



the security technology provider

<http://www.gepitalia.it>



<http://www.security.arjowiggins.com>

Arjowiggins Security SAS - Gep S.p.A.
via Remo De Feo, 1
80022 Arzano (NA), ITALY

Security Target

SOMA801STM Electronic Passport Extended Access Control

Public Version

**Common Criteria version 3.1 revision 4
Assurance Level EAL 4+**

Version 1.2
Date 2013-08-19
Reference TCLE130007
Classification PUBLIC

Version control

Version	Date	Author	Revision Description
1.0	2013-05-23	Marco EVANGELISTA	First version
1.1	2013-07-04	Marco EVANGELISTA	Developer's/Sponsor's name change.
1.2	2013-08-19	Marco EVANGELISTA	SFR FCS_COP.1/SHA has been updated.

Table of Contents

Abbreviations and Notations	6
1. Introduction	7
1.1 ST Overview	7
1.2 ST reference	7
1.3 TOE reference	8
1.4 TOE overview	9
1.4.1 TOE Definition	9
1.4.2 TOE Usage and security features for operational use	10
1.4.3 TOE Life-cycle	13
1.4.4 Non-TOE hardware/software/firmware required by the TOE	17
1.5 TOE Description	17
1.5.1 Physical scope of the TOE	17
1.5.2 Other non-TOE physical components	18
1.5.3 Logical scope of the TOE	18
2. Conformance claims	20
2.1 Common Criteria Conformance	20
2.2 Protection Profile Conformance	20
2.3 Package Conformance	20
2.4 Conformance Rationale	20
3. Security Problem Definition	23
3.1 Introduction	23
3.1.1 Assets	23
3.1.2 Subjects	23
3.2 Assumptions	25
3.3 Threats	27
3.4 Organizational Security Policies	31
4. Security Objectives	33
4.1 Security Objectives for the TOE	33
4.2 Security Objectives for the Operational Environment	36
4.3 Security Objective Rationale	39
5. Extended Components Definition	43
5.1 Definition of the family FAU_SAS	43
5.2 Definition of the family FCS_RND	43
5.3 Definition of the family FIA_API	44
5.4 Definition of the family FMT_LIM	45
5.5 Definition of the family FPT_EMSEC	47
6. Security Requirements	49
6.1 Security Functional Requirements for the TOE	49
6.1.1 Class FAU Security Audit	50
6.1.2 Class Cryptographic Support (FCS)	50
6.1.3 Class FIA Identification and Authentication	56
6.1.4 Class FDP User Data Protection	62
6.1.5 Class FMT Security Management	65
6.1.6 Class FPT Protection of the Security Functions	73
6.2 Security Assurance Requirements for the TOE	76
6.3 Security Requirements Rationale	77

6.3.1	Security functional requirements rationale.....	77
6.3.2	Dependency Rationale	81
6.3.3	Security Assurance Requirements Rationale	84
6.3.4	Security Requirements – Mutual Support and Internal Consistency.....	84
7.	TOE Summary Specification	86
7.1	Coverage of SFRs	86
7.1.1	SS.AG_ID_AUTH Agents Identification & Authentication	86
7.1.2	SS.SEC_MSG Data exchange with Secure Messaging	89
7.1.3	SS.ACC_CNTRL Access Control of stored Data Objects	89
7.1.4	SS.LFC_MNG Life cycle management.....	90
7.1.5	SS.SW_INT_CHECK Software integrity check of TOE's assets	90
7.1.6	SS.SF_HW Security features provided by the hardware	90
7.1.7	SS.SIG_VER Verification of digital signatures.....	90
7.2	Assurance Measures.....	93
8.	References.....	96
8.1	Acronyms	96
8.2	Glossary	97
8.3	Technical References.....	105

List of Tables

Table 1-1	ST Identification	7
Table 1-2	TOE Identification	8
Table 1-3	Roles Identification	15
Table 2-1	Modified security objectives	21
Table 2-2	SFRs assignment changes, refinements, iterations and additions.....	22
Table 4-1	Security Objective Rationale.....	40
Table 5-1	Family FAU_SAS.....	43
Table 5-2	Family FCS_RND	44
Table 5-3	Family FIA_API.....	45
Table 5-4	Family FMT_LIM.....	46
Table 5-5	Family FPT_EMSEC.....	48
Table 6-1	RSA algorithms for signature verification in Terminal Authentication ([R7]).....	55
Table 6-2	ECDSA algorithms for signature verification in Terminal Authentication ([R7])	55
Table 6-3	Overview on authentication SFR	57
Table 6-4	Assurance requirements at EAL4+	76
Table 6-5	Coverage of Security Objectives for the TOE by SFR	77
Table 6-6	Dependencies between the SFR for the TOE.....	82
Table 7-1	Summary of authentication mechanisms	87
Table 7-2	Coverage of SFRs by security services	92
Table 7-3	Assurance Requirements documentation	95

List of Figures

Figure 1-1	TOE life-cycle	14
Figure 1-2	Inlay components	18

Abbreviations and Notations

Numerical values

Numbers are printed in decimal, hexadecimal or binary 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.

Iterations are denoted by showing a slash "/", and the iteration indicator after the component indicator.

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 [R14].

1. Introduction

1.1 ST Overview

This Security Target (ST) document defines the security requirements and the scope of the Common Criteria evaluation of the SOMA801STM electronic passport. The Target Of Evaluation (TOE) is the contactless integrated circuit chip STMicroelectronics SB23YR80 revision B, 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.

This ST covers the Extended Access Control (EAC) mechanism only as defined by the technical report TR-03110 [R7]. The Basic Access Control (BAC) is covered by an other ST [R11].

The SOMA801STM passport was developed in full accordance with the specifications for a Machine Readable Travel Document (MRTD) defined by the International Civil Aviation Organization (ICAO). ICAO Doc 9303 [R12] [R13] details 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 used in the context of the ICAO application as described in the Protection Profiles [R5][R6].

1.2 ST reference

Table 1-1 ST Identification

Title	Security Target SOMA801STM Electronic Passport Extended Access Control – Public Version
Version	1.2
Author	Marco EVANGELISTA
Reference	TCLE130007
Keywords	Security target, security target lite, common criteria

1.3 TOE reference

Table 1-2 TOE Identification

Product Name	SOMA801STM
Product Version	1.0
TOE Identification Data	53h 4Fh 4Dh 41h 38h 30h 31h 53h 54h 4Dh 5Fh 31h 5Fh 30h
Evaluation Criteria	Common Criteria version 3.1 revision 4
Protection Profile	BSI-CC-PP-0056
Evaluation Assurance Level	EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5
Developer	Arjowiggins Security SAS - Gep S.p.A.
Evaluation Sponsor	Arjowiggins Security SAS - Gep S.p.A.
Evaluation Facility	SERMA Technologies' ITSEF
Certification Body	ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information
Certification ID	SOMA-STM
Keywords	electronic passport, e-Passport, ICAO,MRTD, machine readable travel document, extended access control, EAC

The TOE identification data are located in the non-volatile memory of the chip. Instructions for reading identification data are provided by the pre-personalization guidance, the personalization guidance and the user guidance.

The TOE is identified by the following string, representing the Global Reference:

SOMA801STM_1_0

(ASCII codes 53h 4Fh 4Dh 41h 38h 30h 31h 53h 54h 4Dh 5Fh 31h 5Fh 30h)

The first four bytes of the identification data identify the operating system. Bytes from 5 to 10 contain the IC identifier. Last three bytes encode ROM code and patch version (also known as OS version). Bytes 11 and 13 are field separators.

The parts of the Global Reference data have the following meaning:

- OS identifier: SOMA (ASCII codes 53h 4Fh 4Dh 41h)
- IC identifier: 801STM (ASCII codes 38h 30h 31h 53h 54h 4Dh)¹
- ROM code version: 1 (ASCII code 31h)
- Patch version: 0 (ASCII code 30h)

Application Note 1: *The OS 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 “_”*

¹ This six byte string identifies the SB23YR80B chip from STMicroelectronics.

(underscore, ASCII code 5Fh). A minor version number 0 (ASCII code 30h) indicates that no patch is loaded.

1.4 TOE overview

1.4.1 TOE Definition

The TOE is the contactless integrated circuit of MRTD programmed according to the Logical Data Structure (LDS) [R12] and providing Basic Access Control, according to Doc9303 [R12], and Extended Access Control as defined in the technical guideline BSI TR-03110 [R7].

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. The TOE adds security features to an ordinary passport booklet. Cryptographic techniques are applied to confirm the identity of the holder and to verify the authenticity of the passport.

The TOE is connected to an antenna for wireless communication. Both the TOE and the antenna are embedded in a paper or plastic substrate, that provides mechanical support and protection. The resulting device (TOE, antenna and substrate), is called "inlay" as it is intended to be inserted in a passport booklet (see section 1.4.3.2).

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 112 bit symmetric key cryptography to protect the overall content of the passport
- Additional user authentication based on up to 3072 bit asymmetric key cryptography to protect sensitive biometric data such as fingerprints and iris image.
- Sophisticated on-chip sensors to detect physical attacks
- Memory management unit to prevent improper usage of memory and unauthorized code execution.
- Encrypted communications between the passport and the Inspection System

The integrated circuit, along with its OS and application, provides the following security mechanisms:

- Basic Access Control mechanism according to the ICAO Doc 9303 [R12]
- Extended Access Control mechanism, implemented combining the Chip Authentication protocol with the Terminal Authentication protocol as defined in the BSI TR-03110 technical guideline [R7]

The TOE is composed of:

- the circuitry of the MRTD's chip SB23YR80B,
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (SOMA801STM Operating System),
- the MRTD application and
- the associated guidance documentation.

1.4.2 TOE Usage and security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity.

The MRTD in context of this security target contains

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

The authentication of the traveler is based on:

- 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, The receiving state trusts a genuine MRTD of an Issuing State or Organization.

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

- the **physical MRTD** as travel document in the form of paper, plastic and chip. It presents visual 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 contactless 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 biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both²;
 - iv. the other data according to LDS (EF.DG5 to EF.DG14, EF.DG16)
 - v. the Document security object (SO_D),
 - 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 MRTD as the passport book 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

² These biometric reference data are optional according to [R8]. This ST assumes that the issuing State or Organization uses this option and protects these data by means of extended access control.

security measures (e.g. control of materials, personalization procedures) [R12]. 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 and the security features of the MRTD's chip.

The ICAO defines the baseline required security methods Passive Authentication and the following optional advanced security methods:

- Basic Access Control to the logical MRTD,
- Active Authentication of the MRTD's chip,
- Extended Access Control to and
- the Data Encryption of sensitive biometrics as an optional security measure in the ICAO Doc9303 [R12].

The Passive Authentication and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD:

- i. in integrity by write-only-once access control and by physical means and
- ii. in confidentiality by the Extended Access Control Mechanism.

This Security Target addresses the Chip Authentication described in [R7] as an alternative to the Active Authentication stated in [R12].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this ST as the MRTD has additionally to fulfill the "Security Target for the SOMA801STM Electronic Passport, Basic Access Control" [R11].

