General Inspection System
 - implements the Terminal Authentication protocol, and
 - is authorized by the Issuing State or Organization through the Document Verifier of the receiving state to read the sensitive biometric reference data.

The security attributes of the EIS are defined by the Inspection System Certificates.

Application Note 5: *The Personalization Agent is not allowed to disable the BAC mechanism. Therefore, an Inspection System shall implement at least the terminal part of the BAC mechanism and, optionally, may implement the terminal part of the Chip Authentication and of the Terminal Authentication mechanisms.*

- **MRTD Holder:** The rightful holder of the MRTD for whom the Issuing State or Organization personalized the MRTD.
- **Traveler:** A person presenting the MRTD to the Inspection System and claiming the identity of the MRTD holder.
- **Attacker:** A threat agent trying:
 - I. to identify and to trace the movement 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.

Application Note 6: *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.*

- **Initialization and Pre-personalization Terminal (IPT):** A system used by the MRTD Manufacturer to perform TOE initialization and pre-personalization; it allows to
 - implement the terminal part in a Secure Messaging session,
 - write user and TSF Data in the logical MRTD.
- **Personalization Terminal (PT):** A system used by the Personalization Agent to perform TOE personalization and configuration; it allows to
 - implement the terminal part in a Secure Messaging session,
 - write user and TSF Data in the logical MRTD.

3.2 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 is trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker cannot read and does not know in advance the physical MRTD.
- **T.Skimming: Skimming the logical MRTD**

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

- **T.Read_Sensitive_Data: Read the sensitive biometric reference data**

An attacker with high attack potential knowing the Document Basic Access Keys is trying to gain the sensitive biometric reference data through the communication interface of the MRTD's chip.

The attack T.Read_Sensitive_Data is similar to the threats T.Skimming in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data is stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visual readable on the physical MRTD as well.

- **T.Forgery: Forgery of data on MRTD's chip**

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose on an Inspection System by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the Inspection System. The attacker may combine data groups of different logical MRTD's 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 traveler into an other MTRD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD in another contactless chip.

- **T.Counterfeit: Counterfeit of MRTD's chip**

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

The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

The TOE shall avert the 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 initialization 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 which is leaked from the TOE during its usage in order to disclose confidential TSF Data. The information leakage may be inherent in the normal operation or caused by the attacker.

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

- **T.Phys_Tamper: Physical Tampering**

An attacker may perform physical probing of the MRTD's chip in order:

- i. to disclose TSF Data, or
- ii. to disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD's chip in order to:

- i. modify security features or functions of the MRTD's chip,
- ii. modify security functions of the MRTD's chip Embedded Software,
- iii. modify User Data or
- iv. modify TSF Data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the Inspection System) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used.

Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

- **T.Malfunction: Malfunction due to Environmental Stress**

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to:

- i. deactivate or modify security features or functions of the TOE or
- ii. circumvent or deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misuse of administration function. To exploit this an attacker needs information about the functional operation.

3.3 Organizational Security Policies

The TOE shall comply to the following organization security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

- **P.Manufact: Manufacturing of the MRTD's chip**

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process while controlling the MRTD's material in Phase 2 Manufacturing. The initialization data are written by the IC Manufacturer to identify the IC uniquely. The IC identification data is written by the IC Manufacturer. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent's Keys (KA_{PA}).

- **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 (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by Inspection Systems to which the MRTD is presented. Additional to the Basic Access Control Authentication defined by ICAO in [R17] the MRTD's chip shall protect the confidentiality and integrity of the personal data during transmission to the General Inspection System after Chip Authentication.

Application Note 7: *The organizational security policy P.Personal_Data is drawn from the ICAO Technical Report [R17]. Note that the Document BAC Keys are defined by the TOE environment and loaded to the TOE by the Personalization Agent.*

- **P.Sensitive_Data: Privacy of sensitive biometric reference data**

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the MRTD holder. The sensitive biometric reference data can be used only by Inspection Systems which are authorized for this access at the time the MRTD is presented to the Inspection System. The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of Inspection Systems within the limits defined by the Document Verifier Certificate.

3.4 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 BAC Keys,
- iii. the Chip Authentication Public Key Info (EF.DG14) if stored on the MRTD's chip, and
- iv. the Document Signer Public Key Certificate (C_{DS}) if stored on the MRTD's chip.

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

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

The Inspection System is used by the border control officer of the receiving State

- i. examining an MRTD presented by the traveler and verifying its authenticity and
- ii. verifying the traveler as MRTD holder.

The Basic Inspection System for global interoperability

- i. includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and
- ii. implements the terminal part of the Basic Access Control.

The Basic Inspection System reads the logical MRTD being under Basic Access Control and performs the Passive Authentication to verify the logical MRTD. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism.

The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes Secure Messaging with keys established by the Chip Authentication Mechanism.

The Extended Inspection System in addition to the General Inspection System

- i. supports the Terminal Authentication Protocol and
- ii. is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Application Note 8: *The combination of both Chip Authentication and Terminal Authentication provides an implementation of the Extended Access Control mechanism. The TOE allows the Personalization Agent to disable the EAC for use with BISs.*

- **A.Signature_PKI: PKI for Passive Authentication**

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which:

- i. securely generates, stores and uses the Country Signing CA Key pair, and
- ii. manages the MRTD's Chip Authentication Key Pairs.

The CA keeps the Country Signing CA Private Key secret and distributes the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer:

- i. generates the Document Signer Key Pair,
- ii. hands over the Document Signer Public Key to the CA for certification,
- iii. keeps the Document Signer Private Key secret and
- iv. uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs.

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

- **A.Auth_PKI PKI for Inspection Systems**

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

4. Security Objectives

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

4.1 Security Objectives for the TOE

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

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

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [R12] and the TSF Data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF Data can be written only once and can not be changed after personalization.

Application Note 9: *The OT.AC_Pers implies that the data of the LDS groups written during personalization for the MRTD holder (at least EF.DG1 and EF.DG2) cannot be changed by write access after personalization*

- **OT.Data_Int: Integrity of personal data**

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

- **OT.Data_Conf: Confidentiality of personal data**

The TOE must ensure the confidentiality of the data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 and the Document Security Object of the logical MRTD by granting read access to terminals successfully authenticated by as

- i. Personalization Agent or
- ii. Basic Inspection System or
- iii. Extended Inspection System.

The TOE implements the Basic Access Control as defined by ICAO [R17] and enforces Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

Application Note 10: *The traveler grants the authorization for reading the standard User Data to the Inspection System by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security*

function Basic Access Control Authentication independent on the quality of the Document Basic Access Keys which is defined by the TOE environment and loaded into the TOE by the Personalization Agent. Any attack based on the decision of the ICAO TR-PKI technical report to derive the BAC keys from the visual MRZ does not prevents from achieving the security objective OT.Data_Conf.

- **OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data**

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

- **OT.Identification: Identification and Authentication of the TOE**

The TOE must provide means to store IC Identification Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. In Phase 4 “Operational Use” the TOEs shall identify themselves only to a successfully authenticated BIS.

Application Note 11: *The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the MRTD”. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing environment as described in its security objective OD.Material. In the Phase 4 “Operational Use” the TOE is identified by the passport number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit serial number ICCSN) or a MRTD identifier through the contactless interface before successful authentication as Basic Inspection System.*

- **OT.Chip_Auth_Proof Proof of MRTD’S chip authenticity**

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD’s chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [R6]. The authenticity proof provided by MRTD’s chip shall be protected against attacks with high attack potential.

Application Note 12: *The OT.Chip_Auth_Proof implies the MRTD’s chip to have:*

- a unique identity as given by the MRTD’s Document number,*
- a secret to prove its identity by knowledge i.e. a private authentication key as TSF Data.*

The TOE shall protect this TSF Data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD’s chip i.e. a certificate for the

Chip Authentication Public Key that fit to the Chip Authentication Private Key of the MRTD's chip. This certificate is provided:

- i. by the Chip Authentication Public Key (EF.DG14) in the LDS [R6] and
- ii. by the hash value of the Authentication Public Key in the Document Security Object (SO_D) signed by the Document Signer.

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

- **OT.Prot_Abuse-Func: Protection against Abuse of Functionality**

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order:

- i. to disclose critical User Data,
- ii. to manipulate critical User Data of the Smartcard Embedded Software,
- iii. to manipulate Soft-coded Smartcard Embedded Software,
- iv. bypass, deactivate, change or explore security features or functions of the TOE.

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

- **OT.Prot_Inf_Leak: Protection against Information Leakage**

The TOE must provide protection against disclosure of confidential TSF Data stored and/or processed in the MRTD's chip

- i. by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- ii. by forcing a malfunction of the TOE and/or
- iii. by a physical manipulation of the TOE.

Application Note 13: *This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.*

- **OT.Prot_Phys-Tamper: Protection against Physical Tampering**

The TOE must provide protection the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with high attack potential by means of

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

with a prior

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

Application Note 14: *In order to meet the security objectives OT.Prot_Phys-Tamper the TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack. This is addressed by the security objective OD.Assurance.*

- **OT.Prot_Malfunction: Protection against Malfunctions**

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Application Note 15: *A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE's internals.*

4.2 Security Objectives for the environment

4.2.1 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 Initialization Data for unique identification of the TOE and the pre-personalization of the TOE including the writing of the Personalization Agent Authentication key(s). The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against obvious penetration attacks with high attack potential.

- **OD.Material: Control over MRTD Material**

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

4.2.2 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 behalf of the issuing State or Organization

- i. establish the correct identity of the holder and create biographical data for the MRTD,
- ii. enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and
- iii. personalize the MRTD for the holder together with the defined physical and logical security measures (including the digital signature in the SO_D) to protect the confidentiality and integrity of these data.

- **OE.Pass_Auth_Sign: Authentication of logical MRTD by Signature**

The Issuing State or Organization must:

- i. generate a cryptographic secure Country Signing CA Key Pair,
- ii. ensure the secrecy of the Country Signing CA Private Key (SK_{CSCA}) and sign C_{DS}'s in a secure operational environment,
- iii. distribute the Country Signing CA public key to Receiving States and Organizations maintaining its authenticity and integrity.

Moreover 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 (SK_{DS}),
- ii. sign Document Security Objects of genuine MRTD in a secure operational environment only, and
- iii. distribute the Certificate of the Document Signing Public Key to receiving States and organizations. The digital signature in the Document Security Object relates to all data in the data groups EF.DG1 to EF.DG16 if stored in the LDS according to [R16].

- **OE.Auth_Key_MRTD MRTD Authentication Key**

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

- i. generate the MRTD's Chip Authentication Key Pair,
- ii. sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and
- iii. support Inspection Systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

- **OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data**

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

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 traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability

- i. includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and
- ii. implements the terminal part of the Basic Access Control [R6].

Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

- **OE.Passive_Auth_Verif: Verification by Passive Authentication**

The border control officer of the Receiving State uses the Inspection System to verify the traveler as MRTD holder. The Inspection Systems must have successfully verified the signature of the SO_D and the integrity data elements of the logical MRTD before they are used. The Receiving States and Organizations must manage the PK_{CSCA} and the PK_{DS} 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 will prevent eavesdropping to the communication between TOE and Inspection System before Secure Messaging is successfully established based on the Chip Authentication Protocol.

