Security Target Lite for CEITEC ePassport Module CTC21001 with BAC

Version 3.0 – 07/Dec/2016

Document History

1.0	Initial version
2.0	Minor corrections
3.0	Clarifications to section 7.1

Table of contents

1 Introduction 4
1.1 ST Lite reference and TOE reference 4
1.2 TOE overview 4
1.2.1 Usage and major security features for operational use 4
1.2.2 TOE type 6
1.2.3 Required non-TOE hardware, software and firmware 6
1.3 TOE description 6
1.3.1 Physical Scope of the TOE 7
Table 1 – TOE component identification 8
1.3.2 Logical Scope of the TOE 8
1.4 TOE life-cycle 9
Table 2 – Roles in the TOE life-cycle 10
1.4.1 Phase 1 “Development” 10
1.4.2 Phase 2 “Manufacturing” 10
1.4.3 Phase 3 “Personalization of the MRTD” 11
1.4.4 Phase 4 “Operational Use” 11
2 Conformance claims 12
2.1 Common Criteria conformance 12
2.2 Protection Profile conformance 12
2.3 Package conformance 12
3 Security problem definition 13
3.1 Introduction 13
3.2 Assumptions 15
3.3 Threats 16
3.4 Organizational security policies (OSPs) 19
4 Security objectives 21
4.1 Security objectives for the TOE 21
4.2 Security Objectives for the Operational Environment 23
4.3 Security Objective Rationale 25
5 Extended Components Definition 29
5.1 Definition of the Family FAU_SAS 29
5.2 Definition of the Family FCS_RND 29

5.3 Definition of the Family FMT_LIM 30
5.4 Definition of the Family FPT_EMSEC 32
6 Security requirements 34
6.1 Security functional requirements for the TOE 34
6.1.1 Class FAU Security Audit 34
6.1.2 Class FCS Cryptographic Support 34
6.1.3 Class FIA Identification and Authentication 37
6.1.4 Class FDP User Data Protection 40
6.1.5 Class FMT Security Management 42
6.1.6 Class FPT Protection of the Security Functions 45
6.2 Security Assurance Requirements for the TOE 47
6.3 Security Requirements Rationale 47
6.3.1 Security Functional Requirements Rationale 47
6.3.2 Dependency Rationale 50
6.3.3 Security Assurance Requirements Rationale 53
6.3.4 Security Requirements – Mutual Support and Internal Consistency 54
7 TOE summary specification 55
7.1 SF.AC_Pers: Access Control for Personalization 55
7.2 SF.Data_Int: Integrity of Personal Data 55
7.3 SF.Data_Conf: Confidentiality of personal Data 56
7.4 SF.Auth: Identification and Authentication 57
7.5 SM.Prot_Abuse_Func: Protection against Abuse of Functionality 57
7.6 SM.Prot_Inf_Leak: Protection against Information Leakage 57
7.7 SM.Prot_Phys_Tamper: Protection against Physical Tampering 58
7.8 SM.Prot_Malfunction: Protection against Malfunctions 58
8 List of abbreviations 59
9 References 61

1 Introduction

1.1 ST Lite reference and TOE reference

ST Lite identification:	CEITECSA 5.410.051, version 3.0
Author:	Product and Business Development Department (DP&N), CEITEC S.A.
Date:	7 December 2016
TOE identification:	CEITEC ePassport Module, CTC21001, version 1.0.
Applicant:	CEITEC S.A., Porto Alegre, Brazil
Compliant to:	BSI-CC-PP-0055, “Machine Readable Travel Document with ‘ICAO Application’, Basic Access Control” [1]
Assurance level:	EAL4 augmented by ALC_DVS.2
Keywords:	ePassport, MRTD, machine readable travel document, BAC, basic access control, ICAO, International Civil Aviation Organization.

1.2 TOE overview

The TOE is an electronic module for machine readable travel documents (MRTDs) based on the requirements of the International Civil Aviation Organization, as defined in ICAO Doc 9303 [2]. The TOE is developed and produced by CEITEC and delivered to the passport manufacturer as micro modules.

The passport manufacturer makes an ePassport book by embedding the TOE and an antenna into an ePassport book. Neither the antenna nor the ePassport book is part of the TOE. The passport manufacturer delivers the ePassport books with the antenna and the TOE installed on them to a Personalization Agent.

The Personalization Agent personalizes the MRZ information and biometric data of the face and fingerprints of the ePassport holder into the TOE along with the TSF data for authentication and secure messaging between the TOE and the Inspection System. The Personalization Agent is required to perform an authentication procedure in order to be allowed to personalize the module with the holder data.