Application Note 2: *Beside this EAC-ST, there is a separate Security Target for BAC [R11]. Note, that the claim for conformance to the BAC-PP [R5] made in the BAC-ST does not require the conformance claim to the EAC-PP [R6]. Nevertheless, claiming conformance of this EAC-ST to the EAC-PP requires that the TOE meets a (separate) ST [R11] conforming to the BAC-PP [R5].*

For BAC, the inspection system:

- i. reads optically the MRTD,
- ii. authenticates itself as inspection system by means of Document Basic Access Keys.

After successful BAC authentication of the inspection system, the MRTD chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [R12], normative appendix 5.

This security target requires the TOE to implement the Chip Authentication defined in [R7]. The Chip Authentication prevents data traces described in [R12] informative appendix 7, A7.3.3. The Chip Authentication is provided throughout the following steps:

- i. The Inspection System communicates by means of the secure messaging established by Basic Access Control,
- ii. The Inspection System reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object,
- iii. The Inspection System generates an ephemeral key pair,
- iv. The TOE and the Inspection System agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and
- v. The Inspection System verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private key corresponding to the Chip Authentication Public Key used for derivation of the session keys).

The Chip Authentication requires collaboration of the TOE and the TOE environment (see also section 1.4.4).

This ST requires the TOE to implement the Extended Access Control as defined in [R7]. The Extended Access Control consists of two parts:

- i. The Chip Authentication Protocol and
- ii. The Terminal Authentication Protocol

The Chip Authentication Protocol:

- i. Authenticates the MRTD's chip to the Inspection System and
- ii. Establishes secure messaging which is used by Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the Inspection System.

Therefore, Terminal Authentication can only be performed if Chip Authentication has been successfully executed.

The Terminal Authentication Protocol consists of:

- i. the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and
- ii. an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.

The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.4.3 TOE Life-cycle

The TOE life cycle is described in terms of four life cycle phases:

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 embedding of the chip in an inlay with an antenna, (iii) the completion of the operating system, (iv) the initialization and pre-personalization of the MRTD
3. Personalization
4. Operational Use

Application Note 3: *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.*

In Figure 1-1 activities (rounded rectangles) and deliveries (arrows) printed orange are secured by the environment and are covered by assurance class ALC. The ones printed white refer to phases covered by assurance class AGD, in which the TOE is self-protected.

Figure 1-1 TOE life-cycle

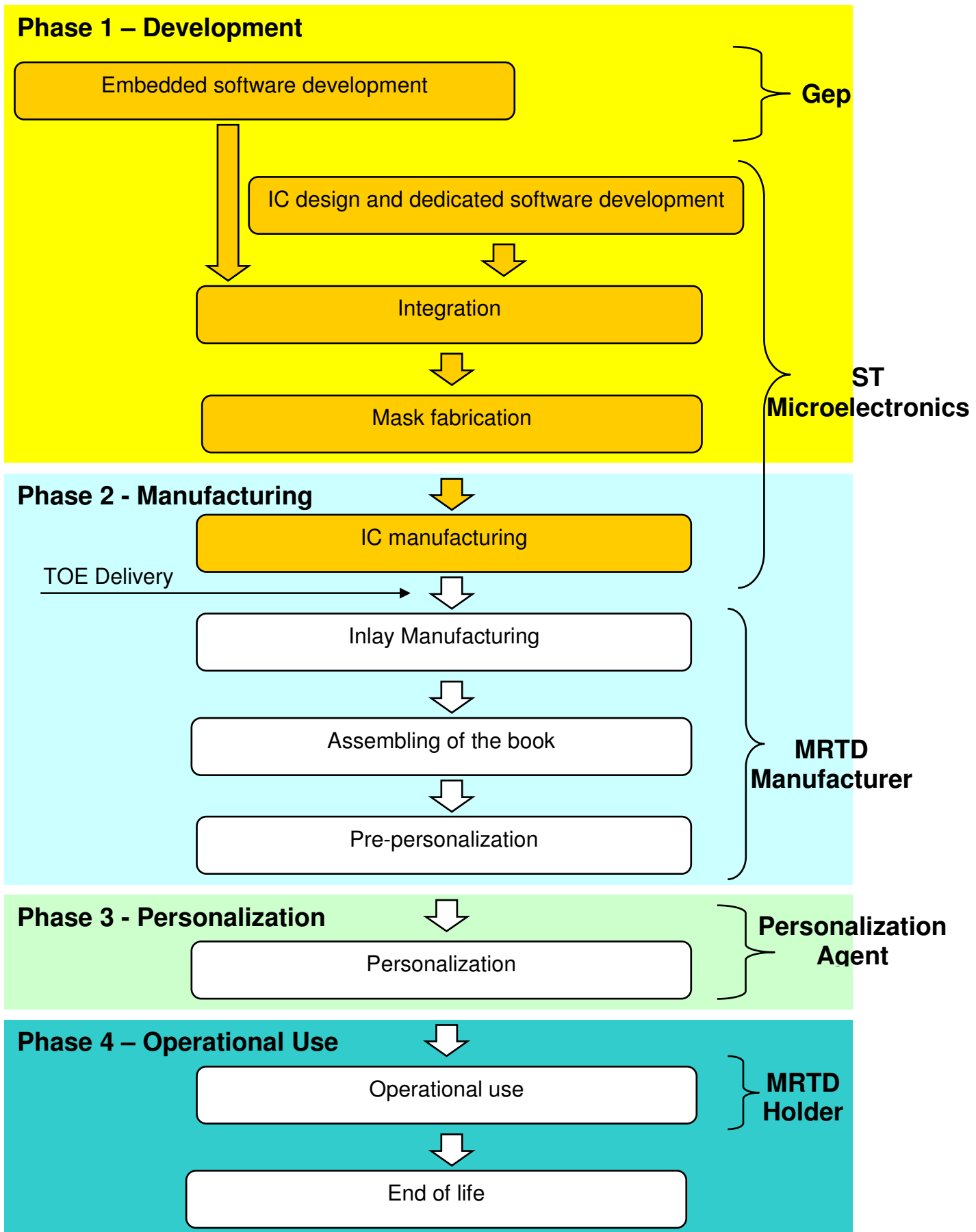


Table 1-3 identifies the roles in each phase of the TOE life cycle.

Table 1-3 Roles Identification

Phase	Role	Identification
1	IC Developer	STMicroelectronics
1	Embedded Software Developer	Gep S.p.A.
2	IC Manufacturer	STMicroelectronics
2	MRTD Manufacturer	the agent who is acting on the behalf of the Issuing State or Organization to assemble the passport book embedding the TOE, and to pre-personalize the MRTD
3	Personalization Agent	the agent who is acting on the behalf of the Issuing State or Organization to personalize the MRTD for the holder
4	MRTD Holder	The rightful owner of the MRTD

1.4.3.1 Phase 1 “Development”

Step1 “IC Development”

The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

Step2 “Embedded Software Development”

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

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

1.4.3.2 Phase 2 “Manufacturing”

Step3 “IC Manufacturing”

In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer

- (i) writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.
- (ii) Creates the MRTD application

Application Note 4: *Creation of the application implies the creation of MF and ICAO.DF*

The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

Step4 “MRTD Manufacturing – Assembling of the book”

The MRTD Manufacturer combines the IC with hardware for the contactless interface, and embeds the inlay in the passport book.

Step5 “MRTD Manufacturing – Pre-Personalization”

The MRTD Manufacturer equips MRTD’s chips with pre-personalization Data.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

1.4.3.3 Phase 3 “Personalization of the MRTD”

Step6 “Personalization”

The personalization of the MRTD includes

- (i) the survey of the MRTD holder’s biographical data,
- (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- (iii) the printing of the visual readable data onto the physical MRTD,
- (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and
- (v) configuration of the TSF if necessary.

The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of

- (i) the digital MRZ data (EF.DG1),
- (ii) the digitized portrait (EF.DG2), and
- (iii) the Document security object.

The signing of the Document security object by the Document signer [R12] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Application Note 5: *The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [R8], section 92) comprise (but are not limited to) the Personalization Agent Key(s) and the Chip Authentication Private Key.*

Application Note 6: *This Security Target [R6] distinguishes between the Personalization Agent as an entity known to the TOE and the Document Signer as an*

entity in the TOE IT environment signing the Document security object as described in [R12]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization, but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows for fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

1.4.3.4 Phase 4 “Operational Use”

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

Application Note 7: *The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.*

Application Note 8: *This ST considers the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore defines the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. The national body of the issuing State or Organization is responsible for these specific production steps. Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the “Operational Use” (phase 4) have to be considered in the product evaluation process under AGD assurance class.*

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

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

1.5 TOE Description

1.5.1 Physical scope of the TOE

The physical TOE is composed of the following:

- the integrated circuit chip SB23YR80B (microcontroller) programmed with the operating system and with the passport application.

The SB23YR80 is a dual contactless high security microcontroller unit, directly derived from the ST23YR80 by the addition of a public key cryptography library named Neslib 3.0 SB. The Neslib library provides the most commonly used operations in symmetric and asymmetric key cryptographic algorithms and protocols, such as specialized functions for AES cryptography, RSA cryptography, Elliptic Curves Cryptography (ECC) and SHA-1, SHA-224 and SHA-256 secure hashing (please note that no AES cryptography is used by the TOE).

The Neslib library is integrated by the Developer in the code and is embedded in the product User ROM.

The chip received a Common Criteria certification at the EAL6 assurance level augmented with ALC_FLR.1 [R1][R2][R28] with certification ID:

ANSSI-CC-2010/02

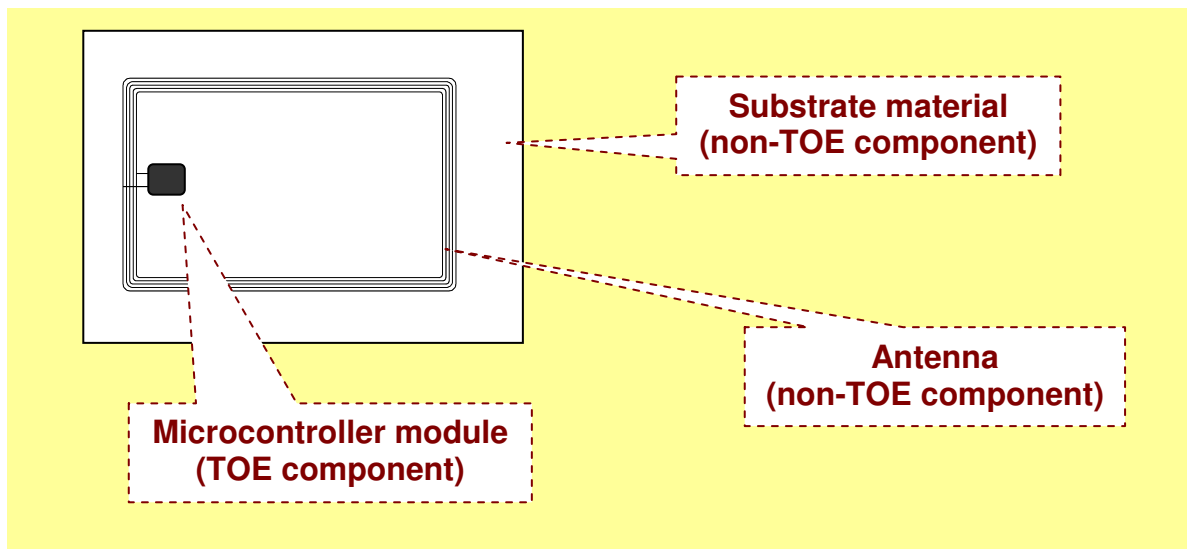
The certified version of the IC is the revision B.
The platform's certificate is valid and up-to-date.