Application Note 16: *Please keep in mind that reading of less sensitive data is allowed after a successful BAC authentication. i.e. this can happen even in a GIS or EIS before establishment of a chip authentication and/or a terminal authentication. The TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication only.*

- **OE.Ext_Insp_Systems: Authorization of Extended Inspection Systems**

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

4.3 Rationale

Table 3 provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OD.Assurance	OD.Material	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System
T.Chip-ID				x	x															x
T.Skimming			x																	
T.Read_Sensitive_Data				x												x				x
T.Forgery	x	x							x					x			x	x		
T.Counterfeit						x						x			x		x			
T.Abuse-Func							x													
T.Information_Leakage								x												
T.Phys-Tamper									x											
T.Malfunction										x										
P.Manufact											x	x								
P.Personalization	x										x		x							
P.Personal_Data		x	x																x	
P.Sensitive_Data				x												x				x
A.Pers_Agent													x							
A.Insp_Sys																	x		x	
A.Signature_PKI														x			x			
A.Auth_PKI																x				x

Table 3 – Security Objectives Rationale

The OSP **P.Manufact** “Manufacturing of the MRTD’s chip” requires the quality and integrity of the manufacturing process and control of the MRTD’s material in the Phase 2 Manufacturing including unique identification of the IC. The security objective for the TOE environment **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment” address these obligations of the IC Manufacturer and MRTD Manufacturer. **OD.Material** “Control over MRTD material” ensures that materials, equipment and tools used to produce genuine and authentic MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs.

The OSP **P.Personalization** “Personalization of the MRTD by Issuing State or Organization only” addresses:

- i. The writing of the Initialization Data and the writing of the Pre-personalization Data.
- ii. the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD”, and

- iii. the access control for the User Data and TSF Data as described by the security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD”.

Note, the manufacturer equips the TOE with the Personalization Agent Authentication keys according to **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment”. The security objective **OT.AC_Pers** limits the management of TSF Data to the Personalization Agent.

The OSP **P.Personal_Data** “Personal data protection policy” requires that the logical MRTD can be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an Inspection System. This OSP is covered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the Secure Messaging based on session keys agreed in this protocol. The security objective **OT.Data_Conf** requires the TOE to implement the Basic Access Control as defined by ICAO [R6] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The security objective **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD” requires the Inspection System to protect their communication with the TOE before Secure Messaging is successfully established based on the Chip Authentication Protocol. After successful Chip Authentication the security objective **OT.Data_Conf** “Confidentiality of personal data” ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System

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

The threat **T.Chip_ID** “Identification of MRTD’s chip” addresses the trace of the MRTD movement by identifying remotely the MRTD’s chip through the contactless communication interface. This threat is countered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the Secure Messaging based on session keys agreed in this protocol. The security objective **OT.Identification** “Identification and Authentication of the TOE” limits the TOE chip identification to the Basic Inspection System. The security objective **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD” requires the Inspection System to protect to their communication (as Basic Inspection System) with the TOE before Secure Messaging based on the Chip Authentication Protocol is successfully established. After successful Chip Authentication the security objective **OT.Data_Conf** “Confidentiality of personal data” ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System.

The threat **T.Skimming** “Skimming digital MRZ data or the digital portrait” addresses the reading of the logical MRTD through the contactless interface outside the communication between the MRTD’s chip and the Inspection System. This threat is countered by the security objective **OT.Data_Conf** “Confidentiality of personal data” through Basic Access Control allowing read data access only after successful authentication of the Basic Inspection System.

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

The threat **T.Counterfeit** “MRTD’s chip” addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** “Proof of MTRD’s chip authentication” using a authentication key pair generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Document Security Objects as demanded by OE.Auth_Key_MRTD “MRTD Authentication Key”. According to **OE.Exam_MRTD** “Examination of the MRTD passport book” the General Inspection System has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD’s chip. MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs targeted on by **OD.Material**.

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

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

The assumption **A.Pers_Agent** “Personalization of the MRTD’s chip” is covered by the security objective for the TOE environment **OE.Personalization** “Personalization of logical

MRTD” including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data and the enabling of security features of the TOE according to the decision of the Issuing State or Organization concerning the BAC.

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objectives for the TOE environment **OE.Exam_MRTD** “Examination of the MRTD passport book” which requires the Inspection System to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the authenticity of the presented MRTD’s chip. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD” require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

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

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

5. Extended Components Definition

This ST uses components defined as extensions to CC part 2 [R8]. Some of these components are defined in [R4], other components are defined in the protection profile [R5].

5.1 Definition of the family FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined in the PP [R5]. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The family “Audit data storage (FAU_SAS)” is specified in the following table.

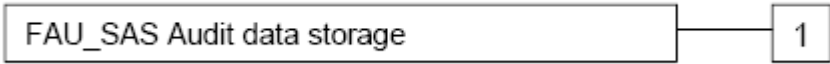
FAU_SAS Audit data storage	
<i>Family behavior:</i>	This family defines functional requirements for the storage of audit data.
<i>Component leveling:</i>	
FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
<i>Management</i>	There are no management activities foreseen.
<i>Audit</i>	There are no actions defined to be auditable.
FAU_SAS.1	Audit storage
<i>Hierarchical to:</i>	No other components
FAU_SAS.1.1	The TSF shall provide [assignment: <i>authorized users</i>] with the capability to store [assignment: <i>list of audit information</i>] in the audit records.
<i>Dependencies:</i>	No Dependencies.

Table 4 – Family FAU_SAS

5.2 Definition of the family FCS_RND

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined in the PP [R5]. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

The family “Generation of random numbers (FCS_RND)” is specified in the following table.

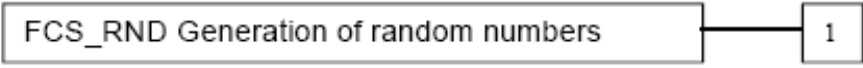
FCS_RND Generation of random numbers	
<i>Family behavior:</i>	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
<i>Component leveling:</i>	
FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
<i>Management:</i>	There are no management activities foreseen.
<i>Audit:</i>	There are no actions defined to be auditable.
FCS_RND.1	Quality metric for random numbers
<i>Hierarchical to:</i>	No other components
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: <i>a defined quality metric</i>].
<i>Dependencies:</i>	No Dependencies.

Table 5 – Family FCS_RND

5.3 Definition of the family FIA_API

To describe the security requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined in the PP [R5]. This family describes the functional requirements for the proof of a the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Application Note 17: *The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the CC part 2 (cf. [R9] "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.*

FIA_API Authentication Proof of Identity	
<i>Family behavior:</i>	This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.
<i>Component leveling:</i>	<div style="border: 1px solid black; padding: 5px; display: inline-block;"> FIA_API Authentication Proof of Identity </div> — <div style="border: 1px solid black; padding: 2px 5px; display: inline-block; margin-left: 10px;">1</div>
FIA_API.1	Authentication Proof of Identity.
<i>Management:</i>	The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
<i>Audit:</i>	There are no actions defined to be auditable.
FIA_API.1	Authentication Proof of Identity
<i>Hierarchical to:</i>	No other components
FIA_API.1.1	The TSF shall provide a [assignment: <i>authentication mechanism</i>] to prove the identity of the [assignment: <i>authorized user or rule</i>].
<i>Dependencies:</i>	No Dependencies.

Table 6 – Family FIA_API

5.4 Definition of the family FMT_LIM

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

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

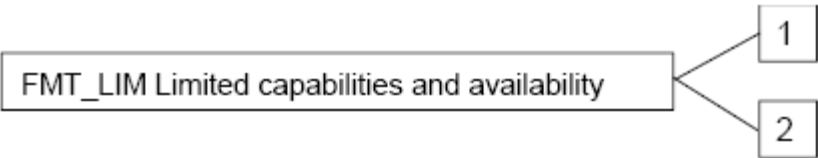
FMT_LIM Limited capabilities and availability	
<i>Family behavior:</i>	This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.
<i>Component leveling:</i>	
FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
<i>Management:</i>	There are no management activities foreseen.
<i>Audit:</i>	There are no actions defined to be auditable.
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.
<i>Management:</i>	There are no management activities foreseen.
<i>Audit:</i>	There are no actions defined to be auditable.

Table 7 – Family FMT_LIM

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

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

FMT_LIM.1	Limited capabilities
<i>Hierarchical to:</i>	No other components
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: <i>Limited capability and availability policy</i>].
<i>Dependencies:</i>	FMT_LIM.2 Limited availability.

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2	Limited capabilities
<i>Hierarchical to:</i>	No other components
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: <i>Limited capability and availability policy</i>].
<i>Dependencies:</i>	FMT_LIM.1 Limited capabilities.

Application Note 18: *the functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that*

- *the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced*

or conversely

- *the TSF is designed with high functionality but is removed or disabled in the product in its user environment.*

The combination of both requirements shall enforce the policy.

5.5 Definition of the family FPT_EMSEC

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in the PP [R5] to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [R8].

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

FPT_EMSEC	
<i>Family behavior:</i>	This family defines requirements to mitigate intelligible emanations.
<i>Component leveling:</i>	<div style="border: 1px solid black; padding: 5px; display: inline-block;"> FPT_EMSEC TOE emanation 1 </div>
FPT_EMSEC.1	TOE emanation has two constituents: <ul style="list-style-type: none"> FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF Data or User Data. FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF Data or User Data.
<i>Management:</i>	There are no management activities foreseen.
<i>Audit:</i>	There are no actions defined to be auditable.
FPT_EMSEC.1	TOE Emanation
<i>Hierarchical to:</i>	No other components
FPT_EMSEC.1.1	The TOE shall not emit [assignment: <i>types of emissions</i>] in excess of [assignment: <i>specified limits</i>] enabling access to [assignment: <i>list of types of TSF Data</i>] and [assignment: <i>list of types of User Data</i>].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: <i>type of users</i>] are unable to use the following interface [assignment: <i>type of connection</i>] to gain access to [assignment: <i>list of types of TSF Data</i>] and [assignment: <i>list of types of User Data</i>].
<i>Dependencies:</i>	No dependencies.

Table 8 – Family FPT_EMSEC

6. Security Requirements

6.1 Security Functional Requirements for the TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

6.1.1 Class FAU Security Audit

6.1.1.1 FAU_SAS.1 Audit storage

The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below (CC part 2).

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1	The TSF shall provide <u>the Manufacturer</u> ¹ with the capability to store <u>the IC Identification Data</u> ² in the audit records.
-------------	--

Dependencies: No dependencies.

Application Note 19: *The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD Manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD’s chip (see FMT_MTD.1/INI_DIS). The security measures in the manufacturing environment assessed under AGD_PRE and ALC_DEL ensure that the audit records will be used to fulfil the security objective OD.Assurance.*

6.1.2 Class Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 Cryptographic key generation

The TOE shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (CC 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/KDF_MRTD Cryptographic key generation – Key Derivation Function by the MRTD

Hierarchical to: No other components.

¹ [assignment: *authorised user*]

² [assignment: *list of audit information*]

FCS_CKM.1.1/ KDF_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>Document Basic Access Key Derivation Algorithm</u> ³ and specified cryptographic key sizes <u>112 bit</u> ⁴ that meet the following: [R17], <u>Annex E</u> ⁵ .
--------------------------	--

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

FCS_CKM.1/CPS_MRTD Cryptographic key generation – Generation of CPS session Keys for Initialization and Personalization by the TOE

Hierarchical to: No other components.

FCS_CKM.1.1/ CPS_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>CPS Keys Generation Algorithm</u> ⁶ and specified cryptographic key sizes <u>112 bit</u> ⁷ that meet following: [R10], <u>section 5.2</u> ⁸
--------------------------	---

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

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

Hierarchical to: No other components.

³ [assignment: *cryptographic key generation algorithm*]

⁴ [assignment: *cryptographic key sizes*]

⁵ [assignment: *list of standards*]

⁶ [assignment: *cryptographic key generation algorithm*]

⁷ [assignment: *cryptographic key sizes*]

⁸ [assignment: *list of standards*]

FCS_CKM.1.1/ DH_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: <u>Diffie-Hellman as defined in the RSA PKCS#3 technical note [R25]</u> ⁹ and specified cryptographic key <u>having bit length of the modulus equal to or shorter than 2048 and bit length of the exponent equal to or shorter than 2048</u> ¹⁰ that meet the following: [R6], <u>Annex A.1</u> ¹¹ .
-------------------------	--

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

6.1.2.2 FCS_CKM.4 Cryptographic key destruction

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (CC part 2).

FCS_CKM.4/MRTD Cryptographic key destruction - MRTD

Hierarchical to: No other components.