After the personalization, an Inspection System shall be able to verify the ePassport presented by the ePassport holder using the secure messaging protocol defined by ICAO. The Inspection System is required to perform the Basic Access Control (BAC) procedure in order to be allowed to read the passport holder data.

1.2.1 Usage and major security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The TOE’s access control function for personalization contributes to assure the authenticity of the MRTD by verifying the access rights of the Personalization Agent. The TOE does not allow the holder data in a personalized MRTD to be altered or deleted. The traveler presents a MRTD to the Inspection System to prove his or her identity. The Inspection System is also required by the TOE to undergo an identification and authentication procedure before being granted

access to the data stored in the MRTD. Once this access is granted, the communication between TOE and Inspection System runs on a secure protocol in order to prevent violations of confidentiality of the holder's data.

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

For this ST the MRTD is viewed as unit of

(a) the physical MRTD as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD Holder

(1) the biographical data on the biographical data page of the passport book,

(2) the printed data in the Machine-Readable Zone (MRZ), and

(3) the printed portrait.

(b) the logical MRTD as data of the MRTD Holder stored according to the Logical Data Structure [2] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD Holder

(1) the digital Machine-Readable Zone Data (digital MRZ data, EF.DG1),

(2) the digitized portrait(s) (EF.DG2),

(3) optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,

(4) other data according to LDS (EF.DG5 to EF.DG16), and

(5) the Document Security Object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the ePassport book and the MRTD's chip is uniquely identified by the Document Number.

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

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [2]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This ST addresses the protection of the logical MRTD (i) in integrity by write only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism. This ST does not address the Active Authentication and the Extended Access Control as optional security mechanisms.

The Basic Access Control is a mandatory security feature supported by the TOE. The Inspection System (i) reads optically the MRZ, and (ii) authenticates itself as Inspection System by means of Document Basic Access Keys. After successful authentication of the Inspection System the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this Inspection System.

1.2.2 TOE type

The TOE is an electronic module for machine readable travel documents (MRTDs) based on the requirements of the International Civil Aviation Organization, as defined in ICAO Doc 9303 [2]. The TOE is developed and produced by CEITEC and delivered to the passport manufacturer as micro modules.

1.2.3 Required non-TOE hardware, software and firmware

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 encapsulated in a micro module and the IC Embedded Software. 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.

1.3 TOE description

The TOE is the CEITEC ePassport Module CTC21001, containing one contactless integrated circuit programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to [2].

The Target of Evaluation (TOE) comprises

(a) at the physical level:

- the contactless integrated circuit chip encapsulated on a micro module;
- IC Software, programmed on the chip;
- data necessary to enable the MRTD personalization (Pre-personalization Data), programmed on the chip; and
- the associated guidance documentation, i.e. guidance documentation delivered to the MRTD Manufacturer and personalization facility on a secure construction and personalization of the ePassport books using the TOE.

(b) at the logical level, functions that provide:

- access control for personalization
- integrity of personal data;
- confidentiality of personal data;
- identification and authentication;
- protection against abuse of functionality;
- protection against information leakage;
- protection against physical tampering;
- protection against malfunctions.

Application Note 1: The antenna and the inlay substrate that will be embedded along with the encapsulated chip into the passport book are not part of the TOE.

1.3.1 Physical Scope of the TOE

In this ST the physical TOE comprises the MRTD chip, encapsulated on a micro module, which provides the contacts for an external antenna. The non-volatile memory of the chip contains the IC Software and the Pre-personalization Data. The TOE also includes the MRTD Manufacturer and personalization facility guidance. The MRTD Manufacturer may provide additional guidance to the personalization facility but that additional guidance is not part of the TOE. The MRTD Manufacturer or the personalization facility may also provide guidance to the MRTD Holder but that guidance is not part of the TOE.

The antenna and its supporting substrate are not part of the TOE.

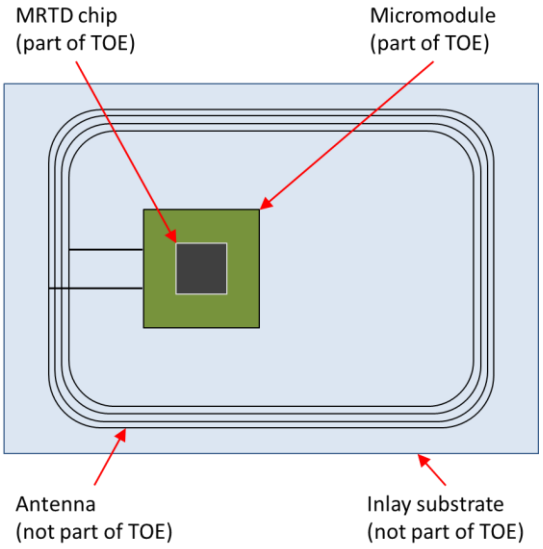


Figure 1 – Parts of the TOE and additional physical parts

The physical components of the TOE can be identified as follows:

Component	Version
Silicon Integrated Circuit	COP V1R0 R
IC Software	1.0.0.719
CEITECSA 5.410.031 - CTC21001 User Guidance	4.0
CEITECSA 5.410.022 - Personalization Protocol	5.0
CEITECSA 5.420.014 - Micromodule CTC21001 MM	R00

Table 1 – TOE component identification

The Pre-personalization Data written on the chip comprise:

- The IC identification number;
- The IC Private Key;
- The Personalization Agent Key;
- The inspection certificate chain;
- The personalization certificate chain; and
- The verification data for the certificates.

1.3.2 Logical Scope of the TOE

Functions performed by the TOE include:

- identification and authentication;
- access control for personalization;
- protection of integrity of personal data;
- protection of confidentiality of personal data;
- protection against abuse of functionality;
- protection against information leakage;
- protection against physical tampering; and
- protection against malfunctions.

Identification and authentication functions concern with the TOE personalization and with the operational stage of the TOE. At the personalization stage, the Personalization Agent must be successfully authenticated and establish a secure session between itself and the terminal for issuing the personalization commands.

At the operational stage, the Inspection System must authenticate himself using a BAC mechanism with keys derived from the MRZ information in order to read the biographical data of the MRTD Holder and TSF data. The optional biometric data can only be read after the Inspection System successfully performs a Chip Authentication and a Terminal Authentication procedure.

The authentication protocols and the data access control performed by the TOE assure that only authorized Personalization Agents are given access to TOE functions or data stored in the

TOE memory, and that the access is selective depending on the agent role and authentication level.

Integrity of the personal data is protected via control of the TOE life-cycle stage. The TOE enforces a unidirectional sequence of life-cycle phases, enabling or disabling TOE functions depending on the current phase. The life-cycle management checks the result of the Personalization Agent authentication and decides whether the TOE can be switched to the personalization state, kept in the pre-personalized state (awaiting a new agent authentication attempt) or be permanently disabled (if a potentially unsecure condition has been detected).

The TOE will only transition to the “Operational Use” phase if the personalization is complete. Any interrupted personalization (e.g. due to power loss) will be discarded and the personalization process will have to be executed from scratch on the next attempt. Changes and additions to data on a personalized TOE are prevented.

Confidentiality of personal data is protected by a secure communication mechanism between the TOE and external systems and via access control to regulate access to the assets stored on the TOE.

A secure communication session is established between the TOE and the Inspection System once the BAC procedure is successfully executed. The secure communication uses data encryption and message authentication according to [2] in order to protect the MRTD Holder’s data from eavesdropping and unauthorized access. If the communication session is finished or interrupted, the session keys are destroyed and the TOE requires that the Inspection System be re-authenticated by the BAC in order to resume the message exchange.

Assets stored in the TOE are protected by measures that enforce their confidentiality and/or integrity. The TOE private key for Chip Authentication and the code memory are not accessible externally after the “Manufacturing” phase of the TOE (the Chip Authentication is out of the scope of this ST, but the reference to the IC private key is made here to exemplify the protection of TOE assets).

Correct software execution is enforced by the use of logical constructs and techniques designed to detect perturbations in the program flow.

The integrated circuit of the TOE provides a number of hardware security features aimed at protecting the stored information against leakage or disclosure.

1.4 TOE life-cycle

The TOE life-cycle is described in terms of the four life-cycle phases. (With respect to [3], the TOE life-cycle is additionally subdivided into 7 steps.)

The roles in each phase of the TOE life-cycle are played by the following entities:

Role	Entity
IC Developer	CEITEC S.A.
Software Developer	CEITEC S.A.
IC Manufacturer	Third-party IC foundry providing services for CEITEC S.A.
Module Manufacturer	CEITEC S.A.
MRTD Manufacturer	The entity that assembles the passport, embedding the TOE in the booklet
Personalization Agent	The entity that personalizes the MRTD with the MRTD Holder data
MRTD Holder	Passport owner; traveler

Table 2 – Roles in the TOE life-cycle

1.4.1 Phase 1 "Development"

(Step 1) 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. This guidance documentation consists of manufacturing documentation intended for the IC Manufacturer and SW development guidance intended for the embedded SW Developer. Neither of the guidance is delivered to the MRTD Manufacturer or to the MRTD Holder.