1.5.2 Other non-TOE physical components

The antenna and the substrate of the inlay are not part of the TOE.

Figure 1-2 shows a picture of the inlay components, distinguishing between TOE components and non-TOE components.

Figure 1-2 Inlay components



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
- MRTD application
- security data objects

The SOMA801STM 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
- Management of the security policies

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

- full support of the ICAO MRTD 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 MRTD application.

Before the initialization, access to IC's resources is protected by a symmetric cryptographic mechanism requiring a mutual authentication between the Initialization System and the e-Passport.

The IC Manufacturer stores identification data, and the MRTD Manufacturer keys.

In the pre-personalization phase, the MRTD Manufacturer stores the Personalization Agent keys, as well as keys and data required by the authentication mechanisms used in the subsequent phases.

In the personalization phase, the Personalization Agent stores the ICAO application data, the BAC keys and other data required by the authentication mechanisms used in the subsequent phases.

Once the passport is in the Operational state, no data can be deleted or modified, except for the current date, the trustpoint and of the EF.CVCA file which can also be modified.

2. Conformance claims

2.1 Common Criteria Conformance

This Security Target claims conformance to:

- Common Criteria version 3.1 revision 4, International English Version [R8][R9][R10], as follows:
 - Part 2 (security functional requirements) extended
 - Part 3 (security assurance requirements) conformant

The software part of the TOE runs on the chip STMicroelectronics SB23YR80B. This integrated circuit is certified against Common Criteria at the assurance level EAL6+.

2.2 Protection Profile Conformance

This ST claims strict conformance to:

- BSI-CC-PP-0056 Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control version 1.10 25th March, 2009 [R6].

Application Note 9: *The TOE is required to fulfill the “Security Target for the SOMA801STM Electronic Passport, Basic Access Control” [R11] as a premise to this security target.*

2.3 Package Conformance

This Security Target claims conformance to:

- EAL4 assurance package augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [R10]

2.4 Conformance Rationale

The parts of the TOE listed in the Protection Profile [R6] correspond to the ones listed in section 1.4 of this ST.

In this ST, the TOE will be delivered from the IC Manufacturer to the MRTD Manufacturer after Step3 “IC Manufacturing” of Phase 2, as a chip, in accordance with Application Note 6 of the PP [R6]. At TOE delivery, there is no user data or machine readable data available. The EF.DG14 file, containing part of the user data, is written by the MRTD Manufacturer in Step5 “MRTD Manufacturing – Pre-Personalization” of Phase 2. The remaining user data as well as applicative files are written by the Personalization Agent, during Phase 3 “Personalization of the MRTD”.

The security problem definition of this ST is taken from the one in the PP with the following modifications:

- New subjects “Initialization and Pre-personalization Terminal” and “Personalization Terminal” have been added as a specialization of the “Terminal” subject from the PP. The introduction of these subjects does not lower security as a 112 bit TDES mutual authentication mechanism is required.
- Some security objectives for the TOE have been modified in a more restrictive way with respect to the PP, as shown in Table 2-1.

Table 2-1 Modified security objectives

Security Objective	Definition	Operation
OT.AC_Pers	Access Control for Personalization of logical MRTD.	Modified in a more restrictive way as data addition is not allowed at all after personalization
OT.Identification	Identification and Authentication of the TOE	Modified in a more restrictive way as access to TOE identification data in Phase 4 is restricted to a BAC authenticated Inspection System only (the Personalization Agent cannot access identification data after personalization).

The functional requirements described in section 6 of this ST correspond to the ones in section 5 of the PP [R6].

Table 2-2 shows assignment changes or refinements/iterations/additions with respect to the PP security functional requirements for the TOE. These changes do not lower the TOE security and, in some cases, changed requirements are more restrictive than the ones from the PP.

Table 2-2 SFRs assignment changes, refinements, iterations and additions

Security Functional Requirement	Operation
Change: FCS_CKM.1/DH FCS_CKM.1/ECDH Cryptographic key generation	The SFR FCS_CKM.1 in the PP has been split up in two SFRs to distinguish between the requirement for the Diffie-Hellman generation algorithm (FCS_CKM.1/DH) and the one for the Elliptic Curves Diffie-Hellman generation algorithm (FCS_CKM.1/ECDH). To this end an iteration was used.
Change: FCS_COP.1/SIG_VER_RSA FCS_COP.1/SIG_VER_ECDSA Signature verification	The SFR FCS_COP.1/SIG_VER in the PP has been split up in two SFRs to distinguish between the requirement for signature verification with RSA (FCS_COP.1/SIG_VER_RSA) and the one for signature verification with ECDSA (FCS_COP.1/SIG_VER_ECDSA). To this end an iteration was used.
Addition: FMT_MTD.1/ADDTSF_WRITE Management of TSF data – additional TSF data write	Iteration that specifies additional TSF data written in personalization
Change: FIA_UAU.4 single use authentication mechanisms – single use authentication of the Terminal by the TOE	This SFR now also relates to the MRTD Manufacturer Authentication (cf. Application Note 40:).
Change: FIA_UAU.5 multiple authentication mechanisms	the MRTD Manufacturer has been added as a user allowed to authenticate to the passport (cf. Application Note 41:).
Change: FMT_MTD.1/INI_DIS	This SFR has been modified in a more restrictive way with respect to the PP since access conditions to initialization and pre-personalization data cannot be modified after Phase 2 “Manufacturing”.
Change: FMT_SMR.1.1	This SFR has been modified to distinguish the roles IC Manufacturer and MRTD Manufacturer.

3. Security Problem Definition

3.1 Introduction

3.1.1 Assets

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

Logical MRTD sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG.4)

Application Note 10: *Due to interoperability reasons the ICAO Doc9303 [R12] requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG14, DG.16. Note the BAC mechanism may not resist attacks with high attack potential.*

Application Note 11: *EF.DG15 is not present in the list of the assets because the SOMA801STM operating system does not support Active Authentication which, therefore, is not addressed by this security target. As an alternative to Active Authentication the SOMA801STM operating system provides the Chip Authentication mechanism.*

A sensitive asset is the following more general one.

Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD's holder is used by the traveler to prove his possession of 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 completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.
- **Personalization Agent:** The agent who is acting on 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 ICAO Doc 9303 [R12].

- **Country Verifying Certification Authority:** The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.
- **Document Verifier:** The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.
- **Terminal:** A terminal is any technical system communicating with the TOE through the contactless interface.
- **Inspection system (IS):** A technical system used by the border control officer of the receiving State (i) in examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

The **Basic Inspection System (BIS):**

- i. contains a terminal for the contactless communication with the MRTD's chip,
- ii. implements the terminals part of the BAC Mechanism and
- iii. 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.

The **General Inspection System (GIS)** is a Basic Inspection System which implements additionally the Chip Authentication Mechanism.

The **Extended Inspection System (EIS)** in addition to the General Inspection System

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

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

- **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 manipulate the logical MRTD without authorization,
 - II. To read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or
 - III. To forge a genuine MRTD

Application Note 12: *Note that an attacker trying to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD) is not considered by this PP since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Key that is covered by [R11]. The same holds for the confidentiality of the user data EF.DG1, EF.DG2, EF.DG5 to EF.DG14, EF.DG16 as well as EF.SOD and EF.COM.*

Application Note 13: *An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore, the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.*

- **Pre-personalization Terminal (PPT):** A system used by the MRTD Manufacturer to perform TOE pre-personalization in phase 2; it allows to write user and TSF data in the logical MRTD, by implementing the terminals part of a pre-personalization process (described in the guidance documentation), using a secure messaging mechanism with diversified keys.
- **Personalization Terminal (PT):** A system used by the Personalization Agent to perform TOE personalization and configuration in phase 3; it allows to write user and TSF data in the logical MRTD, by implementing the terminals part of a personalization process (described in the guidance documentation), using a secure messaging mechanism with diversified keys.

Application Note 14: *The new subjects "Initialization and Pre-personalization Terminal" and "Personalization Terminal" are a specialization of the "Terminal" subject from the PP. The introduction of these subjects does not impact on the security of the TOE, since they are required to establish a mutual authentication based on 112 bit TDES cryptography and the respective authentication keys are destroyed at the completion of phase 2 (Initialization and Pre-personalization Terminal) and phase 3 (Personalization Terminal).*

3.2 Assumptions

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

- **A.MRTD_Manufact** **MRTD manufacturing on steps 4 to 6**
It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft of unauthorized use).
- **A.MRTD_Delivery** **MRTD delivery during steps 4 to 6**

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

- **A.Pers_Agent Personalization of the MRTD's chip**

The Personalization Agent ensures the correctness of:

- i. the logical MRTD with respect to the MRTD holder,
- ii. the Document BAC Keys,
- iii. the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip and
- iv. the Document Signer Public Key Certificate (if stored on the MRTD's chip).

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

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

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

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

The Basic Inspection System for global interoperability

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

The Basic Inspection System reads the logical MRTD being under Basic Access Control and performs the Passive Authentication to verify the logical MRTD. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System:

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

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

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair.

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

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

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

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

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

3.3 Threats

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

Application Note 15: *The threats T.Chip_ID and T.Skimming (cf [R11]) are averted by the mechanism described in the BAC ST (cf. P.BAC-PP). which cannot withstand an attack with high attack potential thus these are not addressed here. T_Chip_ID addresses the threat of tracing the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. T.Skimming addresses the threat of imitating the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Both attacks are conducted by an attacker who cannot read the MRZ or who does not know the physical MRTD in advance.*

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

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

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip. The attack T.Read_Sensitive_Data is similar to the threats T.Skimming (cf. [R11]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are

stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visual readable on the physical MRTD as well.

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

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

• **T.Forgery** **Forgery of data on MRTD's chip**

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

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

Asset: authenticity of logical MRTD data

• **T.Counterfeit** **Counterfeit of MRTD's chip**

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

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

Asset: authenticity of logical MRTD data

The TOE shall avert the threat as specified below.

- **T.Abuse-Func Abuse of Functionality**

Adverse action: An attacker may use functions of the TOE which shall not be used in “Operational Use” phase in order:

- i. to manipulate User Data,
- ii. to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or
- iii. to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

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

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

- **T.Information_Leakage Information Leakage from MRTD’s chip**

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

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

Asset: confidentiality logical MRTD and TSF data

- **T.Phys_Tamper Physical Tampering**

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

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

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

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

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

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

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

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

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

- i. deactivate or modify security features or functions of the TOE or
- ii. circumvent 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 misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

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

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

3.4 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 (see CC part 1, sec. 3.2 [R8]).

- **P.BAC-PP Fulfillment of the Basic Access Control Protection Profile**

The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG14, DG16 as per the 'ICAO Doc 9303' [R12] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [R5] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

Application Note 16: *The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [R12] is addressed by the [R5] (cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG3 and EF.DG4 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [R5]). The TOE shall protect the sensitive biometric reference data in EF.DG3 and EF.DG4 against attacks with high attack potential. Due to the different resistance, the protection of EF.DG3 and EF.DG4 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG2 and EF.DG5 to EF.DG14, EF.DG16 are addressed by separated security targets, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates (cf. also to application note 2).*

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

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

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

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely, to set the initial configuration and to create the MRTD application.