FCS_CKM.4.1/ MRTD	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: <u>physical deletion by overwriting the memory data with zeros</u> ¹² that meets the following: <u>none</u> ¹³ .
----------------------	--

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]

6.1.2.3 FCS_COP.1 Cryptographic operation

The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (CC part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

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

⁹ [assignment: *cryptographic key generation algorithm*]

¹⁰ [assignment: *cryptographic key sizes*]

¹¹ [assignment: *list of standards*]

¹² [assignment: *cryptographic key destruction method*]

¹³ [assignment: *list of standards*]

Hierarchical to: No other components.

FCS_COP.1.1/
SHA_MRTD

The TSF shall perform hashing¹⁴ in accordance with a specified cryptographic algorithm **SHA-1, SHA-256**¹⁵ and cryptographic key sizes none¹⁶ that meet the following: FIPS 180-2 [R12]¹⁷.

Dependencies: [FDP_ITC.1 Import of User Data without security attributes, or
FDP_ITC.2 Import of User Data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

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

Hierarchical to: No other components.

FCS_COP.1.1/
TDES_MRTD

The TSF shall perform Secure Messaging – encryption and decryption¹⁸ in accordance with a specified cryptographic algorithm TDES in CBC mode¹⁹ and cryptographic key sizes 112 bit²⁰ that meet the following: FIPS 46-3 [R11] and Annex E of TR-PKI [R17]²¹.

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

Application Note 20: *This SFR requires the TOE to implement the cryptographic primitive for Secure Messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of*

- i. the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/KDF_MRTD or*
- ii. the Chip Authentication Protocol according to the FCS_CKM.1/DH_MRTD.*

¹⁴ [assignment: *list of cryptographic operations*]

¹⁵ [assignment: *criptographic algorithm*]

¹⁶ [assignment: *cryptographic key sizes*]

¹⁷ [assignment: *list of standards*]

¹⁸ [assignment: *list of cryptographic operations*]

¹⁹ [assignment: *cryptographic algorithm*]

²⁰ [assignment: *cryptographic key sizes*]

²¹ [assignment: *list of standards*]

Note that encryption is also used to check the authentication attempt of a terminal as Personalization Agent by means of the related symmetric authentication mechanism.

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_MRTD	The TSF shall perform <u>Secure Messaging – message authentication code</u> ²² in accordance with a specified cryptographic algorithm <u>Retail MAC</u> ²³ and cryptographic key sizes <u>112 bit</u> ²⁴ that meet the following: <u>ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [R20]</u> ²⁵ .
--------------------------	--

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

Application Note 21: *This SFR requires the TOE to implement the cryptographic primitive for Secure Messaging with encryption and message authentication code over the transmitted data. The keys are agreed between the TOE and the terminal as part of:*

- i. *the BAC Authentication Mechanism according to the FCS_CKM.1/KDF_MRTD or*
- ii. *the Chip Authentication Protocol according to the FCS_CKM.1/DH_MRTD.*

Note that the Retail MAC computation is also used to check the authentication attempt of a terminal as Personalization Agent by means of the related symmetric authentication mechanism.

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

Hierarchical to: No other components.

FCS_COP.1.1/SIG_VER	The TSF shall perform <u>digital signature verification</u> ²⁶ in accordance with a specified cryptographic algorithm <u>RSA as specified in Table 9</u> ²⁷ and cryptographic key <u>having bit length of the modulus equal to 1024, 1280, 1536 or 2048</u> ²⁸
---------------------	---

²² [assignment: list of cryptographic operations]

²³ [assignment: cryptographic algorithm]

²⁴ [assignment: cryptographic key sizes]

²⁵ [assignment: list of standards]

²⁶ [assignment: list of cryptographic operations]

²⁷ [assignment: list of cryptographic operations]

²⁸ [assignment: cryptographic key sizes]

	that meet the following: <u>RSA PKCS#1 technical note [R33]</u> ²⁹
--	--

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

OID	Signature	Hash	Parameters
id-TA-RSA-v1-5-SHA-1	RSASSA-PKCS1-v1_5	SHA-1	N/A
id-TA-RSA-v1-5-SHA-256	RSASSA-PKCS1-v1_5	SHA-256	N/A
id-TA-RSA-PSS-SHA-1	RSASSA-PSS	SHA-1	Default
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	Default

Table 9 - Object Identifiers for Terminal Authentication with RSA

Application Note 22: *The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.*

6.1.2.4 FCS_RND.1 Quality metrics for random numbers

The TOE shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (CC part 2 extended).

FCS_RND.1/MRTD Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1/MRTD	The TSF shall provide a mechanism to generate random numbers that meet <u>requirements that depend on the IC used by the TOE. For a specification of those requirements please refer to Appendix A</u> ³⁰ .
------------------	---

Dependencies: No dependencies.

²⁹ [assignment: list of standards]

³⁰ [assignment: a defined qualità metric]

Application Note 23: *This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4/MRTD.*

6.1.3 Class FIA Identification and Authentication

6.1.3.1 FIA_UID.1 Timing of identification

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

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1	<p>The TSF shall allow</p> <ol style="list-style-type: none"> 1. <u>to establish the communication channel,</u> 2. <u>to read the initialization data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS³¹</u> <p>on behalf of the user to be performed before the user is identified.</p>
FIA_UID.1.2	<p>The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.</p>

Dependencies: No dependencies.

Application Note 24: *The MRTD’s chip and the terminal establish the communication channel through the contactless interface. The Protocol Type A defines an “Answer to Select” (ATS) and the protocol Type B is managed through the commands “Answer to Request” and “Answer to Attrib”. Note that the terminal and the MRTD’s chip use an identifier for the communication channel to allow the terminal for communication with more than one RFID. Historical bytes are not used to avoid possible exploitation of the threat T.Chip_Id in particular contexts (e.g. in the case a MRTD holder has a chip manufactured by a local manufacturer, he could be traced in a foreign country where few holders could have the same ATS content). Therefore, the ATS cannot contain any chip identifying data.*

Application Note 25: *In the “operational use” phase the MRTD must not allow anybody to read the IC Chip Serial Number (ICCSN) or any other unique identification (cf. T.Chip_ID) before the successful authentication as BIS. Note that the terminal and the MRTD’s chip use an identifier (UID) for the communication channel to allow the terminal for communication with more than one RFID. This identifier is randomly selected, so it will not violate the OT.Identification.*

Application Note 26: *In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer may create*

³¹ [assignment: list of TSF-mediated actions]

the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD” by storing the Personalization Keys in the MRTD non-volatile memory. The users in the role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as the default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System. After successful authentication as Basic Inspection System the terminal may identify themselves as Extended Inspection System by selection of the templates for the Terminal Authentication Protocol.

6.1.3.2 FIA_UAU.1 Timing of authentication

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1	<p>The TSF shall allow</p> <ol style="list-style-type: none"> 1. <u>to establish the communication channel,</u> 2. <u>to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,</u> 3. <u>to identify themselves by selection of the authentication key</u>³². <p>on behalf of the user to be performed before the user is authenticated.</p>
FIA_UAU.1.2	<p>The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.</p>

Dependencies: FIA_UID.1 Timing of identification.

6.1.3.3 FIA_UAU.4 Single-use authentication mechanisms

The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (CC part 2).

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

Hierarchical to: No other components.

³² [assignment: list of TSF-mediated actions]

FIA_UAU.4.1/MRTD	<p>The TSF shall prevent reuse of authentication data related to</p> <ol style="list-style-type: none"> 1. <u>BAC Authentication Mechanism,</u> 2. <u>Terminal Authentication Protocol,</u> 3. <u>Authentication Mechanism based on TDES</u>³³.
------------------	---

Dependencies: No dependencies.

Application Note 27: *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 BAC Authentication Mechanism, the Terminal Authentication Protocol and the Authentication Mechanism based on TDES uses the RND.ICC challenge [R17].*

Application Note 28: *The BAC Mechanism is a mutual device authentication mechanism defined in TR-PKI [R17]. In the first step the terminal authenticates itself to the MRTD’s chip and the MRTD’s chip authenticates to the terminal in the second step. In the first step the TOE sends a randomly chosen challenge which shall contain sufficient entropy to prevent T.Chip_ID. In this second step the MRTD’s chip provides the terminal with a challenge-response-pair which 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.*

6.1.3.4 FIA_UAU.5 Multiple authentication mechanisms

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (CC part 2).

FIA_UAU.5/MRTD Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1/MRTD	<p>The TSF shall provide</p> <ol style="list-style-type: none"> 1. <u>BAC Authentication Mechanism,</u> 2. <u>Terminal Authentication Protocol,</u> 3. <u>Secure Messaging in MAC-ENC mode,</u> 4. <u>Symmetric Authentication Mechanism based on TDES</u>³⁴ <p>to support user authentication.</p>
------------------	--

³³ [assignment: *identified authentication mechanisms*]

³⁴ [assignment: *list of multiple authentication mechanisms*]

<p>FIA_UAU.5.2/ MRTD</p>	<p>The TSF shall authenticate any user's claimed identity according to the following rules:</p> <ol style="list-style-type: none"> 1. <u>the TOE accepts the authentication attempt as MRTD Manufacturer by one of the following mechanisms:</u> <ol style="list-style-type: none"> (a) <u>the Basic Access Control Authentication Mechanism with MRTD Manufacturer Keys</u> (b) <u>the Symmetric Authentication Mechanism with the MRTD Manufacturer Keys (K_{MM})</u> (c) <u>the Terminal Authentication Protocol with MRTD Manufacturer Keys.</u> 2. <u>the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms:</u> <ol style="list-style-type: none"> (a) <u>the Basic Access Control Authentication Mechanism with Personalization Agent Keys</u> (b) <u>the Symmetric Authentication Mechanism with the Personalization Agent Keys (K_{PA})</u> (c) <u>the Terminal Authentication Protocol with Personalization Agent Keys.</u> 3. <u>the TOE accepts the authentication attempt as BIS only by means of the BAC Authentication Mechanism with the Document Basic Access Keys.</u> 4. <u>After successful authentication as BIS and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of Secure Messaging with the key agreed upon with the authenticated terminal by means of the BAC Authentication Mechanism.</u> 5. <u>After run of the Chip Authentication Mechanism the TOE accepts only received commands with correct message authentication code sent by means of Secure Messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.</u> 6. <u>The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses Secure Messaging established by the Chip Authentication Mechanism³⁵</u>
------------------------------	---

Dependencies: No dependencies.

Application Note 29: *The Basic Access Control Mechanism includes the Secure Messaging for all commands exchanged after successful authentication of the Inspection System. The MRTD Manufacturer and the Personalization Agent may use Symmetric Authentication Mechanism without Secure Messaging mechanism as well if the*

³⁵ [assignment: rules describing how the multiple authentication mechanisms provide authentication]

personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the Secure Messaging after the mutual authentication. The General Inspection System shall use the Secure Messaging with the keys generated by the Chip Authentication Mechanism. In the operational use phase a BAC authentication is required to an Inspection System wanting to read TOE identification data.

6.1.3.5 FIA_UAU.6 Re-authenticating

The TOE shall meet the requirement “Re-authenticating (FIA_UAU.6)” as specified below (CC part 2).

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

Hierarchical to: No other components.

FIA_UAU.6.1/ MRTD	The TSF shall re-authenticate the user under the conditions <ol style="list-style-type: none"><li data-bbox="491 860 1406 1039">1. <u>Each command sent to the TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS.</u><li data-bbox="491 1046 1406 1151">2. <u>Each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS³⁶.</u>
----------------------	---

Dependencies: No dependencies.

Application Note 30: *The BAC Mechanism and the Chip Authentication Protocol specified in TR-PKI [R17] 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-authenticates the user for each received command and accepts only those commands received from the initially authenticated user.*

6.1.3.6 FIA_AFL.1 Authentication failures

The TOE shall meet the requirement “Authentication failures (FIA_AFL.1)” as specified below (CC part 2).