(Step 2) 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 and the guidance documentation associated with these TOE components. This guidance documentation is intended for the ePassport manufacturer and Personalization Agent but is not delivered to the MRTD Holder. Guidance for the MRTD Holder is not part of the TOE and is to be authored and delivered by the MRTD Manufacturer and/or the Personalization Agent.

The manufacturing documentation of the IC is securely delivered to the IC Manufacturer.

Application Note 2: The development of the TOE is entirely conducted by CEITEC, therefore there is no institutional separation between the IC Developer and the Software Developer.

1.4.2 Phase 2 "Manufacturing"

(Step 3) In a first step the TOE integrated circuit is produced in accordance with the manufacturing documentation by the IC Manufacturer. The IC is securely delivered from the IC Manufacturer to the Module Manufacturer (i.e. CEITEC).

(Step 4) The Module Manufacturer writes the IC Software, the IC Private Key, the Personalization Agent Key, and the remaining Pre-personalization Data onto the chip. The IC is mounted on and connected to an electronic module base. The finished module is securely delivered from the Module Manufacturer to the MRTD Manufacturer along with the guidance documentation for the MRTD Manufacturer. The Personalization Agent Key is delivered to the Personalization Agent via a secure communication channel by the Module Manufacturer.

Application Note 3: The MRTD application is included in the IC Software, therefore there is no need to create the MRTD application as in [1].

Application Note 4: This ST defines the TOE delivery to take place at the end of Step 4. Therefore, the subsequent steps (5 through to 7) are not applicable to the TOE.

Application Note 5: The IC Private Key is used for the Chip Authentication procedure, which is not in the scope of this ST.

(Step 5) The MRTD Manufacturer combines the module with hardware for the contactless interface in the passport book.

The pre-personalized MRTD 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 Phase 3 "Personalization of the MRTD"

(Step 6) 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. 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 [2] 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.

1.4.4 Phase 4 "Operational Use"

(Step 7) The TOE is used as MRTD chip by the traveler and the Inspection Systems in the "Operational Use" phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

Application Note 6: It is not possible to add data to the MRTD application data groups during the Operational Use.

2 Conformance claims

2.1 Common Criteria conformance

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1, Revision 4, CCMB-2012-09-001 [4]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002 [5]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003 [6]

as follows:

- Part 2 extended,
- Part 3 conformant.

2.2 Protection Profile conformance

This ST claims strict conformance to

Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055, Version 1.10, 25th March 2009 [1].

2.3 Package conformance

This ST claims conformance to assurance package EAL4 augmented with ALC_DVS.2 defined in CC part 3.

3 Security problem definition

3.1 Introduction

Assets

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

Logical MRTD Data

The logical MRTD data consists of EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [2]. These data are user data of the TOE. EF.COM lists the existing elementary files (EF) with the user data. EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD Holder. The Chip Authentication Public Key (EF.DG14) is used by the Inspection System for the Chip Authentication. EF.SOD is used by the Inspection System for Passive Authentication of the logical MRTD. Due to interoperability reasons as the 'ICAO Doc 9303' [2] the TOE described in this ST specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD Holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16);
- Chip Authentication Public Key in EF.DG14;
- Document Security Object (SOD) in EF.SOD; and
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data

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

A sensitive asset is the following more general one.

Authenticity of the MRTD's chip

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

Subjects

This ST 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 Phase 2 Manufacturing.

Application Note 7: The Specific TOE only implements a subset of the MRTD life-cycle. This is discussed in Sect. 1.4. Therefore, for the purposes of this ST the role Manufacturer is further decomposed into three types of manufacturer which all play a different role in the

manufacturing process of the TOE. Where necessary, these manufacturer roles shall be referred to instead of generic Manufacturer in order to avoid ambiguity. In general, the role Manufacturer (as in e.g. FMT_SMR.1) refers to the Module Manufacturer. Module Manufacturer has access to the security management functions available to the Manufacturer (FMT_SMF.1), namely to writing the initialization and pre-personalization data to the TOE. These functions shall be disabled prior to the TOE being delivered to the MRTD Manufacturer.

1. IC Manufacturer is an external party operating the foundry where the wafers containing the IC are manufactured;
2. Module Manufacturer is the party completing the TOE, assembling the IC into the modules based and writing the IC Software and the Pre-personalization Data on it. This role is carried out by CEITEC; and
3. MRTD Manufacturer is the agent that manufactures the ePassport booklet, embedding the TOE and the antenna.

Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity 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 (iv) signing the Document Security Object defined in [2].

Terminal

A terminal is any technical system communicating with the TOE through the contactless interface.

Inspection System (IS)

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD Holder. The Basic Inspection System (BIS) (i) contains a terminal for the contactless communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The General Inspection System (GIS) is a Basic Inspection System which implements 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 of the Inspection System Certificates.

Application Note 8: This ST does not distinguish between the BIS, GIS and EIS because the Active Authentication and the Extended Access Control are outside the scope.

MRTD Holder

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

Traveler

Person presenting the MRTD to the Inspection System and claiming the identity of the MRTD Holder.

Attacker

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

Application Note 9: 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.

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_Manufac 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 or 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; and
- 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 Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys *Inspection Systems for global interoperability*

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD Holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [2]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

Application Note 10: According to [2] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

A.BAC-Keys Cryptographic quality of Basic Access Control *Keys*

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [2], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the Inspection System has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

Application Note 11: When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

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.

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

T.Chip_ID *Identification of MRTD's chip*

Adverse action	An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.
Threat agent	Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.
Asset	Anonymity of user.

T.Skimming *Skimming the logical MRTD*

Adverse action	An attacker imitates an Inspection System trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.

Threat agent	Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.
Asset	Confidentiality of logical MRTD data.

T.Eavesdropping Eavesdropping to the communication between TOE and Inspection System

Adverse action	An attacker is listening communication between the MRTD's chip and an Inspection System to gain the logical MRTD or parts of it. The Inspection System uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.
Threat agent	Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.
Asset	Confidentiality of logical MRTD 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 another 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 enhanced basic 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 the phase "Operational Use" 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 enhanced basic 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 enhanced basic 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 enhanced basic 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 enhanced basic 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 (OSPs)

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

P.Manufact Manufacturing of the MRTD's chip

The Initialization Data are written by the Module Manufacturer to identify the IC uniquely. The Module Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

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

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

P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2) and the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD Holder. These data groups are intended to be used only with agreement of the MRTD Holder by Inspection Systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [2].

Application Note 12: The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [2]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

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 [2] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16, the Document Security Object and the TSF data may be written only during and cannot be changed after its personalization.

Application Note 13: The TOE does not support the addition of LDS groups other than EF.DG1, EF.DG2 and EF.DG3 by the Personalization Agent. The TOE does not support addition of data to the existing LDS groups during the “Operational Use” phase.

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 that the Inspection System is able to detect any modification of the transmitted logical MRTD data.

OT.Data_Conf *Confidentiality of personal data*

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16.

Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

Application Note 14: The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the Inspection System by presenting the MRTD.

The MRTD’s chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys.

The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data’s entropy. Any attack based on decision of the ‘ICAO Doc 9303’ [2] that the

Inspection System derives Document Basic Access is ensured by OE.BAC Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this ST. Thus the read access is prevented even in case of a successful BAC Authentication.

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 of the Personalization Agent Key(s). In Phase 4 “Operational Use” the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

Application Note 15: The TOE security objective OT.Identification addresses security features of the TOE to support the life-cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and/or to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the MRTD”. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 “Operational Use” the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

The following TOE security objectives address the protection provided by the MRTD’s chip independent of 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

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

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

OT.Prot_Inf_Leak Protection against Information Leakage

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

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

Application Note 16: 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 enhanced-basic 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 17: 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 details about the TOE´s internals are known.

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); and
- 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 (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only, and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [2].

OE.BAC-Keys *Cryptographic quality of Basic Access Control Keys*

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO

Doc 9303' [2] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the Inspection System has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

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 [2].

OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the receiving State uses the Inspection System to verify the traveler as MRTD Holder. The Inspection Systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document 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 or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use Inspection Systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	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.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID													x			
T.Skimming			x										x			
T.Eavesdropping			x													
T.Forgery	x	x					x					x		x	x	
T.Abuse-Func					x						x					
T.Information_Leakage						x										
T.Phys-Tamper							x									
T.Malfunction								x								
P.Manufact				x												
P.Personalization	x			x							x					
P.Personal_Data		x	x													
A.MRTD_Manufact									x							
A.MRTD_Delivery										x						
A.Pers_Agent											x					
A.Insp_Sys														x		x
A.BAC-Keys													x			

Table 3 – security objectives coverage

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 Module 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 management of TSF to the Personalization Agent.

The OSP P.Personal_Data “Personal data protection policy” requires the TOE (i) to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives OT.Data_Int “Integrity of personal data”

describing the unconditional protection of the integrity of the stored data and during transmission.