The MRTD Manufacturer writes the Pre-Personalization Data which contains at least the Personalization Agent key.

- **P.Personalization Organization only** **Personalization of the MRTD by issuing State or Organization only**

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by the Issuing State or Organization only.

4. Security Objectives

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

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and 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 may be written only during and can not be changed after personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Application Note 17: *The OT.AC_Pers implies that*

- (1) *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,*
- (2) *The Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is not provided.*

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

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

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

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

The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

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

The TOE must provide means to store IC Identification and Pre-Personalization Data in its 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”. The storage of the Pre-Personalization data includes writing the Personalization Agent Key(s).

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

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

Application Note 18: *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 matches the Chip Authentication Private Key of the MRTD’s chip. This certificate is provided by:

- the Chip Authentication Public Key (EF.DG14) in the LDS [R12] and*
- 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**

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to:

- disclose critical User Data,
- manipulate critical User Data of the IC Embedded Software,
- manipulate Soft-coded IC Embedded Software or
- bypass, deactivate, change or explore security features or functions of the TOE.

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

• **OT.Prot_Inf_Leak** **Protection against Information Leakage**

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

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

Application Note 19: *This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.*

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

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

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

• **OT.Prot_Malfunction** **Protection against Malfunctions**

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

Application Note 20: *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 Operational Environment

Issuing State or Organization

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

- **OE.MRTD_Manufact** **Protection of the MRTD Manufacturing**

Appropriate functionality testing of the TOE shall be used in step 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

- **OE.MRTD_Delivery** **Protection of the MRTD delivery**

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
 - origin and shipment details,
 - reception, reception acknowledgement,
 - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

- **OE.Personalization** **Personalization of logical MRTD**

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

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

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

The issuing State or Organization must:

- generate a cryptographic secure Country Signing CA Key Pair,
- ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment and
- distribute the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity.

The issuing State or Organization must:

- generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys,
- sign Document Security Objects of genuine MRTD in a secure operational environment only, and
- distribute the Certificate of the Document Signer Public Key to receiving States and Organizations.

The digital signature in the Document Security Object relates to all data in the data groups EF.DG1 to EF.DG16 if stored in the LDS according to [R12].

- **OE.Auth_Key_MRTD MRTD Authentication Key**

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

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

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

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

- **OE.BAC_PP Fulfilment of the Basic Access Control Protection Profile**

It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [R5]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data.

Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

Receiving State or Organization

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

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

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability

- i. includes the Country Signing 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 [R12].

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 Document Security Objects and the integrity data elements of the logical MRTD before they are used. The Receiving States and Organizations must manage the Country Signing CA Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

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

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

Application Note 21: *The figure 2.1 in [R7] supposes that the GIS and the EIS follow the order*

- i. *running the Basic Access Control Protocol,*
- ii. *reading and verifying only those parts of the logical MRTD that are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key),*
- iii. *running the Chip Authentication Protocol, and*
- iv. *reading and verifying the less-sensitive data of the logical MRTD after Chip*
- v. *Authentication.*

The supposed sequence has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. The inspection system will prevent additionally eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. Note that reading the less sensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this PP. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

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

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

4.3 Security Objective Rationale

Table 4-1 provides an overview for security objectives coverage.

Table 4-1 Security Objective Rationale

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.BAC-PP	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_Systems
T.Read_Sensitive_Data			x												x					x
T.Forgery	x	x						x					x				x	x		
T.Counterfeit					x									x			x			
T.Abuse-Func						x														
T.Information_Leakage							x													
T.Phys-Tamper								x												
T.Malfunction									x											
P.BAC-PP																x				
P.Sensitive_Data			x												x					x
P.Manufact				x																
P.Personalization	x			x								x								
A.MRTD_Manufact										x										
A.MRTD_Delivery											x									
A.Pers_Agent												x								
A.Insp_Sys																	x		x	
A.Signature_PKI													x				x			
A.Auth_PKI															x					x

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

The OSP **P.Manufact** “Manufacturing of the MRTD’s chip” requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by **OT.Identification**.

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

- i. 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
- ii. 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 Key(s) according to **OT.Identification** “Identification and Authentication of the TOE”. The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

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

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

The threat **T.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 MRTD’s chip authentication” using a authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_MRTD** “MRTD Authentication Key”.

According to **OE.Exam_MRTD** “Examination of the MRTD passport book” the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD’s chip.

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

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

The assumption **A.MRTD_Manufact** “MRTD manufacturing on step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_Manufact** “Protection of the MRTD Manufacturing” that requires to use security procedures during all manufacturing steps.

The assumption **A.MRTD_Delivery** “MRTD delivery during step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_Delivery** “Protection of the MRTD delivery” that requires to use security procedures during delivery steps of the MRTD.

The assumption **A.Pers_Agent** “Personalization of the MRTD’s chip” is covered by the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD” including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

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

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

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

5. Extended Components Definition

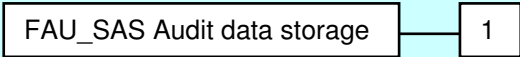
This ST uses components defined as extensions to CC part 2 [R9]. Some of these components are defined in [R4], other components are defined in the protection profile [R6].

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 [R6]. 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.

Table 5-1 Family FAU_SAS

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
<i>Dependencies:</i>	No Dependencies.
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.

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 [R6]. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

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

Table 5-2 Family FCS_RND

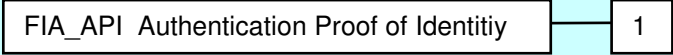
FCS_RND Generation of random numbers	
<i>Family behavior:</i>	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
<i>Component leveling:</i>	<div style="border: 1px solid black; padding: 5px; display: inline-block;"> FCS_RND Generation of random numbers </div> — <div style="border: 1px solid black; padding: 2px 5px; display: inline-block; margin-left: 10px;">1</div>
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
<i>Dependencies:</i>	No Dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: <i>a defined quality metric</i>].

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 [R6]. 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 22: *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. [R10] “Explicitly stated IT security requirements (APE_SRE)” from a TOE point of view.*

Table 5-3 Family FIA_API

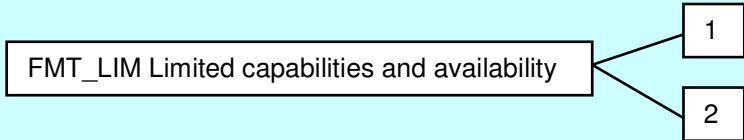
FIA_API Authentication Proof of Identity	
<i>Family behavior:</i>	This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.
<i>Component leveling:</i>	
FIA_API.1	Authentication Proof of Identity.
<i>Management:</i>	The 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
<i>Dependencies:</i>	No Dependencies.
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>].

5.4 Definition of the family FMT_LIM

The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

Table 5-4 Family FMT_LIM

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>	 <pre> graph LR A[FMT_LIM Limited capabilities and availability] --> B[1] A --> C[2] </pre>
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.

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

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

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

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

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

Application Note 23: *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*

- 1. 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 test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.*

The combination of both requirements shall enforce the policy.

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 [R6] 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 [R9].

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

Table 5-5 Family FPT_EMSEC

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;"> <div style="border: 1px solid black; padding: 2px; display: inline-block;">FPT_EMSEC TOE emanation</div> — <div style="border: 1px solid black; padding: 2px; display: inline-block; width: 20px; text-align: center;">1</div> </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 to 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
<i>Dependencies:</i>	No dependencies.
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>].

6. Security Requirements

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 [R8] of the CC. Each of these operations is used in this PP.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word “refinement” in bold text and the added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized like *this*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [R9]. The operation “load” is synonymous to “import” used in [R9].

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.

Dependencies: No dependencies.

FAU_SAS.1.1	The TSF shall provide <u>the Manufacturer</u> ³ with the capability to store <u>the IC Identification Data</u> ⁴ in the audit records.
-------------	--

Application Note 24: *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).*

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/DH Cryptographic key generation - Diffie-Hellman keys

Hierarchical to: No other components.

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

³ [assignment: *authorised user*]

⁴ [assignment: *list of audit information*]

<p>FCS_CKM.1.1/ DH</p>	<p>The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3 [R27]⁵</u> and specified cryptographic key sizes: <u>bit length of the modulus equal to or shorter than 2048 and bit length of the exponent equal to or shorter than 2048⁶</u>, that meet the following: <u>[R7], Annex A.1⁷</u>.</p>
----------------------------	---

Application Note 25: *The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [R7], sec. 3.1 and Annex A.1. This protocol is based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf [R27]). The shared secret value is used to derive the Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [R12], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC.*

FCS_CKM.1/ECDH Cryptographic key generation - Elliptic Curves Diffie-Hellman keys

Hierarchical to: No other components.

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

<p>FCS_CKM.1.1/ ECDH</p>	<p>The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: <u>ECDH compliant to ISO 15946 [R24]⁸</u> and specified cryptographic key sizes: <u>160 bit – 521 bit⁹</u>, that meet the following: <u>[R7], Annex A.1¹⁰</u>.</p>
------------------------------	---

Application Note 26: *The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [R7], sec. 3.1 and Annex A.1. This protocol is based on the ECDH compliant to ISO 15496 (i.e. an elliptic curve cryptography algorithm) (cf. [R7], Annex A.1 and [R24] for details). The shared secret value is used to derive the*

⁵ [selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946]

⁶ [assignment: cryptographic key sizes]

⁷ [assignment: list of standards]

⁸ [selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946]

⁹ [assignment: cryptographic key sizes]

¹⁰ [assignment: list of standards]

Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [R12], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC.

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 Cryptographic key destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1/ MRTD	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: physical deletion by overwriting the memory data with zeros ¹¹ that meets the following: none ¹² .
----------------------	--

Application Note 27: *The TOE shall destroy the BAC Session Keys:*

- i. after detection of an error in a received command by verification of the MAC, and*
- ii. after successful run of the Chip Authentication Protocol.*

The TOE shall destroy the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

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 Cryptographic operation – Hash for Key Derivation by MRTD

Hierarchical to: No other components.

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

¹¹ [assignment: *cryptographic key destruction method*]

¹² [assignment: *list of standards*]

FCS_COP.1.1/ SHA	The TSF shall perform <u>hashing</u> ¹³ in accordance with a specified cryptographic algorithm <u>SHA-1, SHA-224, SHA-256</u> ¹⁴ and cryptographic key sizes <u>none</u> ¹⁵ that meet the following: <u>FIPS 180-2 [R25]</u> ¹⁶ .
------------------	---

Application Note 28: *The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication mechanism (cf. [R12], annex E.1, cf. [R5] also). The Chip Authentication Protocol may use SHA-1 (cf. [R7], normative appendix 5, A5.1). The TOE may implement additional hash functions SHA-224, and SHA-256 for the Terminal Authentication Protocol (cf. [R7], Annex A.2.2 for details).*

Application Note 29: *For secure hashing with hash functions SHA, the TOE makes use of the STMicroelectronics Neslib library. This library is Common Criteria certified at the assurance level EAL6+.*

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

Hierarchical to: No other components.