FIA_AFL.1 Authentication failure handling

³⁶ [assignment: list of conditions under which re-authentication is required]

Hierarchical to: No other components.

FIA_AFL.1.1	The TSF shall detect when a defined number of consecutive ³⁷ unsuccessful authentication attempts occur related to the authentication events specified in column 1 of Table 10 ^{38, 39} .
FIA_AFL.1.2	When the defined number of consecutive unsuccessful authentication attempts has been met ⁴⁰ , the TSF shall perform the actions specified in column 2 of Table 10 ⁴¹ .

Refinement: refer to Table 10.

Column 1 Assignment: Authentication Events	Column 2 Assignment: Actions
Unsuccessful BAC authentication	The outcome of the authentication is issued with a delay, in order to prevent brute-force attacks.
Unsuccessful MAC verification after BAC authentication	Session closed
Unsuccessful MAC verification after Chip Authentication	Session closed
Unsuccessful MAC verification after Terminal Authentication	Session closed
Unsuccessful Terminal Authentication due to application error (such as key import failure or signature verification failure)	Access to sensitive biometric data denied
Unsuccessful mutual authentication with MRTD Manufacturer keys	MRTD Manufacturer keys blocked
Unsuccessful mutual authentication with Personalization Agent keys	Personalization Agent keys blocked

Table 10 – FIA_AFL.1 Refinement

Dependencies: FIA_UAU.1 Timing of authentication

6.1.3.7 FIA_API.1/CAP Authentication Proof of Identity – MRTD

The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1(CAP))” as specified below (CC part 2 extended).

FIA_API.1/CAP Authentication Proof of Identity - MRTD

³⁷ [assignment: positive integer number]

³⁸ [assignment: list of authentication events]

³⁹ [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

⁴⁰ [selection: *met, surpassed*]

⁴¹ [assignment: *list of actions*]

Hierarchical to: No other components.

FIA_API.1.1/CAP	The TSF shall provide a <u>Chip Authentication Protocol according to [R6]</u> ⁴² to prove the identity of the <u>TOE</u> ⁴³ .
-----------------	---

Dependencies: No dependencies.

Application Note 31: *This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [R6]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol DH and two session keys for Secure Messaging in ENC_MAC mode according to [R17], Annex E.1. The terminal verifies by means of Secure Messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication key stored in EF.DG14.*

6.1.4 Class FDP User Data Protection

6.1.4.1 FDP_ACC.1 Subset access control

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (CC part 2).

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1	The TSF shall enforce the <u>Access Control SFP</u> ⁴⁴ on <u>terminals gaining write, read and modification access in the EF.COM, EF.SOD, EF.DG1 to EF.DG13, EF.DG16</u> of the logical <u>MRTD</u> ⁴⁵ .
-------------	--

Dependencies: FDP_ACF.1 Security attribute based access control

Application Note 32: *The BAC SFP addresses the configuration of the TOE for usage with BIS's only.*

6.1.4.2 FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1 Security attribute based access control

⁴² [assignment: *authentication mechanism*]

⁴³ [assignment: *authorized user or rule*]

⁴⁴ [assignment: *access control SFP*]

⁴⁵ [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Hierarchical to: No other components.

<p>FDP_ACF.1.1</p>	<p>The TSF shall enforce the <u>Access Control SFP</u>⁴⁶ to objects based on the following:</p> <ol style="list-style-type: none"> 1. <u>Subjects:</u> <ol style="list-style-type: none"> a. <u>Personalization Agent,</u> b. <u>Basic Inspection System,</u> c. <u>Extended Inspection System</u> d. <u>Terminal,</u> 2. <u>Objects:</u> <ol style="list-style-type: none"> a. <u>data EF.DG1 to EF.DG14, EF.DG16 of the logical MRTD,</u> b. <u>data in EF.COM,</u> c. <u>data in EF.SOD,</u> 3. <u>Security attributes:</u> <ol style="list-style-type: none"> a. <u>authentication status of terminals,</u> b. <u>Terminal Authorization</u>⁴⁷.
<p>FDP_ACF.1.2</p>	<p>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:</p> <ol style="list-style-type: none"> 1. <u>the successfully authenticated Personalization Agent is allowed to write the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG14, EF.DG16 of the logical MRTD,</u> 2. <u>the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG14, EF.DG16 of the logical MRTD,</u> 3. <u>the successfully authenticated Extended Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG14, EF.DG16 of the logical MRTD,</u> 4. <u>the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG3 according to the Terminal Authorization,</u> 5. <u>the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG4 according to the Terminal Authorization</u>⁴⁸

⁴⁶ [assignment: *access control SFP*]

⁴⁷ [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u> ⁴⁹ .
FDP_ACF.1.4	<p>The TSF shall explicitly deny access of subjects to objects based on the rule:</p> <ol style="list-style-type: none"> 1. <u>A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,</u> 2. <u>A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,</u> 3. <u>A terminal authenticated as DV is not allowed to read data in the EF.DG3,</u> 4. <u>A terminal authenticated as DV is not allowed to read data in the EF.DG4,</u> 5. <u>Any Terminal is not allowed to modify any of the EF.DG1 to EF.DG14, EF.DG16 of the logical MRTD</u>⁵⁰

Hierarchical to: No other components.

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

Application Note 33: *The TOE verifies the certificate chain established by the Country Verifier Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifier Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.*

6.1.4.3 FDP_UCT.1 Basic data exchange confidentiality

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

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

⁴⁸ [assignment: rules governing access among controlled subjects and controlled objects using controlled operations or controlled objects]

⁴⁹ [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

⁵⁰ [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FDP_UCT.1.1/MRTD	The TSF shall enforce the <u>Access Control SFP</u> ⁵¹ to be able to <u>transmit and receive</u> ⁵² User Data in a manner protected from unauthorized disclosure after Chip Authentication .
------------------	---

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

6.1.4.4 FDP_UIT.1 Basic data exchange integrity

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

FDP_UIT.1/MRTD Data exchange integrity - MRTD

Hierarchical to: No other components.

FDP_UIT.1.1/MRTD	The TSF shall enforce the <u>Access Control SFP</u> ⁵³ to be able to <u>transmit and receive</u> ⁵⁴ User Data in a manner protected from <u>modification, deletion, insertion and replay</u> ⁵⁵ errors after Chip Authentication .
FDP_UIT.1.2/MRTD	The TSF shall be able to determine on receipt of User Data, whether <u>modification, deletion, insertion and replay</u> ⁵⁶ has occurred after Chip Authentication .

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

Application Note 34: *FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the protection of the User Data transmitted from the TOE to the terminal by Secure Messaging with encryption and message authentication codes after successful Chip Authentication to the General Inspection System. The authentication mechanism as part of Basic Access Control Mechanism and the Chip Authentication Protocol establish different key sets to be used for Secure Messaging (each set of keys for the encryption and the message authentication key).*

⁵¹ [assignment: access control SFP(s) and/or information flow control SFP(s)]

⁵² [selection: transmit, receive]

⁵³ [assignment: access control SFP(s) and/or information flow control SFP(s)]

⁵⁴ [selection: transmit, receive]

⁵⁵ [selection: modification, deletion, insertion, replay]

⁵⁶ [selection: modification, deletion, insertion, replay]

6.1.5 Class FMT Security Management

Application Note 35: *The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF Data.*

6.1.5.1 FMT_SMF.1 Specification of Management Functions

The TOE shall meet the requirement “Specification of Management Functions (FMT_SMF.1)” as specified below (CC part 2).

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: <ol style="list-style-type: none">1. <u>Initialization</u>,2. <u>Personalization</u>,3. <u>Configuration</u>⁵⁷.
-------------	---

Dependencies: No Dependencies

6.1.5.2 FMT_SMR.1 Security roles

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below (CC part 2).

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1	The TSF shall maintain the roles: <ol style="list-style-type: none">1. <u>Manufacturer</u>2. <u>Personalization Agent</u>3. <u>Country Verifier Certification Authority</u>4. <u>Documents Verifier</u>5. <u>Basic Inspection System</u>6. <u>domestic Extended Inspection System</u>7. <u>foreign Extended Inspection System</u>⁵⁸.
-------------	--

⁵⁷ [assignment: *list of security management functions to be provided by the TSF*]

⁵⁸ [assignment: *the authorised identified roles*]

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

Hierarchical to: FIA_UID.1 Timing of identification.

Application Note 36: *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.*

6.1.5.3 FMT_LIM.1 Limited capabilities

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below (CC part 2 extended).

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

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: <u>Deploying Test Features after TOE Delivery does not allow:</u> <ol style="list-style-type: none"><u>User Data to be disclosed or manipulated,</u><u>TSF Data to be disclosed or manipulated,</u><u>software to be reconstructed and</u><u>substantial information about construction of TSF to be gathered which may enable other attacks</u>⁵⁹.
-------------	---

Dependencies: FMT_LIM.2 Limited availability.

6.1.5.4 FMT_LIM.2 Limited availability

The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below (CC part 2 extended).

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

⁵⁹ [assignment: limited capability and availability policy]

FMT_LIM.2.1	<p>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: <u>Deploying Test Features after TOE Delivery does not allow:</u></p> <ol style="list-style-type: none"> 1. <u>User Data to be disclosed or manipulated,</u> 2. <u>TSF Data to be disclosed or manipulated,</u> 3. <u>software to be reconstructed and</u> 4. <u>substantial information about construction of TSF to be gathered which may enable other attacks⁶⁰.</u>
-------------	---

Dependencies: FMT_LIM.1 Limited capabilities.

Application Note 37: *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.*

6.1.5.5 FMT_MTD.1 Management of TSF Data

The TOE shall meet the requirement “Management of TSF Data (FMT_MTD.1)” as specified below (CC part 2). The iterations address different management functions and different TSF Data.

FMT_MTD.1/INI_ENA Management of TSF Data – Writing of Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

FMT_MTD.1.1/ INI_ENA	<p>The TSF shall restrict the ability to <u>write⁶¹ the Initialization Data and Pre-personalization Data⁶² to the Manufacturer⁶³.</u></p>
-------------------------	--

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

Application Note 38: *The pre-personalization Data includes but is not limited to*

- i. *the authentication reference data for the Personalization Agent, which is the symmetric cryptographic Personalization Agent Authentication Keys (K_{PA})*

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

Hierarchical to: No other components.

⁶⁰ [assignment: *limited capability and availability policy*]

⁶¹ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

⁶² [assignment: *list of TSF Data*]

⁶³ [assignment: *the authorised identified roles*]

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to <u>disable read access for users</u> ⁶⁴ to the <u>Initialization Data</u> ⁶⁵ to <u>the MRTD Manufacturer</u> ⁶⁶ .
-------------------------	---

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/CVCA_INI	The TSF shall restrict the ability to <u>write</u> ⁶⁷ the: 1. <u>initial Country Verifying Certification Authority Public Key</u> , 2. <u>initial Country Verifying Certification Authority CAR</u> ⁶⁸ , 3. <u>initial current date</u> ⁶⁹ to <u>the Personalization Agent</u> ⁷⁰ .
----------------------	--

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/CVCA_UPD	The TSF shall restrict the ability to <u>update</u> ⁷¹ the: 1. <u>Country Verifying Certification Authority Public Key</u> , 2. <u>Country Verifying Certification Authority CAR</u> ⁷²⁷³ , to <u>Country Verifying Certification Authority</u> ⁷⁴ .
----------------------	--

⁶⁴ [selection: *change_default, query, modify, dolete, clear*, [assignment: *other operations*]]

⁶⁵ [assignment: *list of TSF Data*]

⁶⁶ [assignment: *the authorised identified roles*]

⁶⁷ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁶⁸ CAR: Certificate Authority Reference

⁶⁹ [assignment: *list of TSFdata*]

⁷⁰ [assignment: *the authorised identified roles*]

⁷¹ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁷² CAR: Certificate Authority Reference

⁷³ [assignment: *list of TSF Data*]

⁷⁴ [assignment: *the authorised identified roles*]

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

Application Note 39: *The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key by means of the Country Verifying CA Link-Certificates (cf. [R6], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifier CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [R6], sec. 2.2.3 and 2.2.4).*

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

Hierarchical to: No other components.