The security objective OT.Data_Conf “Confidentiality of personal data” describes the protection of the confidentiality.

The threat T.Chip_ID “Identification of MRTD’s chip” addresses the trace of the MRTD movement by identifying remotely the MRTD’s chip through the contactless communication interface. This threat is countered as described by the security objective OT.Identification by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

The threat T.Skimming “Skimming digital MRZ data or the digital portrait” and T.Eavesdropping “Eavesdropping to the communication between TOE and Inspection System” address the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD’s chip and a terminal. This threat is countered by the security objective OT.Data_Conf “Confidentiality of personal data” through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

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.Abuse-Func “Abuse of Functionality” addresses attacks using the MRTD’s chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD Holder to disclose or to manipulate the logical MRTD.

This threat is countered by OT.Prot_Abuse-Func “Protection against Abuse of Functionality”.

Additionally this objective is supported by the security objective for the TOE environment: OE.Personalization “Personalization of logical MRTD” ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD Holder are enabled according to the intended use of the TOE.

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 T.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”. The security objectives for the TOE environment OE.Prot_Logical_MRTD “Protection of data from the logical MRTD” will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

The assumption A.BAC-Keys “Cryptographic quality of Basic Access Control Keys” is directly covered by the security objective for the TOE environment OE.BAC-Keys “Cryptographic quality of Basic Access Control Keys” ensuring the sufficient key quality to be provided by the issuing State or Organization.

5 Extended Components Definition

This ST uses components defined as extensions to CC part 2. Some of these components are defined in [7], other components are defined in this ST.

5.1 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE a sensitive family (FAU_SAS) of the Class FAU (Security Audit) is defined here. 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 as follows.

FAU_SAS Audit data storage

Family behavior

This family defines functional requirements for the storage of audit data.

Component leveling:

FAU_SAS Audit data storage	1

FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1
	There are no management activities foreseen.
Audit:	FAU_SAS.1
	There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. 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.

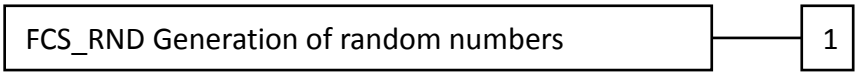
The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behavior

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:



FCS_RND Generation of random numbers 1

FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1
	There are no management activities foreseen.
Audit:	FCS_RND.1
	There are no actions defined to be auditable.

FCS_RND.1 *Quality metric for random numbers*

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3 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.

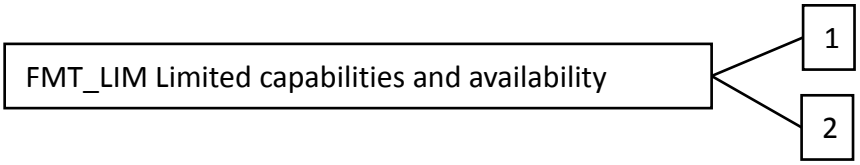
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behavior

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.

Component leveling:



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.
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 lifecycle.
Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 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

Hierarchical to:	No other components.
Dependencies:	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: *Limited capability and availability policy*].

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

FMT_LIM.2 Limited availability

Hierarchical to:	No other components.
Dependencies:	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: *Limited capability and availability policy*].

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

5.4 Definition of the Family FPT_EMSEC

The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE 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 [5].

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMSEC TOE emanation	1

FPT_EMSEC.1	TOE emanation has two constituents:
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.
Management:	FPT_EMSEC.1
	There are no management activities foreseen.
Audit:	FPT_EMSEC.1
	There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 Security requirements

6.1 Security functional requirements for the TOE

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

6.1.1 Class FAU Security Audit

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

FAU_SAS.1 *Audit storage*

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide **the Manufacturer**[1] with the capability to store **the IC Identification Data**[2] in the audit records.

Application Note 19: The Manufacturer here refers to the Module Manufacturer.

6.1.2 Class FCS Cryptographic Support

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

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Document Basic Access Key Derivation Algorithm**[3] and specified cryptographic key sizes **112 bit**[4] that meet the following: [2]**, normative appendix 5**[5]

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

[1] [assignment: authorized users]
[2] [assignment: list of audit information]
[3] [assignment: cryptographic key generation algorithm]
[4] [assignment: cryptographic key sizes]
[5] [assignment: list of standards]

FCS_CKM.4	*Cryptographic key destruction – 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.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: **overwriting the memory data**[6] that meets the following: **none**[7].

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

FCS_COP.1/SHA	*Cryptographic operation – Hash for Key Derivation*
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/SHA	The TSF shall perform **hashing**[8] in accordance with a specified cryptographic algorithm **SHA-1**[9] and cryptographic key sizes **none**[10] that meet the following: **FIPS 180-4**[11] [8].