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

FCS_COP.1.1/ SYM	The TSF shall <u>perform secure messaging – encryption and decryption</u> ¹⁷ in accordance with a specified cryptographic algorithm <u>TDES in CBC mode</u> ¹⁸ and cryptographic key sizes <u>112 bit</u> ¹⁹ that meet the following: <u>TR-03110 [R7]</u> ²⁰ .
------------------	---

Application Note 30: *This SFR requires the TOE to implement the cryptographic primitive Triple-DES for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol according to the FCS_CKM.1. Furthermore the SFR is used for authentication attempts Note the TDES in CBC mode with zero initial vector include also the TDES in*

¹³ [assignment: list of cryptographic operations]

¹⁴ [selection: SHA-1, SHA-224, SHA-256 or other approved algorithms]

¹⁵ [assignment: cryptographic key sizes]

¹⁶ [selection: FISP 180-2 or other approved standards]

¹⁷ [assignment: list of cryptographic operations]

¹⁸ [assignment: cryptographic algorithm]

¹⁹ [assignment: cryptographic key sizes]

²⁰ [assignment: list of standards]

ECB mode for blocks of 8 byte used to check the authentication attempts of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

FCS_COP.1/MAC Cryptographic operation – MAC

Hierarchical to: No other components.

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

FCS_COP.1.1/MAC	The TSF shall perform <u>secure messaging – message authentication code</u> ²¹ in accordance with a specified cryptographic algorithm <u>Retail MAC</u> ²² and cryptographic key sizes <u>112 bit</u> ²³ that meet the following: <u>TR-03110 [R7]</u> ²⁴ .
-----------------	---

Application Note 31: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Chip Authentication Protocol according to the FCS_CKM.1. The Retail-MAC as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 (cf [R5]) is DES resp. two-key Triple-DES base.

FCS_COP.1/SIG_VER_RSA Cryptographic operation – Signature verification by MRTD with RSA

Hierarchical to: No other components.

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

FCS_COP.1.1/SIG_VER_RSA	The TSF shall perform <u>digital signature verification</u> ²⁵ in accordance with a specified cryptographic algorithm <u>RSA as specified in Table 6-1</u> ²⁶ and cryptographic key sizes: <u>bit length of the modulus equal to 1024, 1280, 1536, 2048 or 3072</u> ²⁷ that meet the following: <u>RSA PKCS#1 [R26]</u> ²⁸
-------------------------	---

²¹ [assignment: list of cryptographic operations]

²² [assignment: cryptographic algorithm]

²³ [assignment: cryptographic key sizes]

²⁴ [assignment: list of standards]

²⁵ [assignment: list of cryptographic operations]

²⁶ [assignment: list of cryptographic operations]

Table 6-1 RSA algorithms for signature verification in Terminal Authentication ([R7])

Object Identifier	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

Application Note 32: *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.*

Application Note 33: *For RSA cryptography the TOE makes use of the STMicroelectronics Neslib library. This library is Common Criteria certified at the assurance level EAL6+.*

FCS_COP.1/SIG_VER_ECDSA Cryptographic operation – Signature verification by MRTD with ECDSA

Hierarchical to: No other components.

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

FCS_COP.1.1/SIG_VER_ECDSA	The TSF shall perform <u>digital signature verification</u> ²⁹ in accordance with a specified cryptographic algorithm <u>ECDSA with SHA-1, SHA-224 or SHA-256 as specified in Table 6-2</u> ³⁰ and cryptographic key sizes: <u>160, 192, 224 or 256 bit</u> ³¹ that meet the following: <u>FIPS 186-2</u> [R23]
---------------------------	---

Table 6-2 ECDSA algorithms for signature verification in Terminal Authentication ([R7])

Object Identifier	Signature	Hash
id-TA-ECDSA-SHA-1	ECDSA	SHA-1

²⁷ [assignment: cryptographic key sizes]

²⁸ [assignment: list of standards]

²⁹ [assignment: list of cryptographic operations]

³⁰ [assignment: list of cryptographic operations]

³¹ [assignment: cryptographic key sizes]

Object Identifier	Signature	Hash
id-TA-ECDSA-SHA-224	ECDSA	SHA-224
id-TA-ECDSA-SHA-256	ECDSA	SHA-256

Application Note 34: *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.*

Application Note 35: *For ECDSA cryptography the TOE makes use of the STMicroelectronics Neslib library. This library is Common Criteria certified at the assurance level EAL6+.*

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 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet BSI AIS-31 functionality class P2 [R3] (see Application Note 37:) ³² .
-------------	---

Application Note 36: *This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.*

Application Note 37: *The composite TOE makes use of the true random number generator (TRNG) of the IC SB23YR80B. The TRNG has already been evaluated as conformant to class P2 of BSI-AIS31 with SOF level “high”. Random numbers are therefore suitable for the generation of:*

- signature key pairs
- session keys for symmetric encryption mechanisms
- random padding bits
- seeds for key generation

6.1.3 Class FIA Identification and Authentication

Application Note 38: *Table 6-3 provides an overview on the authentication mechanisms used including the algorithm and relevant key size [R12], [R7].*

³² [assignment: a defined quality metric]

Table 6-3 Overview on authentication SFR

Mechanism	SFR for the TOE	Algorithm (Key Size)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	TDES (112 bit keys) Retail MAC (112 bit keys)
Chip Authentication Protocol	FIA_API.1, FIA_UAU.5, FIA_UAU.6	TDES (112 bit keys) Retail MAC (112 bit keys) DH ECDH
Terminal Authentication Protocol	FIA_UAU.5	RSASSA-PKCS1-v1_5 ECDSA

Note the Chip Authentication Protocol as defined in this security target includes:

- the BAC authentication protocol as defined in ‘ICAO Doc 9303’ [R12] in order to gain access to the Chip Authentication Public Key in EF.DG14,
- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

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

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.

Dependencies: No dependencies.

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_DIS</u> 3. <u>to carry out the Chip Authentication Protocol</u>³³ <p>on behalf of the user to be performed before the user is identified.</p>
-------------	---

³³ [assignment: *list of TSF-mediated actions*]

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

Application Note 39: *In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the Document Basic Access Keys, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Basic Inspection System (cf. PP MRTD BAC [R5]) is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to run the BAC Authentication Protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol (i.e. the BAC mechanism is not seen as an independent mechanism in this PP, it is a mandatory part within the Chip Authentication Protocol, and thus noted here for reasons of completeness). After successful authentication of the chip the terminal may identify itself as*

- (i) *Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or*
- (ii) *if necessary and available by symmetric authentication as Personalization Agent (using the Personalization Agent Key).*

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 (Common Criteria part 2).

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

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>4. <u>to carry out the Chip Authentication Protocol</u>³⁴. <p>on behalf of the user to be performed before the user is authenticated.</p>
-------------	--

³⁴ [assignment: *list of TSF-mediated actions*]

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

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 Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to <ol style="list-style-type: none"> 1. <u>Terminal Authentication Protocol</u>, 2. <u>Authentication Mechanism based on TDES</u>³⁵.
-------------	---

Application Note 40: *The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalization Agent and of MRTD Manufacturer may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.*

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 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1	The TSF shall provide <ol style="list-style-type: none"> 1. <u>Terminal Authentication Protocol</u>, 2. <u>Secure messaging in MAC-ENC mode</u>, 3. <u>Symmetric Authentication Mechanism based on TDES</u>³⁶ to support user authentication.
-------------	---

³⁵ [selecion: *Triple-DES, AES or other approved algorithms*]

³⁶ [selection: *Triple-DES, AES or other approved mechanisms*]

FIA_UAU.5.2	<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 the Symmetric Authentication Mechanism with MRTD Manufacturer Keys.</u> 2. <u>the TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with Personalization Agent Keys.</u> 3. <u>After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.</u> 4. <u>The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism³⁷</u>
-------------	---

Application Note 41: *The MRTD Manufacturer holds a key for the Symmetric Authentication Mechanism. The MRTD Manufacturer may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the pre-personalization environment prevents eavesdropping to the communication between TOE and pre-personalization terminal.*

Application Note 42: *The Personalization Agent holds a key for the Symmetric Authentication Mechanism. The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System 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.*

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

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

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

³⁷ [assignment: rules describing how the multiple authentication mechanisms provide authentication]

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions <u>each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS</u> ³⁸ .
-------------	---

Application Note 43: *the BAC Mechanism and the Chip Authentication Protocol specified in [R12] include 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 for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticate the user for each received command and accept only those commands received from the initially authenticated user.*

6.1.3.6 FIA_API.1 Authentication Proof of Identity

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

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1	The TSF shall provide a <u>Chip Authentication Protocol according to [R7]</u> ³⁹ to prove the identity of the <u>TOE</u> ⁴⁰ .
-------------	---

Application Note 44: *This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [R7]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol DH and two session keys for secure messaging in ENC_MAC mode according to [R12]. , normative appendix 5, A5.1. The terminal verifies by means of secure messaging whether the MRTD’s chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication key (EF.DG14).*

³⁸ [assignment: list of conditions under which re-authentication is required]

³⁹ [assignment: authentication mechanism]

⁴⁰ [assignment: authorized user or rule]

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 (Common Criteria part 2).

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1	The TSF shall enforce the <u>Access Control SFP</u> ⁴¹ on <u>terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG14, EF.DG16 of the logical MRTD</u> ⁴² .
-------------	---

Application Note 45: Access to EF.DG15 is not listed in FDP_ACC.1.1 because this ST does not address Active Authentication.

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

Hierarchical to: No other components.

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

FDP_ACF.1.1	The TSF shall enforce the <u>Access Control SFP</u> ⁴³ to objects based on the following: <ol style="list-style-type: none"> 1. <u>Subjects</u>: <ol style="list-style-type: none"> a. <u>Personalization Agent</u>, b. <u>Extended Inspection System</u> c. <u>Terminal</u>, 2. <u>Objects</u>: <ol style="list-style-type: none"> a. <u>data EF.DG1, EF.DG2 and EF.DG5 to EF.DG14, EF.DG16 of the logical MRTD</u>, b. <u>data EF.DG3 and EF.DG4 of the logical MRTD</u>
-------------	--

⁴¹ [assignment: access control SFP]

⁴² [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

⁴³ [assignment: access control SFP]

	<ul style="list-style-type: none"> c. <u>data in EF.COM,</u> d. <u>data in EF.SOD,</u> <p>3. <u>Security attributes:</u></p> <ul style="list-style-type: none"> a. <u>authentication status of terminals,</u> b. <u>Terminal Authorization</u>⁴⁴. <p>-</p>
<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> <ul 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 Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read data in EF.DG3 of the logical MRTD</u> 3. <u>the successfully authenticated Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read data in EF.DG3 of the logical MRTD</u>⁴⁵
<p>FDP_ACF.1.3</p>	<p>The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u>⁴⁶.</p>
<p>FDP_ACF.1.4</p>	<p>The TSF shall explicitly deny access of subjects to objects based on the rule:</p> <ul 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>

⁴⁴ [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]

⁴⁵ [assignment: rules governing access among controlled subjects and controlled objects using controlled operations or controlled objects]

⁴⁶ [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

	<p>5. <u>Any Terminal is not allowed to modify any of the EF.DG1 to EF.DG14, EF.DG16 of the logical MRTD</u></p> <p>6. <u>Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD⁴⁷</u></p>
--	---

Application Note 46: *The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [R7], Annex A.5.1, table A.8. The TOE verifies the certificate chain established by the Country Verifying 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 Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.*

Application Note 47: *Note the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG14, EF.DG16 of the logical MRTD. According to P.BAC-PP this security features of the MRTD are not subject of this security target.*

Application Note 48: *Access to EF.DG.15 is not listed in FDP_ACF.1.2 because this ST does not address Active Authentication.*

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 Basic data exchange confidentiality

Hierarchical to: No other components.