FMT_MTD.1.1/DATE	The TSF shall restrict the ability to <u>modify</u> ⁷⁵ the <u>current date</u> ⁷⁶ to: <ol style="list-style-type: none">1. <u>Country Verifying Certification Authority</u>,2. <u>Document Verifier</u>,3. <u>domestic Extended Inspection System</u>⁷⁷
------------------	---

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

Application Note 40: *The authorized roles are identified in their certificate (cf. [R6], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [R6], Annex A.3.3, for details).*

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

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to <u>write</u> ⁷⁸ the <u>Document Basic Access Keys</u> ⁷⁹ to the <u>Personalization Agent</u> ⁸⁰ .
---------------------------	--

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

⁷⁵ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁷⁶ [assignment: *list of TSF Data*]

⁷⁷ [assignment: *the authorised identified roles*]

⁷⁸ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁷⁹ [assignment: *list of TSF Data*]

⁸⁰ [assignment: *the authorised identified roles*]

FMT_MTD.1/ADDTSF_WRITE Management of TSF Data – Additional TSF Data Write

Hierarchical to: No other components.

FMT_MTD.1.1/ ADDTSF_WRITE	The TSF shall restrict the ability to <u>write</u> the Security Environment and the Document Number to the <u>Personalization Agent</u> ⁸¹ .
------------------------------	---

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

Application Note 41: *The Country Verifying Certification Authority Public Key is the TSF Data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.*

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

Hierarchical to: No other components.

FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to <u>create and load</u> ⁸² the <u>Chip Authentication Private Key</u> ⁸³ to <u>the Manufacturer</u> ⁸⁴
----------------------	--

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

Application Note 42: *The verb “load” means here that the Chip Authentication private Key is generated securely outside the TOE and written into the TOE memory.*

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

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to <u>read</u> ⁸⁵ : 1. <u>the Document Basic Access Keys,</u> 2. <u>the Chip Authentication Private key,</u> 3. <u>the Personalization Agent Keys</u> ⁸⁶
-----------------------	--

⁸¹ [assignment: *the authorised identified roles*]

⁸² [selection: *create, load*]

⁸³ [assignment: *list of TSF Data*]

⁸⁴ [assigned: *the authorised identified roles*]

	to <u>none</u> ⁸⁷ .
--	--------------------------------

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.*

6.1.5.6 FMT_MTD.3 Secure TSF Data

The TOE shall meet the requirement “Secure TSF Data (FMT_MTD.3)” as specified below (CC part 2).

FMT_MTD.3 Secure TSF Data

Hierarchical to: No other components.

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

Dependencies: FMT_MTD.1 Management of TSF Data

Refinement: The certificate chain is valid if and only if :

1. **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**
2. **the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,**
3. **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.**

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

⁸⁵ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

⁸⁶ [assignment: *list of TSF Data*]

⁸⁷ [assignment: *the authorised identified roles*]

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

6.1.6 Class FPT Protection of the Security Functions

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

6.1.6.1 FPT_EMSEC.1 TOE emanation

The TOE shall meet the requirement “TOE emanation (FPT_EMSEC.1)” as specified below (CC part 2 extended):

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

<p>FPT_EMSEC.1.1</p>	<p>The TOE shall not emit electromagnetic and current emissions⁸⁸ in excess of intelligible threshold⁸⁹ enabling access to:</p> <ol style="list-style-type: none"> 1. MRTD Manufacturer Authentication Keys, 2. Personalization Agent Authentication Keys, 3. Document Basic Access Keys, 4. Chip Authentication Private Key⁹⁰ <p>and:</p> <ol style="list-style-type: none"> 1. EF.DG1 to EF.DG14, EF.DG16, 2. EF.SOD, 3. EF.COM⁹¹
<p>FPT_EMSEC.1.2</p>	<p>The TSF shall ensure any unauthorised users⁹² are unable to use the following interface smart card circuits contacts⁹³ to gain access to:</p> <ol style="list-style-type: none"> 5. MRTD Manufacturer Authentication Keys, 6. Personalization Agent Authentication Keys, 7. Document Basic Access Keys, 8. Chip Authentication Private Key⁹⁴ <p>and:</p> <ol style="list-style-type: none"> 4. EF.DG1 to EF.DG14, EF.DG16, 5. EF.SOD, 6. EF.COM⁹⁵

Dependencies: No other components.

6.1.6.2 FPT_FLS Failure with preservation of secure state

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

The TOE shall meet the requirement “Failure with preservation of secure state (FPT_FLS.1)” as specified below (CC part 2).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

⁸⁸ [assignment: *type of emissions*]

⁸⁹ [assignment: *specified limits*]

⁹⁰ [assignment: *list of types of TSF Data*]

⁹¹ [assignment: *list of types of User Data*]

⁹² [assignment: *type of users*]

⁹³ [assignment: *type of connection*]

⁹⁴ [assignment: *list of types of TSF Data*]

⁹⁵ [assignment: *list of types of User Data*]

FPT_FLS.1.1	<p>The TSF shall preserve a secure state when the following types of failures occur:</p> <ol style="list-style-type: none"> 1. <u>exposure to operating conditions where therefore a malfunction could occur,</u> 2. <u>failure detected by TSF according to FPT_TST.1⁹⁶</u>
-------------	---

Dependencies: No dependencies

6.1.6.3 FPT_TST.1 TSF testing

The TOE shall meet the requirement “TSF testing (FPT_TST.1)” as specified below (CC part 2).

FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1	<p>The TSF shall run a suite of self tests <u>during initial start-up, and before any use of TSF Data</u>⁹⁷ to demonstrate the correct operation of the TSF.</p>
FPT_TST.1.2	<p>The TSF shall provide authorized users with the capability to verify the integrity of TSF Data.</p>
FPT_TST.1.3	<p>The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.</p>

Dependencies: No dependencies.

6.1.6.4 FPT_PHP.3 Resistance to physical attack

The TOE shall meet the requirement “Resistance to physical attack (FPT_PHP.3)” as specified below (CC part 2).

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1	<p>The TSF shall resist <u>physical manipulation and physical probing</u>⁹⁸ to the <u>TSF</u>⁹⁹ by responding automatically such that the TSP is not violated.</p>
-------------	--

Dependencies: No dependencies.

⁹⁶ [assignment: list of types of failures in the TSF]

⁹⁷ [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which sel test should occur]]

⁹⁸ [assignment: physical tampering scenarios]

⁹⁹ [assignment: list of TSF devices/elements]

6.2 Security Assurance Requirements for the TOE

The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following components:

ALC_DVS.2 and AVA_VAN.5

Table 11 summarizes the assurance components that define the security assurance requirements for the TOE.

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1
ASE	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.5

Table 11 –Assurance requirements at EAL4+

All the Assurance Requirements are fully defined in the Common Criteria v3.1 revision 3 part 3 documentation [R9].

6.3 Security Requirements Rationale

6.3.1 Security functional requirements rationale

Table 12 provides an overview for security functional requirements coverage of security objectives.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1					x					
FCS_CKM.1/KDF_MRTD	x	x	x	x		x				
FCS_CKM.1/DH_MRTD	x	x		x		x				
FCS_CKM.1/CPS_MRTD	x	x								
FCS_CKM.4/MRTD	x	x	x	x						
FCS_COP.1/SHA_MRTD	x	x	x	x		x				

FCS_COP.1/TDES_MRTD	x	x	x			x				
FCS_COP.1/MAC_MRTD	x	x	x	x		x				
FCS_COP.1/SIG_VER	x			x						
FCS_RND.1/MRTD	x			x						
FIA_UID.1	x	x	x	x	x					
FIA_UAU.1	x	x	x	x	x					
FIA_UAU.4/MRTD	x	x	x	x						
FIA_UAU.5/MRTD	x	x	x	x						
FIA_UAU.6/MRTD	x	x	x	x						
FIA_AFL.1			x							
FIA_API.1/CAP						x				
FDP_ACC.1	x	x	x	x						
FDP_ACF.1	x	x	x	x						
FDP_UCT.1/MRTD			x	x						
FDP_UIT.1/MRTD		x		x						
FMT_SMF.1	x	x	x							
FMT_SMR.1	x	x	x							
FMT_LIM.1							x			
FMT_LIM.2							x			
FMT_MTD.1/INI_ENA					x					
FMT_MTD.1/INI_DIS					x					
FMT_MTD.1/CVCA_INI				x						
FMT_MTD.1/CVCA_UPD				x						
FMT_MTD.1/DATE				x						
FMT_MTD.1/KEY_WRITE	x		x							
FMT_MTD.1/ADDTSF_WRITE	x		x	x						
FMT_MTD.1/CAPK		x	x	x		x				
FMT_MTD.1/KEY_READ	x	x	x	x		x				
FMT_MTD.3				x						
FPT_EMSEC.1	x						x			
FPT_TST.1							x			x
FPT_FLS.1	x						x			x
FPT_PHP.3	x						x	x		

Table 12 – Security Objectives Coverage for the TOE by the SFR

6.3.1.1 OT.AC_Pers

The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD and the management of the TSF for Basic Access Control. The write access to the logical MRTD data are defined by the SFR FIA_UID.1, FIA_UAU.1, FDP_ACC.1 and FDP_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization).

The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control. The Personalization Agent also handles the security environment and the document number according to the SFR FMT_MTD.1/ADDTSF_WRITE.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD and FIA_UAU.5/MRTD. If the Basic Access Control Authentication Mechanism with the Personalization Agent Authentication Key is used the TOE will use the FCS_RND.1/MRTD (for the generation of the challenge), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode Secure Messaging) and FIA_UAU.6/MRTD (for the re-authentication). If the Personalization Terminal want to authenticate themselves to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1/MRTD (for the generation of the challenge), FCS_CKM.1/DH_MRTD, FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode Secure Messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6/MRTD (for the re-authentication). If the Personalization Terminal wants to authenticate themselves to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1/MRTD (for the generation of the challenge) and FCS_COP.1/TDES_MRTD (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use. The SFR FCS_CKM.1/CPS_MRTD allows to protect the transmitted data by means Secure Messaging during the initialization and personalization processes.

The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMSEC.1 the confidentiality of these keys.

6.3.1.2 OT.Data_Int

The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4).

The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing the logical LDS. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the Inspection System detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD. The SFR FIA_UAU.6/MRTD and FDP_UIT.1/MRTD requires the integrity protection of the transmitted data after chip authentication by means of Secure Messaging implemented by the cryptographic functions according to FCS_CKM.1/DH_MRTD (for the generation of the shared secret) , FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), FCS_CKM.1/CPS_MRTD (for the generation of the initialization and personalization keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the

ENC_MAC_Mode Secure Messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

6.3.1.3 OT.Data_Conf

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: only the successful authenticated Personalization Agent, Basic Inspection System and Extended Inspection System are allowed to read the data of the logical MRTD. The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys). The SFR FMT_MTD.1/KEY_WRITE and FMT_MTD.1/ADDTSF_WRITE address the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

The SFR FIA_AFL.1 strengthens the authentication function as terminal part of the BAC Authentication Protocol or other authentication functions where necessary. The SFR FIA_UAU.4/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5/MRTD enforces the TOE:

- i. to accept the authentication attempt as Basic Inspection System only by means of the BAC Authentication Mechanism with the Document Basic Access Keys and
- ii. to accept chip authentication only after successful authentication as Basic Inspection System.

Moreover, the SFR FIA_UAU.6/MRTD requests Secure Messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

After Chip Authentication the TOE and the General Inspection System establish protection of the communication by Secure Messaging (cfr. The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD) in ENC_MAC_Mode by means of the cryptographic functions according to FCS_CKM.1/DH_MRTD (for the generation of the shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode Secure Messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires the Chip Authentication Key cannot be written unauthorized or read afterwards.