FCS_COP.1/ENC Triple DES	*Cryptographic operation – 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/ENC	The TSF shall perform **secure messaging (BAC) – encryption and decryption**[12] in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode**[13] and cryptographic key sizes **112 bit**[14] that

[6] [assignment: cryptographic key destruction method]
[7] [assignment: list of standards]
[8] [assignment: list of cryptographic operations]
[9] [selection: SHA-1 or other approved algorithms]
[10] [assignment: cryptographic key sizes]
[11] [selection: FIPS 180-2 or other approved standards]
[12] [assignment: list of cryptographic operations]
[13] [assignment: cryptographic algorithm]
[14] [assignment: cryptographic key sizes]

	meet the following: **FIPS 46-3** [9] **and** [2]**, normative appendix 5, A5.3**[15].

FCS_COP.1/AUTH Cryptographic operation – Authentication

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/AUTH	The TSF shall perform **symmetric authentication – encryption and decryption**[16] in accordance with a specified cryptographic algorithm: **Triple-DES**[17] and cryptographic key sizes **112**[18] bit that meet the following: **FIPS 46-3**[19] [9].

FCS_COP.1/MAC Cryptographic operation – Retail 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 **secure messaging – message authentication code**[20] in accordance with a specified cryptographic algorithm **Retail MAC**[21] and cryptographic key sizes **112 bit**[22] that meet the following: **ISO/IEC 9797** [10] **(MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)**[23].

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

FCS_RND.1 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 **AIS-31 class PTG.2**[24] [11].

[15] [assignment: list of standards]
[16] [assignment: list of cryptographic operations]
[17] [selection: Triple-DES, AES]
[18] [selection: 112, 128, 168, 192, 256]
[19] [selection: FIPS 46-3, FIPS 197]
[20] [assignment: list of cryptographic operations]
[21] [assignment: cryptographic algorithm]
[22] [assignment: cryptographic key sizes]
[23] [assignment: list of standards]
[24] [assignment: a defined quality metric]

6.1.3 Class FIA Identification and Authentication

Application Note 20: The table below provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [2], normative appendix 5, and [12]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)

Table 4– Authentication Mechanisms

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2).

FIA_UID.1 *Timing of identification*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 "Manufacturing",
2. To read the random identifier in Phase 3 "Personalization of the MRTD",
3. To read the random identifier in Phase 4 "Operational Use"[28]

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

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

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 The TSF shall allow

[28] [assignment: list of TSF-mediated actions]

1. to read the Initialization Data in Phase 2 "Manufacturing",
2. To read the random identifier in Phase 3 "Personalization of the MRTD",
3. To read the random identifier in Phase 4 "Operational Use" [29]

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

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

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria 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

1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on **Triple-DES**[30].

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

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on **Triple-DES** to support user authentication [31]

to support user authentication**.**

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

1. the TOE accepts the authentication attempt as Personalization Agent by ~~one of~~[33] the following mechanism~~(s)~~[34]: **(1) symmetric authentication with the Transport Key**,
2. The TOE accepts the authentication attempt as Basic Inspection

[29] [assignment: list of TSF-mediated actions]
[30] [selection: Triple-DES, AES or other approved algorithms]
[31] [selection: Triple-DES, AES]
[33] [Refinement: removed ´one of´ as there is only a single mechanism for Personalization Agent authentication consisting of three stages]
[34] [Refinement: only a single mechanism – but consisting of three stages]

System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.[36]

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism**[37]

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

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when **a defined number (defined in Table 5, column "Maximum Consecutive Attempts") of consecutive**[38] unsuccessful authentication attempts occur related to **each authentication event listed in Table 5, column "Authentication Event"**[39].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **surpassed**[40], the TSF shall **execute the action defined in Table 5, column "Action"**[41].

Authentication Event	Maximum Consecutive Attempts	Action
Personalization	3	Enter violated state
Inspection BAC	1	Stop authenticating the IS for at least 5 s
MAC verification	1	Close Secure Messaging session

Table 5 – FIA_AFL.1 refinement

[36] [assignment: rules describing how the multiple authentication mechanisms provide authentication]
[37] [assignment: list of conditions under which re-authentication is required]
[38] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[39] [assignment: list of authentication events]
[40] [assignment: met or surpassed]
[41] [assignment: list of actions]

Application Note 21: The number of unsuccessful authentication attempts is stored in a non-volatile memory in the TOE, so that it is unaffected by powering down the TOE, and the count is reset to zero only after a successful authentication.