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

FDP_UCT.1.1	The TSF shall enforce the <u>Access Control SFP⁴⁸</u> to be able to <u>transmit and receive⁴⁹</u> user data in a manner protected from unauthorized disclosure after Chip Authentication .
-------------	---

⁴⁷ [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

⁴⁸ [assignment: access control SFP(s) and/or information flow control SFP(s)]

⁴⁹ [selection: transmit, receive]

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 Data exchange integrity

Hierarchical to: No other components.

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

FDP_UIT.1.1	The TSF shall enforce the <u>Access Control SFP</u> ⁵⁰ to be able to <u>transmit and receive</u> ⁵¹ user data in a manner protected from <u>modification, deletion, insertion and replay</u> ⁵² errors after Chip Authentication .
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether <u>modification, deletion, insertion and replay</u> ⁵³ has occurred after Chip Authentication .

Rationale for Refinement: *Note that the Access Control SFP (cf. FDP_ACF.1.2) allows the Extended Inspection System (as of [R12] and [R5]) to access the data EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG14, EF.DG16 of the logical MRTD. Nevertheless there is explicitly no rule for preventing access to these data. More over their data integrity (cf. FDP_UIT.1) and confidentiality (cf. FDP_UCT.1) is ensured by the BAC mechanism being addressed and covered by [R5]. The fact that the BAC mechanism is not part of the PP in hand is addressed by the refinement “after Chip Authentication”.*

Application Note 49: *FDP_UCT.1 and FDP_UIT.1 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).*

6.1.5 Class FMT Security Management

Application Note 50: *The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.*

⁵⁰ [assignment: access control SFP(s) and/or information flow control SFP(s)]

⁵¹ [selection: transmit, receive]

⁵² [selection: modification, deletion, insertion, replay]

⁵³ [selection: modification, deletion, insertion, replay]

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 (Common Criteria part 2).

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: <ol style="list-style-type: none">1. <u>Initialization</u>,2. <u>Pre-Personalization</u>,3. <u>Personalization</u>⁵⁴.
-------------	---

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.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1	The TSF shall maintain the roles: <ol style="list-style-type: none">1. <u>IC Manufacturer</u>2. <u>MRTD Manufacturer</u>3. <u>Personalization Agent</u>4. <u>Country Verifier Certification Authority</u>5. <u>Documents Verifier</u>6. <u>Basic Inspection System</u>7. <u>domestic Extended Inspection System</u>8. <u>foreign Extended Inspection System</u>⁵⁵.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

⁵⁴ [assignment: *list of security management functions to be provided by the TSF*]

⁵⁵ [assignment: *the authorised identified roles*]

Application Note 51: Note that the MRTD also maintains the role Basic Inspection System due to a direct consequence of P.BAC-PP resp. OE.BAC-PP. Nevertheless this role is not explicitly listed in FMT_SMR.1.1, above since the TSF cannot maintain the role with respect to the assumed high attack potential due to the known weaknesses of the Document Basic Access Keys.

Application Note 52: 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.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1	<p>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></p> <ol style="list-style-type: none"> 1. <u>User Data to be disclosed or manipulated,</u> 2. <u>sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,</u> 3. <u>TSF data to be disclosed or manipulated,</u> 4. <u>software to be reconstructed and</u> 5. <u>substantial information about construction of TSF to be gathered which may enable other attacks⁵⁶.</u>
-------------	---

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.

Dependencies: FMT_LIM.1 Limited capabilities.

⁵⁶ [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>sensitive User Data (EF.DG3 and EF.DG4) to e disclosed,</u> 3. <u>TSF data to be disclosed or manipulated,</u> 4. <u>software to be reconstructed and</u> 5. <u>substantial information about construction of TSF to be gathered which may enable other attacks⁵⁷.</u>
-------------	--

Application Note 53: *The formulation of “Deploying Test Features ...” in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.*

Note that the term “software” in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

6.1.5.5 FMT_MTD.1 Management of TSF data

Application Note 54: *the following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.*

The TOE shall meet the requirement “Management of TSF data (FMT_MTD.1)” as specified below (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.

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

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to <u>write⁵⁸ the Initialization Data and Pre-personalization Data⁵⁹ to the Manufacturer⁶⁰.</u>
-------------------------	---

⁵⁷ [assignment: *limited capability and availability policy*]

⁵⁸ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

⁵⁹ [assignment: *list of TSF data*]

⁶⁰ [assignment: *the authorised identified roles*]

Application Note 55: *the pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent, which is the symmetric cryptographic Personalization Agent Authentication Keys*

Application Note 56: *Initialization Data are written by the IC Manufacturer and Pre-personalization Data are written by the MRTD Manufacturer, according to the description given in section 1.5.3.*

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to <u>disable read access for users to</u> ⁶¹ the <u>Initialization Data</u> ⁶² to <u>the IC Manufacturer and to the MRTD Manufacturer</u> ⁶³ .
-------------------------	--

Application Note 57: *After Phase 2 “Manufacturing” the read access conditions to Initialization Data and Pre-personalization Data cannot be modified by anyone. This is a more restrictive requirement than the one defined in the PP.*

Application Note 58: *According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing”. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by:*

- i. *allowing to write these data only once and*
- ii. *blocking the role Manufacturer at the end of the Phase 2.*

The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides an unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

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

⁶² [assignment: *list of TSF data*]

⁶³ [assignment: *the authorised identified roles*]

FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_INI	<p>The TSF shall restrict the ability to <u>write</u>⁶⁴ the:</p> <ol style="list-style-type: none"> 1. <u>initial Country Verifying Certification Authority Public Key,</u> 2. <u>initial Country Verifying Certification Authority Certificate,</u> 3. <u>initial Current Date</u>⁶⁵ <p>to <u>the Personalization Agent</u>⁶⁶.</p>
----------------------	---

Application Note 59: *The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalization phase or by the Personalization Agent (cf. [R7], sec. 2.2.6). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.*

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/CVCA_UPD	<p>The TSF shall restrict the ability to <u>update</u>⁶⁷ the:</p> <ol style="list-style-type: none"> 1. <u>Country Verifying Certification Authority Public Key,</u> 2. <u>Country Verifying Certification Authority Certificate</u>⁶⁸, <p>to <u>Country Verifying Certification Authority</u>⁶⁹.</p>
----------------------	--

Application Note 60: *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. [R7], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [R7], sec. 2.2.3 and 2.2.4).*

⁶⁴ [selection: *change_default, query, modify, delete, 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 [assignment: *list of TSF data*]

⁶⁹ [assignment: *the authorised identified roles*]

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/DATE	The TSF shall restrict the ability to <u>modify</u> ⁷⁰ the <u>Current Date</u> ⁷¹ 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>⁷²
------------------	--

Application Note 61: *The authorized roles are identified in their certificate (cf. [R7], 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 [R7], Annex A.3.3, for details).*

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_WRITE	The TSF shall restrict the ability to <u>write</u> ⁷³ the <u>Document Basic Access Keys</u> ⁷⁴ to the <u>Personalization Agent</u> ⁷⁵ .
-----------------------	--

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/ADDTSF_WRITE	The TSF shall restrict the ability to <u>write</u> ⁷⁶ <u>the Security Environment object and the Document Number</u> to the <u>Personalization Agent</u> ⁷⁷ .
--------------------------	--

⁷⁰ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁷¹ [assignment: *list of TSF data*]

⁷² [assignment: *the authorised identified roles*]

⁷³ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁷⁴ [assignment: *list of TSF data*]

⁷⁵ [assignment: *the authorised identified roles*]

Application Note 62: *The Security environment object stores links to internal data.*

Application Note 63: *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.

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

FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to load ⁷⁸ the <u>Chip Authentication Private Key</u> ⁷⁹ to the MRTD Manufacturer ⁸⁰
----------------------	--

Application Note 64: *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.

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

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read ⁸¹ : 1. <u>the Document Basic Access Keys.</u> 2. <u>the Chip Authentication Private key.</u> 3. <u>the Personalization Agent Keys</u> ⁸² to none ⁸³ .
-----------------------	--

Application Note 65: *The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.*

⁷⁶ [selection: *change_default, query, modify, dolete, clear, [assignment: other operations]*]

⁷⁷ [assignment: *the authorised identified roles*]

⁷⁸ [selection: *create, load*]

⁷⁹ [assignment: *list of TSF data*]

⁸⁰ [assigned: *the authorised identified roles*]

⁸¹ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

⁸² [assignment: *list of TSF data*]

⁸³ [assignment: *the authorised identified roles*]

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.

Dependencies: FMT_MTD.1 Management of TSF data

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

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

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

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

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

Application Note 66: *The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.*

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.

Dependencies: No dependencies.

FPT_EMSEC.1.1	The TOE shall not emit electromagnetic and current emissions ⁸⁴ in excess of intelligible threshold ⁸⁵ enabling access to <u>Personalization Agent Keys and Chip Authentication Private Key</u> ⁸⁶ and <u>EF.DG1 to EF.DG14, EF.DG16, EF.SOD, EF.COM</u> ⁸⁷
FPT_EMSEC.1.2	The TSF shall ensure <u>any users</u> ⁸⁸ are unable to use the following interface <u>smart card circuits contacts</u> ⁸⁹ to gain access to <u>Personalization Agent Keys and Chip Authentication Private Key</u> ⁹⁰ and <u>EF.DG1 to EF.DG14, EF.DG16, EF.SOD, EF.COM</u> ⁹¹

Application Note 67: *The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD’s chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) additional contacts according to ISO/IEC 7816-2 as well. This TOE does not support any contact based communication protocol like ISO/IEC 7816-3. Examples of measurable phenomena include, but are not limited to variations in the power*

⁸⁴ [assignment: type of emissions]

⁸⁵ [assignment: specified limits]

⁸⁶ [assignment: list of types of TSF data]

⁸⁷ [assignment: list of types of user data]

⁸⁸ [assignment: type of users]

⁸⁹ [assignment: type of connection]

⁹⁰ [assignment: list of types of TSF data]

⁹¹ [assignment: list of types of user data]

consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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 (Common Criteria part 2).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: <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.1⁹²</u>
-------------	--

6.1.6.3 FPT_TST.1 TSF testing

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up, and before any use of TSF data⁹³ to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

⁹² [assignment: list of types of failures in the TSF]

⁹³ [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]]

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.

Dependencies: No dependencies.