The SFR FIA_AFL.1 addresses the actions that the TSF shall take in the case of authentication failure.

The Personalization Agent is not required to use Secure Messaging.

6.3.1.4 OT.Sens_Data_Conf

The security objective **OT.Sens_Data_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP_ACC.1 and FDP_ACF.1 allowing the data of EF.DG3 and EF.EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a validly verifiable certificate according FCS_COP.1/SIG_VER.

The SFR FIA_UID.1 and FIA_UAU.1 requires authentication of the Inspection Systems. The SFR FIA_UAU.5/MRTD requires the successful Chip Authentication before any authentication attempt as Extended Inspection System. The SFR FIA_UAU.6/MRTD and FDP_UCT.1/MRTD requires the confidentiality protection of the transmitted data after chip authentication by means of Secure Messaging implemented by the cryptographic functions according to FCS_RND.1/MRTD (for the generation of the terminal authentication challenge), FCS_CKM.1/DH_MRTD (for the generation of the shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode Secure Messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

The Personalization Agent manages the security environment data required for Chip Authentication and for Terminal Authentication according to SFR FMT_MTD.1/ADDTSF_WRITE.

6.3.1.5 OT.Identification

The security objective **OT.Identification** “Identification and Authentication of the TOE” address the storage of the IC Identification Data uniquely identifying the MRTD’s chip in its non-volatile memory. This will be ensure by TSF according to SFR FAU_SAS.1.

The TOE identifies itself only to a successful authenticated Basic Inspection System in Phase 4 “Operational Use”. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data. The SFR FMT_MTD.1/INI_DIS allow the MRTD Manufacturer only to disable Initialization Data because their use in the phase 4 “Operational Use” can violate the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD’s chip before successfully authentication of the Basic Inspection Terminal and will stop communicating after unsuccessful authentication attempt.

6.3.1.6 OT.Chip_Auth_Proof

The security objective **OT.Chip_Auth_Proof** “Proof of MRTD’s cgip authenticity” is ensured by the Chip Authentication Protocol provided by FIA_API.1/CAP proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/DH_MRTD is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol requires additional TSF according to FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode Secure Messaging).

6.3.1.7 OT.Prot_Abuse-Func

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

6.3.1.8 OT.Prot_Inf_Leak

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

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

6.3.1.9 OT.Prot_Phys_Tamper

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

6.3.1.10 OT.Prot_Malfunction

The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by:

- i. the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF Data and TSF code,
- ii. the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction and

6.3.1.11 OD.Assurance

The security objective **OD.Assurance** for the IT environment will be supported by non-IT security measures only.

6.3.1.12 OD.Material

The security objective **OD.Material** for the IT environment will be supported by non-IT security measures only.

6.3.1.13 OT.Authoriz_Sens_Data

The security objective **OT.Authoriz_Sens_Data** is directed to establish the Document Verifier PKI and will be supported by non-IT security measures only.

6.3.2 Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

Table 13 shows the dependencies between the SFR and of the SFR to the SAR of the TOE.



SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1/KDF_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD
FCS_CKM.1/CPS_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD
FCS_CKM.1/DH_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD
FCS_CKM.4/MRTD	[FDP_ITC.1 Import of User Data without security attributes, FDP_ITC.2 Import of User Data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1
FCS_COP.1/SHA_MRTD	[FDP_ITC.1 Import of User Data without security attributes, FDP_ITC.2 Import of User Data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/TDES_MRTD	[FDP_ITC.1 Import of User Data without security attributes, FDP_ITC.2 Import of User Data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/MAC_MRTD	[FDP_ITC.1 Import of User Data without security attributes, FDP_ITC.2 Import of User Data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of User Data without security attributes, FDP_ITC.2 Import of User Data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FCS_RND.1/MRTD	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled
FIA_UAU.4/MRTD	No dependencies	n.a.
FIA_UAU.5/MRTD	No dependencies	n.a.
FIA_UAU.6/MRTD	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled
FIA_AP1.1/CAP	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1 Justification 1 for non-satisfied dependencies
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.1,
FDP_UCT.1/MRTD	[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_ACC.1
FDP_UIT.1/MRTD	[FTP_ITC.1 Inter-TSF trusted channel, or	FDP_ACC.1, Justification 2 for non-

	FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	satisfied dependencies
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled
FMT_LIM.1	FMT_LIM.2	Fulfilled
FMT_LIM.2	FMT_LIM.1	Fulfilled
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/ADDTSF_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.3	FMT_MTD.1	Fulfilled
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 13 – Dependencies between the SFR for the TOE

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

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

Justification 2. The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the use of Secure Messaging between the MRTD and the BIS. There is no need for sensitive SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels it is the only one.

Justification 3. The TOE consists of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

6.3.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The TOE assurance level is augmented with respect to the EAL4 package for what refers to development security (ALC_DVS.2 instead of ALC_DVS.1) and vulnerability analysis (AVA_VAN.5 instead of AVA_VAN.3).

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing, especially for the secure handling of the MRTD's material.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives OT.Sens_Data_Conf, OT.Chip_Auth_Proof and OD.Assurance.

The ALC_DVS.2 has no dependencies.

The AVA_VAN.5 component depends on:

- ADV_ARC.1, Security architectural description
- ADV_FSP.4, Security enforcing functional specification
- ADV_TDS.3, Basic modular design
- ADV_IMP.1, Implementation representation of the TSF
- AGD_OPE.1, Operational user guidance
- AGD_PRE.1, Preparative procedures

All of these are met or exceeded in the EAL4 assurance package.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The analysis of the TOE's security requirements with regard to their mutual support and internal consistency demonstrates:

- The dependency analysis in section 6.3.2 shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All

dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

- The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional assurance dependencies which are not met, a possibility which has been shown not to arise in section 6.3.2 “Dependency Rationale” and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7. TOE Summary Specification

The following sections provide a general understanding of how the TOE is implemented. To facilitate reading, the description of the security features of the TOE is organized in security services. A requirements traceability matrix against each security service is also given in Table 14.

7.1 Coverage of SFRs

7.1.1 Agents Identification & Authentication

This security service meets the following SFRs:

FCS_CKM.4/MRTD, FCS_COP.1/SHA_MRTD, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD, FCS_COP.1/SIG_VER, FIA_AFL.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4/MRTD, FIA_UAU.5/MRTD, FIA_API.1/CAP.

Access to functions and data of the TOE is only allowed to authenticated users. The authentication mechanism applied depends on the system used for operations.

The MRTD Manufacturer and the Personalization Agent authenticate themselves to the e-Passport by means of a mutual authentication mechanism (FIA_UID.1, FIA_UAU.1, FIA_UAU.5/MRTD, FCS_COP.1/TDES_MRTD, FCS_CKM.1/MAC_MRTD).

This function detects each unsuccessful authentication attempt. The MRTD Manufacturer and the Personalization Agent have only a limited number of authentication attempts after which the related keys are blocked (FIA_AFL.1, see Table 10).

In case of regular termination of the protocol, both parties possess authentic keying materials only known to them. The user may establish a Secure Messaging session (FCS_CKM.1/CPS/MRTD) and at the end of the session, the session keys are securely erased (FCS_CKM.4/MRTD).

The Basic Access System and the MRTD mutually authenticate by means of Basic Access Control mechanism, based on a three pass challenge-response protocol (FIA_UID.1, FIA_UAU.1, FIA_UAU.5/MRTD). The challenge is the random number sent from one party to the other. This random number will be enciphered with the secret symmetric key by the receiver and then will be verified by the sender. This security service manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way. The algorithm used for encryption/decryption and MAC computation is consistent with SFRs FCS_COP.1/TDES_MRTD, FCS_CKM.1/MAC_MRTD, and FCS_COP.1/SHA_MRTD.

After a successful BAC authentication, the Basic Access System is able to read less sensitive data, such as the MRZ, the facial image and other data easily available from other sources.

In the operational use phase, the TOE identification data can be obtained by an authenticated BIS only. A BAC mechanism is used for this authentication (FIA_UAU.5/MRTD).

If passport inspection is performed on a General Inspection System, then the MRTD authenticity is proved executing the Chip Authentication Protocol. Chip Authentication proves that the chip is genuine and also provides strong keys for Secure Messaging (FIA_UID.1, FIA_UAU.1, FIA_UAU.5/MRTD, FIA_API.1/CAP).

If passport inspection is performed on an Extended Inspection System, then after a successful Chip Authentication the MRTD chip recognizes that the Inspection System is entitled to access sensitive data, such as fingerprints, iris image and other data not easily available from other sources by means of the Terminal Authentication protocol (FIA_UID.1, FIA_UAU.1, FIA_UAU.5/MRTD, FCS_COP.1/SIG_VER). Terminal Authentication attempts are only accepted after a successful Chip Authentication and a consequent restart of the Secure Messaging session.

The combination of Chip Authentication and Terminal Authentication provides an implementation of the Extended Access Control mechanism.

7.1.2 Data exchange with Secure Messaging

This security service meets the following SFRs:

FCS_CKM.1/KDF_MRTD, FCS_CKM.1/DH_MRTD, FCS_CKM.1/CPS_MRTD,
FCS_COP.1/SHA_MRTD, FCS_COP.1/TDES_MRTD, FCS_CKM.4/MRTD,
FCS_COP.1/MAC_MRTD, FCS_COP.1/SIG_VER, FIA_UAU.6/MRTD, FIA_API.1/CAP.

This security service concerns the creation and the management of a secure communication channel for the sensitive data exchange between the TOE and either the MRTD Manufacturer, the Personalization Agent, or the Inspection System. On this channel the data will be encrypted and authenticated with session keys so that the TOE is able to verify the integrity and authenticity of received data. The session keys are calculated during the authentication phase. During operational use, if a Chip Authentication protocol is executed, then the Secure Messaging is restarted using the session keys computed during the Chip Authentication. The channel will be closed in case of a received message with:

- wrong Secure Messaging format,
- plain access.

Session keys are overwritten after usage (FCS_CKM.4/MRTD).

7.1.3 Access Control of stored Data Objects

This security service meets the following SFRs:

FAU_SAS.1, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1/MRTD, FDP_UIT.1/MRTD,
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/CVCA_INI, FMT_MTD.1/CVCA_UPD,
FMT_MTD.1/DATE, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/ADDTSF_WRITE,
FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ

As required in FDP_ACF.1, read and write access to stored data must be controlled in different phases of the production and during operational use.

This security service ensures that the assets can only be accessed as defined by the related access rights and allows access to the TOE identification data in the Personalization phase. Furthermore, access conditions allow to differentiate the roles based on the knowledge of secret keys. Any access not explicitly allowed is denied.

After keys have been written, any type of direct access to any key is not allowed (FMT_MTD.1/KEY_WRITE, FMT_MTD.1/ADDTSF_WRITE and FMT_MTD.1/KEY_READ).

7.1.4 Life cycle management

This security service meets the following SFRs:
FMT_SMF.1, FMT_SMR.1

It ensures that the TOE life cycle status is set in an irreversible way to mark the following operating system phases in the given order: initialization phase (corresponding to both manufacturing and personalization stages of the production process) and operational phase (corresponding to passport operational use).

7.1.5 Software integrity check of TOE's assets

This security service meets the following SFRs:
FMT_LIM.1, FMT_LIM.2, FPT_TST.1

The TOE does not allow to analyze, debug or modify TOE's software during the operational use. In phases 3 and 4 no commands are allowed to load executable code. This security service also checks the integrity of the following assets:

- application files,
- security data objects.

Integrity checks will be executed before any use of TSF Data.

This service warns the entity connected upon detection of an integrity error of the sensitive data and preserves a secure state when failure is detected by TSF.

7.1.6 Security features provided by the hardware

This security service meets the following SFRs: FCS_RND.1/MRTD, FMT_LIM.1, FMT_LIM.2, FPT_EMSEC.1, FPT_TST.1, FPT_FLS.1, FPT_PHP.3.