FPT_PHP.3.1	The TSF shall resist <u>physical manipulation and physical probing</u> ⁹⁴ to the <u>TSF</u> ⁹⁵ by responding automatically such that the SFRs are always enforced.
-------------	--

Application Note 68: *The TOE will use appropriate countermeasures implemented by the IC manufacturer to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here:*

- *assuming that there might be an attack at any time and*
- *countermeasures are provided at any time.*

6.2 Security Assurance Requirements for the TOE

The 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 6-4 summarizes the assurance components that define the security assurance requirements for the TOE.

Table 6-4 Assurance requirements at EAL4+

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ADV_COMP.1
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

⁹⁴ [assignment: *physical tampering scenarios*]

⁹⁵ [assignment: *list of TSF devices/elements*]

Assurance Class	Assurance Components
AVA	AVA_VAN.5

Application Note 69: *The TOE shall protect the assets against high attack potential under the assumption that the inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol (OE.Prot_Logical_MRTD). Otherwise the confidentiality of the standard data shall be protected against attacker with at least low attack potential (AVA_VAN.3).*

6.3 Security Requirements Rationale

6.3.1 Security functional requirements rationale

Table 6-5 provides an overview for security functional requirements coverage of security objectives.

Table 6-5 Coverage of Security Objectives for the TOE by SFR

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1				x					
FCS_CKM.1/DH	x	x	x		x				
FCS_CKM.1/ECDH	x	x	x		x				
FCS_CKM.4	x	x	x						
FCS_COP.1/SHA	x	x	x		x				
FCS_COP.1/SYM	x	x	x		x				
FCS_COP.1/MAC	x	x	x		x				
FCS_COP.1/SIG_VER_RSA	x		x						
FCS_COP.1/SIG_VER_ECDSA	x		x						
FCS_RND.1	x		x						
FIA_UID.1	x	x	x						
FIA_UAU.1	x	x	x						
FIA_UAU.4	x	x	x						
FIA_UAU.5	x	x	x						
FIA_UAU.6	x	x	x						
FIA_API.1					x				
FDP_ACC.1	x	x	x						
FDP_ACF.1	x	x	x						
FDP_UCT.1			x						
FDP_UIT.1		x							
FMT_SMF.1	x	x							

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FMT_SMR.1	x	x							
FMT_LIM.1						x			
FMT_LIM.2						x			
FMT_MTD.1/INI_ENA				x					
FMT_MTD.1/INI_DIS				x					
FMT_MTD.1/CVCA_INI			X						
FMT_MTD.1/CVCA_UPD			X						
FMT_MTD.1/DATE			X						
FMT_MTD.1/KEY_WRITE	x								
FMT_MTD.1/ADDTSF_WRITE	x		X						
FMT_MTD.1/CAPK		x	X		x				
FMT_MTD.1/KEY_READ	x	x	X		x				
FMT_MTD.3			X						
FPT_EMSEC.1	x						x		
FPT_TST.1							x		x
FPT_FLS.1							x		x
FPT_PHP.3							x	x	

The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FIA_UID.1, 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 object 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 and FIA_UAU.5. If the Personalization Terminal want to authenticate itself 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 (for the generation of the challenge), FCS_CKM.1, FCS_COP.1/SHA (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER_RSA and FCS_COP.1/SIG_VER_ECDSA (as part of the Terminal Authentication Protocol) and FIA_UAU.6 (for the re-authentication). If the Personalization Terminal wants to authenticate itself 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 (for the generation of the challenge) and FCS_COP.1/SYM (to verify the authentication attempt).

The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMSEC.1 the confidentiality of these keys.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6.

The SFR FIA_UAU.6 and FDP_UIT.1 requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1 (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys) and FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

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

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

The SFR FIA_UID.1 and FIA_UAU.1 requires the identification and authentication of the inspection systems. The SFR FIA_UAU.5 requires the successful Chip Authentication (CA) before any authentication attempt as Extended Inspection System. During the protected communication following the CA the reuse of authentication data is prevented by FIA_UAU.4.

The SFR FIA_UAU.6 and FDP_UCT.1 requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1 (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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 object data required for Chip Authentication and for Terminal Authentication according to SFR FMT_MTD.1/ADDTSF_WRITE.

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

The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 “Operational Use” violates the security objective OT.Identification.

The security objective **OT.Chip_Auth_Proof** “Proof of MRTD’s chip authenticity” is ensured by the Chip Authentication Protocol provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1 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 [R7] requires additional TSF according to FCS_COP.1/SHA (for the derivation of the session keys), FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging).

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

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

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

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

The security objective **OT.Prot_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

6.3.2 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 6-6 shows the dependencies between the SFR of the TOE.

Table 6-6 Dependencies between the SFR for the TOE

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1/DH	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/SYM, FCS_COP.1/MAC Fulfilled by FCS_CKM.4,
FCS_CKM.1/ECDH	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/SYM, FCS_COP.1/MAC Fulfilled by FCS_CKM.4,
FCS_CKM.4	[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]	Fulfilled by FCS_CKM.1
FCS_COP.1/SHA	[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	Justification 1 for non-satisfied dependencies Fulfilled by FCS_CKM.4
FCS_COP.1/SYM	[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	Fulfilled by FCS_CKM.1 Fulfilled by FCS_CKM.4
FCS_COP.1/MAC	[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	Fulfilled by FCS_CKM.1 Fulfilled by FCS_CKM.4
FCS_COP.1/SIG_VER_RS A FCS_COP.1/SIG_VER_EC DSA	[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	Fulfilled by FCS_CKM.1 Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_API.1	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1 Justification 2 for non-satisfied dependencies
FDP_UCT.1	[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]	Justification 3 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[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]	Justification 3 for non-satisfied dependencies Fulfilled by FDP_ACC.1

SFR	Dependencies	Support of the Dependencies
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/ADDTSF_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT.1/CVCA_UPD
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.

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

Justification 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

Justification 2: 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 3: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels

since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

Justification 4: 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 to 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 selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing, especially for the secure handling of the MRTD's material.

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

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 depends on:

- ADV_ARC.1, Security architectural description
- ADV_FSP.2, 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 Dependency Rationale 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 Security Assurance Requirements Rationale 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 Security Assurance Requirements Rationale, 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 given in Table 7-2.

7.1 Coverage of SFRs

7.1.1 SS.AG_ID_AUTH Agents Identification & Authentication

This security service meets the following SFRs:

FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC,
FCS_COP.1/SIG_VER_RSA, FCS_COP.1/SIG_VER_ECDSA, FIA_UID.1, FIA_UAU.1,
FIA_UAU.4, FIA_UAU.5, FIA_API.1.

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. Table 7-1 summarizes the authentication mechanisms for the various systems, later detailed in this section.

Table 7-1 Summary of authentication mechanisms

System type	MRTD Life-Cycle status	Authentication Mechanism
Initialization and Pre-personalization system	Non-Initialized	Symmetric authentication with MRTD Manufacturer Keys, as requested by FIA_UAU.4
Personalization System	Initialized	Symmetric authentication with Personalization Agent Keys, as requested by SFR FIA_UAU.4
Basic Inspection System	Operational	BAC with TDES algorithm and 112 byte Document Basic Access Keys
General Inspection System	Operational	BAC with TDES algorithm and 112 byte Document Basic Access Keys. Chip Authentication with either: <ul style="list-style-type: none"> • Diffie-Hellman (DH) algorithm and keys having bit length of the modulus up to 2048 and bit length of the exponent up to 2048 or • Elliptic curves Diffie-Hellman (ECDH) algorithm with keys having bit length of the modulus up to 521.
Extended Inspection System	Operational	BAC with TDES algorithm and 112 byte Document Basic Access Keys. Chip Authentication may use either: <ul style="list-style-type: none"> • Diffie-Hellman algorithm with keys having bit length of the modulus equal to or shorter than 2048 and bit length of the exponent equal to or shorter than 2048 or • ECDH algorithm with keys having bit length of the modulus up to 521. Terminal Authentication may use either: <ul style="list-style-type: none"> • RSA algorithm with SHA-1 or SHA-256 hashing algorithm as in Table 6-1 and key sizes up to 3072 or • ECDSA algorithm with SHA-1, SHA-224 or SHA-256 as in Table 6-2 and key sizes up to 256 bit.

The MRTD Manufacturer and the Personalization Agent authenticates themselves to the e-Passport by means of a mutual authentication mechanism (FIA_UID.1, FIA_UAU.1, FIA_UAU.5). The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and ICAO Doc 9303, normative appendix 5) (FCS_COP.1/SYM) and the message authentication code computation accords to Retail

MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) (FCS_COP.1/MAC).

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.

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 in [R11]) and at the end of the session, the session keys are securely erased (FCS_CKM.4).

The Basic Access System and the MRTD mutually authenticate by means of a Basic Access Control mechanism based on a three pass challenge-response protocol (FIA_UID.1, FIA_UAU.1, FIA_UAU.5). 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 is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and normative appendix 5 of the ICAO Doc 9303 [R12]) (FCS_COP.1/SYM), while the message authentication code is computed according to Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) (FCS_COP.1/MAC). These authentication keys are derived by the SHA-1 algorithm (FIPS 180-2) like described in the ICAO Doc 9303, normative appendix 5 [R12] [R13] (FCS_COP.1/SHA).

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-like mechanism is used for this authentication (FIA_UAU.5).

If passport inspection is performed on a General Inspection System or an Extended Inspection System, then the MRTD authenticity is proved executing the Chip Authentication Protocol. To this end two algorithms may be used: (i) a Diffie-Hellman key agreement compliant to PKCS #3 with key size up to 2048 bit or (ii) ECDH key agreement compliant to ISO15946 with key size up to 521 bit. 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, FIA_API.1).

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, FCS_COP.1/SIG_VER_RSA, FCS_COP.1/SIG_VER_ECDSA). Terminal Authentication attempts are only accepted after a successful Chip Authentication and a consequent restart of the Secure Messaging session with the strong keys computed in the Chip Authentication.

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

7.1.2 SS.SEC_MSG Data exchange with Secure Messaging

This security service meets the following SFRs:

FCS_CKM.1/DH, FCS_CKM.1/ECDH, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_CKM.4, FCS_COP.1/MAC, FCS_COP.1/SIG_VER_RSA, FCS_COP.1/SIG_VER_ECDSA, FIA_UAU.6, FIA_API.1.

This security service concerns the creation and the management of a secure communication channel for the sensitive data exchange between the TOE and the Inspection System. On this channel the data will be encrypted and authenticated with session keys (data TDES-encryption and MAC computation) such that the TOE is able to verify the integrity and authenticity of received data. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and ICAO Doc 9303, normative appendix 5), while the message authentication code is according to Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2). The session keys are calculated during the authentication phase. 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:

- inconsistent or missing MAC,
- wrong sequence counter,
- plain access.

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

7.1.3 SS.ACC_CNTRL 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, FDP_UIT.1, 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 (user data and TSF data) can only be accessed as defined by the access right written during the personalization process and allows the access to the TOE identification data in the Personalization phase. Furthermore, the access conditions allow to differentiate the roles based on the knowledge of secret keys. Any access not explicitly allowed is denied.

The Chip Authentication key pair (public key in DG14), the symmetric keys for the authentication of the Personalization Agent, the passport number, the application serial number and the Application Restricted Secret Code are written during the initialization phase by the MRTD Manufacturer.

The Document Basic Access Keys, the current date, the CVCA public key, the trustpoint, the EF.CVCA, the Document Number and the Security Environment object will be written during the personalization phase by the Personalization Agent.