The TOE benefits of a set of features provided by the integrated circuit to enforce security. These security functions have already been evaluated and certified being the chips already certified; a more detailed formulation of the security functions provided by each chip can be found in the related Security Target [R22].

7.1.7 Verification of digital signatures

This security service meets the following SFRs: FCS_COP.1/SHA_MRTD, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD, FCS_COP.1/SIG_VER, FMT_SMR.1, FMT_MTD.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/ADDTSF_WRITE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ

The signature verification is performed through the check of the certificate chain up to a trusted start point (a public key of the Country Verifying Certificate Authority, see FMT_MTD.3) and the current date handling (cf. [BSI, 2.2.4]). Once a signature is recognized as valid then security roles can be maintained according to FMT_SMR.1 and

the CVCA certificate and the current date can be updated (FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE).

The validity of the certificate chain is proven at the TOE current date if and only if:

- i. the digital signature of the Inspection System Certificate, checked using the public key of the Document Verifier Certificate, is recognized as valid and the Inspection System Certificate is not expired
- ii. the digital signature of the Document Verifier Certificate, checked using the public key in the Certificate of the Country Verifying Certification Authority, is recognized as valid and the Document Verifier Certificate is not expired
- iii. the digital signature of the Certificate of the Country Verifying Certification Authority, checked using its own public key, is recognized as valid and the Certificate of the Country Verifying Certification Authority is not expired

Table 14 shows the coverage of SFRs by the security services described above.

	Agents Identification & Authentication	Data exchange with Secure Messaging	Access Control of Stored Data Object	Life Cycle Management	SW Integrity check of TOE's Assets	Security features provided by the hardware	Verification of digital signatures
FAU_SAS.1			X				
FCS_CKM.1/KDF_MRTD		X					
FCS_CKM.1/DH_MRTD		X					
FCS_CKM.1/CPS_MRTD		X					
FCS_CKM.4/MRTD	X	X					
FCS_COP.1/SHA_MRTD		X					X
FCS_COP.1/TDES_MRTD		X					X
FCS_COP.1/MAC_MRTD		X					X
FCS_COP.1/SIG_VER		X					X
FCS_RND.1/MRTD						X	
FIA_UID.1	X						
FIA_UAU.1	X						
FIA_UAU.4/MRTD	X						
FIA_UAU.5/MRTD	X						
FIA_UAU.6/MRTD		X					
FIA_AFL.1	X						
FIA_API.1/CAP	X	X					
FDP_ACC.1			X				
FDP_ACF.1			X				
FDP_UCT.1/MRTD			X				
FDP_UIT.1/MRTD			X				
FMT_SMF.1			X	X			
FMT_SMR.1			X	X			X
FMT_LIM.1			X		X	X	
FMT_LIM.2			X		X	X	
FMT_MTD.1/INI_ENA			X				X
FMT_MTD.1/INI_DIS			X				X
FMT_MTD.1/CVCA_INI			X				X
FMT_MTD.1/CVCA_UPD			X				X
FMT_MTD.1/DATE			X				X
FMT_MTD.1/KEY_WRITE			X				X
FMT_MTD.1/ADDTSF_WRITE			X				X
FMT_MTD.1/CAPK			X				X
FMT_MTD.1/KEY_READ			X				X
FMT_MTD.3							X
FPT_EMSEC.1						X	
FPT_TST.1					X	X	
FPT_FLS.1						X	
FPT_PHP.3						X	

Table 14 – Coverage of SFRs by security services

7.2 Assurance Measures

Assurance measures applied to the TOE are fully compliant to those described in part 3 of the Common Criteria v3.1 [R9].

The implementation is based on a description of the security architecture of the TOE and on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements. These documents, together with the source code of the software, address the ADV_ARC, ADV_FSP, ADV_TDS and ADV_IMP families.

The configuration management plan addresses the ALC_CMC and ALC_CMS families and enforces good practices to securely manage configuration items including, but not limiting to, design documentation, user documentation, source code, test documentation and test data.

The configuration management process guarantees the separation of the development configuration libraries from the configuration library containing the releases and also supports the generation of the TOE.

All the configuration items are managed with the help of automated tools. In particular configuration items regarding security flaws are managed with the support of an issue tracking system, while all the other configuration items are managed with the help of a version control system.

The software test process, addressing the class ATE, is machine-assisted to guarantee a repeatable error-free execution of the tests.

A secure delivery of the TOE is guaranteed by the application of dedicated procedures. The prevention measures, the checks and all the actions to be performed at the developer's site are described in the secure delivery procedure addressing the family ALC_DEL, while the security measures related to delivery to be applied at the user's site are defined in the pre-personalization guidance. The latter document also addresses the family AGD_PRE.

The necessary information for the passport personalization is provided by a dedicated guidance and the information for its usage after delivery to the legitimate holder is provided by the guidance for the operational user. These documents address the AGD_OPE assurance family.

To protect the confidentiality and integrity of the TOE design and implementation, the development and production environment and tools conform to the security policies defined in the documentation dedicated to the development security, which addresses the family ALC_DVS.

The life-cycle model adopted in the manufacturing phases and the tools supporting the development and production of the TOE are described in a dedicated document addressing the families ALC_LCD and ALC_TAT.

An independent vulnerability analysis, meeting requirements of the family AVA_VAN, is conducted by a third party.

Due to the composite nature of the evaluation, which is based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be covered in

documents from the IC manufacturer. The security procedures described in the ST of each of the ICs supported by PEACOS have been taken into consideration.

Table 15 shows the documentation that provides the necessary information related to the assurance requirements defined in this Security Target.

Security Assurance Requirements	Documents
ADV_ARC.1	Description of the Security Architecture of the PEACOS embedded software
ADV_FSP.4	Functional Specification for the PEACOS embedded software
ADV_IMP.1	Source code of the PEACOS embedded software
ADV_TDS.3	Description of the Design of the PEACOS embedded software
AGD_OPE.1	Personalization Guidance for the PEACOS electronic passport User Guidance for the PEACOS electronic passport
AGD_PRE.1	Pre-personalization guidance for the PEACOS electronic passport.
ALC_CMC.4, ALC_CMS.4	Configuration Management Plan, configuration list evidences of configuration management
ALC_DEL.1	Secure Delivery procedure Delivery documentation
ALC_DVS.2	Development security description Development security documentation
ALC_LCD.1, ALC_TAT.1	Life-cycle definition
ATE_COV.2	Coverage of Test Analysis for the PEACOS Electronic Passport
ATE_DPT.1	Depth of Test Analysis for the PEACOS Electronic Passport
ATE_FUN.1	Functional Test Specification for the PEACOS Electronic Passport Evidences of tests
AVA_VAN.5	Documentation related to an independent vulnerability analysis.

Table 15 – Assurance Requirements documentation

Assurance measures described in this section cover the assurance requirements in section 6.3.3.

8. References

8.1 Acronyms

KA_{MM}	MRTD Manufacturer Key Pair
KA_{PA}	Personalization Agent Key Pair
ASC_{RASD}	Administrative Secret Code – Restricted Application Security Domain
ATS	Answer to Select
BAC	Basic Access Control
BIS	Basic Inspection System
C_{DS}	DS Public Key Certificate
CBC	Cipher-block Chaining (block cipher mode of operation)
CC	Common Criteria
COM	Common data group of the LDS (ICAO TR-LDS)
CPS	Common Personalization Standard
CPU	Central Processing Unit
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DF	Dedicated File (ISO 7816)
DG	Data Group (ICAO TR-LDS)
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
ECB	Electronic Codebook (block cipher mode of operation)
EEPROM	Electrically Erasable Read Only Memory
EF	Elementary File (ISO 7816)
EIS	Extended Inspection System
ESW	Embedded Software
GIS	General Inspection System
IC	Integrated Circuit
ICCSN	IC Chip Serial Number
IS	Inspection System
K_{ENC}	A key used for Encryption
K_{MAC}	A key used for computation of a checksum
LDS	Logical Data Security
LCS	Life Cycle Status
MAC	Message Authentication Code
MED	Memory Encryption and Decryption unit
MF	Master File (ISO 7816)
MMU	Memory Management Unit
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
N/A	Not Applicable
n.a.	Not Applicable
OCR	Optical Character Recognition
OS	Operating System
OSP	Organization Security Policy
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RND.ICC	ICC Random (used in BAC)

RNG	Random Number Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SO_D	Document Security Object
SOF	Strength of Function
SPA	Simple Power Analysis
ST	ST
TDES	Triple DES
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TR	Technical Report
TR-LDS	TR published by ICAO which defines the LDS
TR-PKI	TR published by ICAO which defines SO _D and the BAC mechanism
TR-03110	TR published by BSI which defines the EAC mechanism
VIZ	Visual Inspection Zone

8.2 Glossary

<i>Active Authentication</i>	Security mechanism defined in TR-PKI [R17] option by which means the MTRD's chip proves and the Inspection System verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known state or organization.
<i>application note</i>	Additional information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
<i>audit records</i>	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
<i>authenticity</i>	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the Issuing State or Organization.
<i>Basic Access Control</i>	Security mechanism defined by ICAO [R17] by which means the MTRD's chip proves and the Inspection System protect their communication by means of Secure Messaging with the Document BAC Keys.
<i>Basic Inspection System</i>	An Inspection System which implements the terminals part of the BAC Mechanism and authenticates themselves to the MRTD's chip using the Document BAC Keys derived from the printed MRZ data for reading the logical MRTD.

<i>biographical data</i>	The personalized details of the bearer of the document appearing as text in the VIZ and MRZ on the biographical data page of a passport book or on a travel card or visa [R14].
<i>biometric reference data</i>	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
<i>Certificate chain</i>	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the previous Country Verifying Certification Authority public key.
<i>Chip Authentication</i>	Authentication protocol used to verify the genuinity of the MRTD chip.
<i>counterfeit</i>	An unauthorized copy or reproduction of a genuine security document made by whatever means [R14].
<i>Country Signing Certification Authority (CSCA)</i>	Certification Authority of the Issuing State or Organization which attests the validity of certificates and digital signatures issued by the Document Signer.
<i>Country Signing Certification Authority Certificate (C_{CSCA})</i>	Certificate of the Country Signing Certification Authority Public Key (PK _{CSCA}) issued by Country Signing Certification Authority stored in the Inspection System.
<i>Country Verifying Certification Authority (CVCA)</i>	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing Country or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.
<i>Current Date</i>	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
<i>CVCA link Certificate</i>	Certificate of the new public key of the Country Verifying Certification Authority signed with the old private key of the Country Verifying Certification Authority where the certificate effective date for the new keys is before the certificate expiration date of the certificate for the old key.

<i>Document Basic Access Keys</i>	Pair of symmetric TDES keys used for Secure Messaging with encryption (K_{ENC_BAC}) and message authentication (K_{MAC_BAC}) of data transmitted between the MRTD's chip and the Inspection System [R17]. It is derived from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
<i>Document Security Object</i>	A RFC3369 CMS Signed Data Structure, signed by the Document Signer. It carries the hash values of the LDS DG's and is stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}) [R17].
<i>Document Signer</i>	Entity delegated by the Issuing State or Organization to digitally sign the DG's present in the LDS.
<i>eavesdropper</i>	A threat agent with low attack potential reading the communication between the MRTD's chip and the Inspection System to gain the data on the MRTD's chip.
<i>enrolment</i>	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity [R15].
<i>Extended Access Control</i>	Security mechanism identified in TR-PKI [R17] by which means the MTRD's chip (i) verifies the authentication of the Inspection Systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the Inspection System by Secure Messaging.
<i>Extended Inspection System</i>	A role of a terminal as part of an Inspection System which is in addition to the BIS authorized by the Issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
<i>Forgery</i>	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait [R14].
<i>General Inspection System</i>	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
<i>Global interoperability</i>	The capability of Inspection Systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in

other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs.

impostor

A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document [R14].

Initialization Data

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

inspection

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

Inspection System

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

Integrated Circuit

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

integrity

Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from those created by the Issuing State or Organization

Issuing Organization

Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer) [R16].

Issuing State

The Country issuing the MRTD [R16].

Logical Data Structure

The collection of groupings of DG's stored in the optional capacity expansion technology [R16]. The capacity expansion technology used is the MRTD's chip.

<i>Logical MRTD</i>	Data of the MRTD holder stored according to the LDS [R16] as specified by ICAO on the contactless IC. It presents contactless readable data including (but not limited to): <ol style="list-style-type: none">personal data of the MRTD holderthe digital Machine Readable Zone Data (digital MRZ data, EF.DG1),the digitized portraits (EF.DG2),the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both andthe other data according to LDS (EF.DG5 to EF.DG16).
<i>Machine Readable Document</i>	<i>Travel</i> Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read [R16].
<i>Machine Readable Zone</i>	Fixed dimensional area located on the front of the MRTD Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods [R16].
<i>machine-verifiable feature</i>	<i>biometrics</i> A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine.
<i>MRTD application</i>	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes: <ol style="list-style-type: none">the file structure implementing the LDS [R16],the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14 and EF.DG 16) andthe TSF Data including the definition the authentication data but except the authentication data itself.
<i>MRTD Basic Access Control</i>	Mutual authentication protocol followed by Secure Messaging between the Inspection System and the MRTD's chip based on MRZ information as a key seed and access condition to data stored on MRTD's chip according to LDS.
<i>MRTD holder</i>	The rightful holder of the MRTD for whom the issuing

State or Organization personalized the MRTD.

MRTD's chip

A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the LDS [R16].

MRTD's chip Embedded Software

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

Optional biometric reference data

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

Passive Authentication

Passive Authentication is a mechanism that ensures the authenticity of the DG's present in the LDS by:

- i. the verification of the digital signature of the SO_D and
- ii. comparing the hash values of the read LDS data fields with the hash values contained in the SO_D .

Personalization

The process by which the portrait, signature and biographical data are applied to the document [R14].

Personalization Agent

The agent delegated by the Issuing State or Organization to personalize the MRTD for the holder by

- i. establishing the identity the holder for the biographic data in the MRTD,
- ii. enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or the encoded iris image(s) and
- iii. writing these data on the physical and logical MRTD for the holder.

Personalization Agent Authentication Information

TSF Data used for authentication proof and verification of the Personalization Agent.

Physical travel document

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

- i. biographical data,
- ii. data of the MRZ,
- iii. photographic image and
- iv. other data.

<i>Pre-personalization Data</i>	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair (KA_{PA}).
<i>Pre-personalized MRTD's chip</i>	MRTD's chip equipped with a unique identifier, the KA_{PA} , and a unique asymmetric Active Authentication Key Pair of the chip.
<i>Primary Inspection System</i>	An Inspection System that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
<i>Receiving State</i>	The Country to which the MRTD holder is applying for entry [R16].
<i>reference data</i>	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
<i>secondary image</i>	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.
<i>Secure Messaging</i>	Secure Messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R18].
<i>skimming</i>	Imitation of the Inspection System to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
<i>travel document</i>	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.
<i>traveler</i>	A person presenting the MRTD to the Inspection System and claiming the identity of the MRTD holder.
<i>TSF Data</i>	Data created by and for the TOE, that might affect the operation of the TOE [R7].
<i>Unpersonalized MRTD</i>	MRTD material prepared to produce an personalized MRTD containing an initialized and pre-personalized MRTD's chip.
<i>User Data</i>	Data created by and for the user, that does not affect the

operation of the TSF [R7].

<i>Verification</i>	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template [R15].
<i>Verification data</i>	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

8.3 Technical References

- [R1] **BSI:** *Functionality classes and evaluation methodology for physical random number generators, AIS31, Version 1, 25.9.2001*

- [R2] **BSI:** *Certification Report BSI-DSZ-CC-0680-2010 for NXP Secure Smart Card Controller P5CD080V0B, P5CC080V0B and P5CC073V0B each with specific IC Dedicated Software;3 November 2010.*

- [R3] **BSI:** *Evaluation Technical Report BSI-DSZ-CC-0680 NXP P5CD080V0B Secure Smart Card Controller, Version 1.39, 29 October 2010, (confidential document)*

- [R4] **BSI:** *Protection Profile conformant to Smartcard IC Platform Protection Profile, Version 1.0, 11 July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001*

- [R5] **BSI:** *Protection Profile Machine Readable Travel Document with „ICAO Application " Extended Access Control, Version 1.2, BSI-PP-0026, 2007-11-19. Maintenance report BSI-PP-0026-2006-MA-01, 2008-06-30.*

- [R6] **BSI:** *Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11*

- [R7] **CCRA:** *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009, version 3.1 rev.3, CCMB-2009-07-001*

- [R8] **CCRA:** *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, July 2009, version 3.1 rev.3, CCMB-2009-07-002*

- [R9] **CCRA:** *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, July 2009, version 3.1 rev 3, CCMB-2009-07-003*

- [R10] **EMV CPS:** *EMV Card Personalization Specification – version 1.0, June 2003*
- [R11] **FIPS 46-3:** *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology*
- [R12] **FIPS 180-2:** *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 180-2, SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology – 2002 August 1*
- [R13] **GlobalPlatform:** *GlobalPlatform Card Specification – version 2.1.1, March 2003*
- [R14] **ICAO Doc 9303:** *MACHINE READABLE TRAVEL DOCUMENTS – Part 3 Machine Readable Official Travel Documents Volume 2 Specifications for Electronically Enabled Official Travel Documents with Biometric Identification Capability Approved by the Secretary General and published under his authority – Third Edition – 2006*
- [R15] **ICAO TR-BD:** *Biometrics Deployment of MACHINE READABLE TRAVEL DOCUMENTS – Technical Report: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using MRTD's; Version 2.0*
- [R16] **ICAO TR-LDS:** *MACHINE READABLE TRAVEL DOCUMENTS – Technical Report: Development of a LOGICAL DATA STRUCTURE for Optional Capacity Expansion Technologies; Version 1.7*
- [R17] **ICAO TR-PKI:** *MACHINE READABLE TRAVEL DOCUMENTS – Technical Report: PKI for MRTD offering ICC Read-only Access; Version 1.1*
- [R18] **ISO/IEC 7816–4 2005.01.15:** *Information Technology – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange*
- [R19] **ISO/IEC 9796–2 2002:** *Information Technology – Security Techniques – Digital Signature Scheme – Part 2: Integer factorization based mechanism, 2002*
- [R20] **ISO/IEC 9797–1 1999:** *Information Technology – Security Techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher, 1999*
- [R21] **ISO/IEC 11568–2 2005:** *Banking – Key management (retail) – Part 2: Symmetric ciphers, their key management and life cycle*
- [R22] **NXP Semiconductors:** *P5CD080/P5CN080/P5CC080/P5CC073V0B Security Target Lite Rev. 1.9 – 14 July 2010, BSI-DSZ-CC-0410-2007*

- [R23] **NXP Semiconductors:** *Guidance, Delivery and Operation Manual for the P5Cx012/02x/040/073/080/144 family, NXP Semiconductors, Version 1.8, Document number: 129918, February 15th, 2010 (confidential document)*
- [R24] **IETF Network Working Group:** *Request For Comments 3447, Public-Key Cryptography Standard (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003.*
- [R25] **RSA Laboratories:** *PKCS #3 - Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, version 1.4 November 1993.*
- [R26] **ISO/IEC:** *International Standard 14443-1 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 1: Physical characteristics.*
- [R27] **ISO/IEC:** *International Standard 14443-2 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 2: Radio frequency interface power and signal interface.*
- [R28] **ISO/IEC:** *International Standard 14443-3 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 3: Initialization and anticollision.*
- [R29] **ISO/IEC:** *International Standard 14443-4 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 4: Transmission protocol.*
- [R30] **ISO/IEC:** *International Standard 15946-1 – Information Technology – Security Techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002.*
- [R31] **ISO/IEC:** *International Standard 15946-2 – Information Technology – Security Techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.*
- [R32] **ISO/IEC:** *International Standard 15946-3 – Information Technology – Security Techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment, 2002.*
- [R33] **RSA Laboratories:** *PKCS#1 – RSA cryptography standard, An RSA Laboratories Technical Note, version 2.1 June 2002.*
- [R34] **IETF Network Working Group:** *Request For Comments 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.*
- [R35] **Gep:** *User Guidance for the PEACOS electronic passport with Extended Access Control*

Appendix A Integrated Circuits supported by PEACOS

This section highlights the peculiarities of the integrated circuits supported by PEACOS. This composite ST trusts in and relies on the Security Target of the underlying hardware.

A.1 NXP P5CD080V0B Integrated Circuit

A.1.1 Chip Identification

The TOE is based on the integrated circuit P5CD080V0B. This chip received Common Criteria certification at the assurance level EAL5 augmented with AVA_VLA.4, with certification ID: BSI-DSZ-CC-0680-2010 [R2][R3][R22][R23].

A.1.2 IC Developer Identification

The developer of the P5CD080V0B chip is NXP Semiconductors.

A.1.3 IC Manufacturer Identification

The manufacturer of the P5CD080V0B chip is NXP Semiconductors.

A.1.4 Main Features

The NXP P5CD080V0B is a high security microcontroller equipped with:

- A CPU including a memory encryption and decryption module
- A memory management unit (MMU)
- 6144 bytes of volatile memory (RAM) to hold temporary data,
- 200 Kbytes of non-volatile read-only memory (ROM) to hold the operating system
- 80 Kbytes of non-volatile, readable and writable memory (EEPROM), to hold the file system and additions to the operating system
- A true random number generator
- A 112 bit dual key TDES co-processor
- An AES co-processor
- A Public Key co-processor
- Security sensors
- Checksum module
- Interrupt module
- Timer
- A radiofrequency transceiver for contactless communications
- ISO/IEC 7816 and 14443 type A interface

The random number generator has already been evaluated [R2] as conformant to AIS31 functionality class P2 [R1] with SOF level “high” (see SFR FCS_RND.1/MRTD in section 6.1.2.4).

Figure 3 shows the internal architecture of this chip.

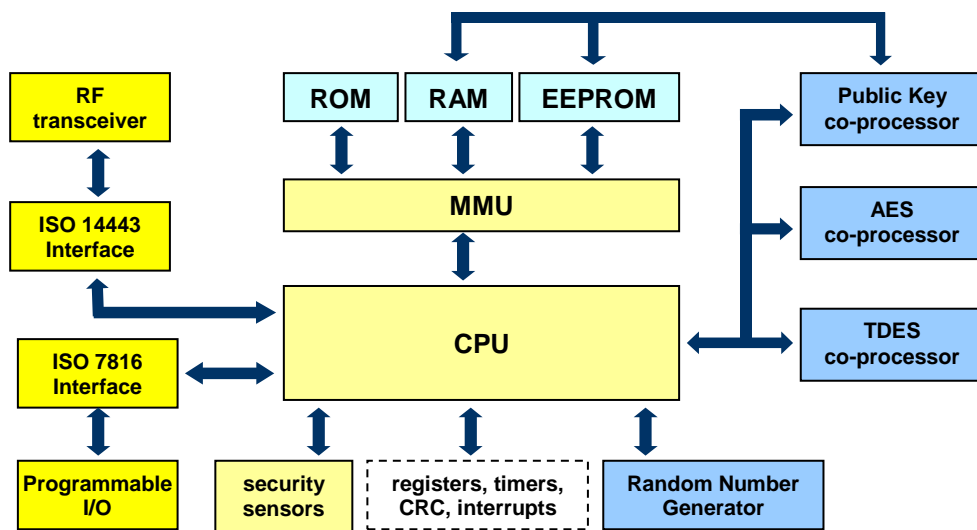


Figure 3 – NXP P5CD080V0B internal architecture

END OF DOCUMENT