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 SS.LFC_MNG 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 phases in the given order: manufacturing, personalization and operational use. The only role allowed to set the life cycle status is the Manufacturer.

The transition between the manufacturing phase and personalization phase is performed disabling the MRTD Manufacturer Keys.

7.1.5 SS.SW_INT_CHECK 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 doesn't allow to analyze, debug or modify TOE's software during the operational use. In phase 3 and 4 no commands are allowed to load executable code. Self tests will be executed at initial start-up on ROM area (this functionality is implemented by the underlying hardware).

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 SF warns the entity connected upon detection of an integrity error of the sensitive data stored within the TOE Scope of Control and preserves a secure state when failure is detected by TSF.

7.1.6 SS.SF_HW Security features provided by the hardware

This security service meets the following SFRs: FCS_RND.1, 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 chip already certified; a more detailed formulation of the security functions provided by the chip can be found in the related security target [R28].

7.1.7 SS.SIG_VER Verification of digital signatures

This security service meets the following SFRs: FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER_RSA, FCS_COP.1/SIG_VER_ECDSA, 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 signatures to be verified are based on (i) RSA according to PKCS#1 [R26] (see FCS_COP.1/SIG_VER_RSA) with key sizes up to 3072 bit or (ii) ECDSA with key sizes up to 256 (see FCS_COP.1/SIG_VER_ECDSA).

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 certificate of the Country Verifying Certification Authority is not expired

Table 7-2 shows the coverage of SFR by the security services described above.

Table 7-2 Coverage of SFRs by security services

	SS.AG_ID_AUTH Agents Identification & Authentication	SS.SEC_MSG Data exchange with Secure Messaging	SS.ACC_CNTRL Access Control of Stored Data Object	SS.LFC_MNG Life Cycle Management	SS.SW_INT_CHECK SW Integrity check of TOE's Assets	SS.SF_HW Security features provided by the hardware	SS.SIG_VER Verification of digital signatures
FAU_SAS.1			X				
FCS_CKM.1/DH		X					
FCS_CKM.1/ECDH		X					
FCS_CKM.4	X	X					
FCS_COP.1/SHA		X					X
FCS_COP.1/SYM		X					X
FCS_COP.1/MAC		X					X
FCS_COP.1/SIG_VER_RSA		X					X
FCS_COP.1/SIG_VER_ECDSA		X					X
FCS_RND.1						X	
FIA_UID.1	X						
FIA_UAU.1	X						
FIA_UAU.4	X						
FIA_UAU.5	X						
FIA_UAU.6		X					
FIA_API.1	X	X					
FDP_ACC.1			X				
FDP_ACF.1			X				
FDP_UCT.1			X				
FDP_UIT.1			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	

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 [R10].

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 same test chains in both the system test and in the validation phases.

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 platform (IC) will be covered in documents from the IC manufacturer. Security procedures described in such documents have been taken into consideration.

Table 7-3 shows the documentation that provides the necessary information related to the assurance requirements defined in this security target.

Table 7-3 Assurance Requirements documentation

Security Assurance Requirements	Documents
ADV_ARC.1	Description of the Security Architecture of the SOMA801STM embedded software
ADV_FSP.4	Functional Specification for the SOMA801STM embedded software
ADV_IMP.1	Source code of the SOMA801STM embedded software
ADV_TDS.3	Description of the Design of the SOMA801STM embedded software
ADV_COMP.1	Rationale for Embedded Software Design Compliance concerning the composite evaluation of the SOMA801STM electronic passport.
AGD_OPE.1	Personalization Guidance for the SOMA801STM electronic passport User Guidance for the SOMA801STM electronic passport
AGD_PRE.1	Pre-personalization guidance for the SOMA801STM 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	Life-cycle definition
ALC_TAT.1	Description of the tools and techniques.
ATE_COV.2	Coverage of Test Analysis for the SOMA801STM Electronic Passport
ATE_DPT.1	Depth of Test Analysis for the SOMA801STM Electronic Passport
ATE_FUN.1	Functional Test Specification for the SOMA801STM Electronic Passport Evidences of tests
ATE_IND.2	Documentation related to an independent test.
AVA_VAN.5	Documentation related to an independent vulnerability analysis.

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

8. References

8.1 Acronyms

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 Doc 9303)
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 Doc 9303)
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
IS	Inspection System
LDS	Logical Data Security
LCS	Life Cycle Status
MAC	Message Authentication Code
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
PP	Protection Profile
RAM	Random Access Memory
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	Security Target
TDES	Triple DES
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TR	Technical Report
VIZ	Visual Inspection Zone

8.2 Glossary

<i>Active Authentication</i>	Security mechanism defined in ICAO Doc 9303 [R12] 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 [R12] 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 Visual Inspection Zone (VIZ) and Machine Readable Zone (MRZ) on the biographical data page of a passport book or on a travel card or visa [R12].
<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 public key it contains (self-signed certificate).
<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 [R12].
<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 public 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 and message authentication of data transmitted between the MRTD's chip and the inspection system [R12]. 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}) [R12].
<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 [R12].
<i>Extended Access Control</i>	Security mechanism identified in BSI TR-03110 [R7] 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. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Keys and to get write and read access to the logical MRTD and TSF data.
<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 [R12].
<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.
<i>impostor</i>	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 [R12].
<i>Initialization Data</i>	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).
<i>inspection</i>	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity.
<i>Inspection System</i>	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.
<i>Integrated Circuit</i>	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
<i>integrity</i>	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the Issuing State or Organization
<i>Issuing Organization</i>	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the passport) [R12].
<i>Issuing State</i>	The Country issuing the MRTD [R12]
<i>Logical Data Structure</i>	The collection of groupings of DG's stored in the optional capacity expansion technology [R12]. The capacity expansion technology used is the MRTD's chip.

<p><i>Logical MRTD</i></p>	<p>Data of the MRTD holder stored according to the LDS [R12] as specified by ICAO on the contactless IC. It presents contactless readable data including (but not limited to):</p> <ul style="list-style-type: none"> i. personal data of the MRTD holder ii. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), iii. the digitized portraits (EF.DG2), iv. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and v. the other data according to LDS (EF.DG5 to EF.DG16).
<p><i>Machine Readable Travel Document</i></p>	<p>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 [R12].</p>
<p><i>Machine Readable Zone</i></p>	<p>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 [R12].</p>
<p><i>machine-verifiable biometrics feature</i></p>	<p>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.</p>
<p><i>MRTD application</i></p>	<p>Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes:</p> <ul style="list-style-type: none"> i. the file structure implementing the LDS [R12], ii. 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) and iii. the TSF Data including the definition the authentication data but except the authentication data itself.
<p><i>MRTD Basic Access Control</i></p>	<p>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.</p>
<p><i>MRTD holder</i></p>	<p>The rightful holder of the MRTD for whom the issuing</p>

	State or Organization personalized the MRTD.
<i>MRTD's chip</i>	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the LDS [R12].
<i>MRTD's chip Embedded Software</i>	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.
<i>Optional biometric reference data</i>	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.
<i>Passive Authentication</i>	Passive Authentication is a mechanism that ensures the authenticity of the DG's present in the LDS by: <ul style="list-style-type: none"> 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.
<i>Personalization</i>	The process by which the portrait, signature and biographical data are applied to the document [R12].
<i>Personalization Agent</i>	The agent delegated by the Issuing State or Organization to personalize the MRTD for the holder by <ul style="list-style-type: none"> 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.
<i>Personalization Agent Authentication Information</i>	TSF data used for authentication proof and verification of the Personalization Agent.
<i>Physical travel document</i>	Travel document in the form of paper, plastic and chip using secure printing to present data including (but not limited to): <ul style="list-style-type: none"> 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.
<i>Pre-personalized MRTD's chip</i>	MRTD's chip equipped with a unique identifier, the Personalization Agent Keys, 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 [R12].
<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>secure messaging</i>	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R15].
<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 [R8].
<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 [R8].

<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 [R12].
<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] **ANSSI:** *Certification Report ANSSI-CC-2010/02 SA23YR48/80B and SB23YR48/R80B Secure Microcontrollers, including the cryptographic library Neslib v2.0 or v3.0, in SA or SB configuration, February 1st, 2010*
- [R2] **ANSSI:** *Maintenance Report ANSSI-CC-2010/02-M01 Secured microcontrollers SA23YR48/80B and SB23YR48/R80B, including the cryptographic library Neslib v2.0 or v3.0, in SA or SB configuration, 19th March 2010*
- [R3] **BSI:** *Functionality classes and evaluation methodology for physical random number generators, AIS31, Version 1, 25.9.2001*
- [R4] **BSI:** *Security IC Platform Protection Profile version 1.0 15 June, 2007; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035*
- [R5] **BSI:** *Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Basic Access Control, Version 1.10, 25th March 2009, BSI-CC-PP-0055.*
- [R6] **BSI:** *Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control, Version 1.10, 25th March 2009, BSI-CC-PP-0056.*
- [R7] **BSI:** *Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11*
- [R8] **CCRA:** *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, version 3.1 rev.4, CCMB-2012-09-001*
- [R9] **CCRA:** *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, September 2012, version 3.1 rev.4, CCMB-2012-09-002*
- [R10] **CCRA:** *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, September 2012, version 3.1 rev 4, CCMB-2012-09-003*
- [R11] **Gep:** *Security Target SOMA801STM Electronic Passport, Basic Access Control” v1.0 04.03.2011.*
- [R12] **ICAO:** *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 – Doc 9303, Third Edition – 2008*

- [R13] **ICAO:** *SUPPLEMENT TO DOC 9303 – Release 11 – November 17, 2011*
- [R14] **IETF Network Working Group:** *Request For Comments 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.*
- [R15] **ISO/IEC:** *International Standard 7816-4 2005 Information Technology – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange – January 15, 2005*
- [R16] **ISO/IEC:** *International Standard 9797-1 1999 Information Technology – Security Techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher, 1999*
- [R17] **ISO/IEC:** *International Standard 14443-1 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 1: Physical characteristics.*
- [R18] **ISO/IEC:** *International Standard 14443-2 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 2: Radio frequency interface power and signal interface.*
- [R19] **ISO/IEC:** *International Standard 14443-3 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 3: Initialization and anticollision.*
- [R20] **ISO/IEC:** *International Standard 14443-4 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 4: Transmission protocol.*
- [R21] **JIL:** *Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.*
- [R22] **NIST:** *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*
- [R23] **NIST:** *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 186-2, DIGITAL SIGNATURE STANDARD (DSS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, January 2000*
- [R24] **ISO/IEC:** *International Standard 15946 – Information Technology – Security Techniques – Cryptographic techniques based on elliptic curves.*
- [R25] **NIST:** *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*

- [R26] **RSA Laboratories:** *PKCS#1 – RSA cryptography standard, An RSA Laboratories Technical Note, version 2.1 June 2002.*
- [R27] **RSA Laboratories:** *PKCS #3 - Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, version 1.4 November 1993.*
- [R28] **STMicroelectronics:** *SA23YR48B/SB23YR48B/SB23YR80B/SB23YR80B Security Target – Public Version, SMD_Sx23YRxx_ST_09_002 Rev.02.01, November 2009*

END OF DOCUMENT