6.1.4 Class FDP User Data Protection

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2).

FDP_ACC.1 Subset access control – Basic 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 Basic Access Control SFP** [42] on **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD**[43].

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

FDP_ACF.1 Basic Security attribute based access control – Basic 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 Basic Access Control SFP**[44] to objects based on the following:

1. Subjects:
- **a. Personalization Agent,**
- **b. Basic Inspection System,**
- **c. Terminal,**

2. Objects:
- **a. data EF.DG1 to EF.DG16 of the logical MRTD,**
- **b. data in EF.COM,**
- **c. data in EF.SOD,**

3. Security attributes
- **a. authentication status of terminals.**[45]

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

[42] [assignment: access control SFP]
[43] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[44] [assignment: access control SFP]
[45] [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]

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,

Application Note 22: The Personalization Agent may only write the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 after being successfully authenticated.

2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.[46]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**[47]

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

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.[48]

Application Note 23: The Inspection System needs special authentication and authorization for read access to DG3 and DG4 not defined in this ST (cf. [13] for details).

Inter-TSF-Transfer

Application Note 24: 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 authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

FDP_UCT.1 *Basic data exchange confidentiality – MRTD*

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]

[46] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[47] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
[48] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FDP_UCT.1.1	The TSF shall enforce the **Basic Access Control SFP** [49] to be able to **transmit and receive** [50] user data in a manner protected from unauthorized disclosure.

The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2).

FDP_UIT.1	*Data exchange integrity – MRTD*
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 **Basic Access Control SFP** [51] to be able to **transmit and receive** [52] user data in a manner protected from **modification, deletion, insertion and replay** [53] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** [54] has occurred.

6.1.5 Class FMT Security Management

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 management functions: **1. Initialization,** **2. Pre-personalization,** **3. Personalization.** [55]

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

FMT_SMR.1	*Security roles*
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.

[49] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[50] [selection: transmit, receive]
[51] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[52] [selection: transmit, receive]
[53] [selection: modification, deletion, insertion, replay]
[54] [selection: modification, deletion, insertion, replay]
[55] [assignment: list of management functions to be provided by the TSF]

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Basic Inspection System. [56]

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

Application Note 25: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: 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:

Deploying Test Features after TOE Delivery does not allow
1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. Software to be reconstructed and
4. Substantial information about construction of TSF to be gathered which may enable other attacks [57]

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: 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:

Deploying Test Features after TOE Delivery does not allow
1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. Software to be reconstructed and
4. Substantial information about construction of TSF to be gathered which may enable other attacks. [58]

[56] [assignment: the authorized identified roles]
[57] [assignment: Limited capability and availability policy]
[58] [assignment: Limited capability and availability policy]

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

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

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 **write** [59] the **Initialization Data and Pre-personalization Data** [60] to **the Manufacturer**. [61]

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 **disable read access for users to** [62] the **Initialization Data** [63] to **the Personalization Agent**. [64]

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 **write** [65] the **Document Basic Access Keys** [66] to the **Personalization Agent**. [67]

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

[59] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[60] [assignment: list of TSF data]
[61] [assignment: the authorized identified roles]
[62] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[63] [assignment: list of TSF data]
[64] [assignment: the authorized identified roles]
[65] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[66] [assignment: list of TSF data]
[67] [assignment: the authorized identified roles]

FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to **read** [68] the **Document Basic Access Keys and Personalization Agent Keys** [69] to **none**. [70]

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.

The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below (Common Criteria 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 fields and power consumption information**[71] in excess of **non-useful information**[72] enabling access to **Personalization Agent Key(s)** [73] and **data stored in EF.COM, EF.SOD, EF.DG1 to EF.DG16**[74].
FPT_EMSEC.1.2	The TSF shall ensure any **unauthorized users** [75] are unable to use the following interface **smart card circuit contacts** [76] to gain access to **Personalization Agent Key(s)** [77] and **data stored in EF.COM, EF.SOD, EF.DG1 to EF.DG16**[78].

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

[68] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[69] [assignment: list of TSF data]
[70] [assignment: the authorized identified roles]
[71] [assignment: types of emissions]
[72] [assignment: specified limits]
[73] [assignment: list of types of TSF data]
[74] [assignment: list of types of user data]
[75] [assignment: type of users]
[76] [assignment: type of connection]
[77] [assignment: list of types of TSF data]
[78] [assignment: list of types of user data]

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: **1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,** **2. Failure detected by TSF according to FPT_TST.1.** [79]

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, periodically during normal operation, at the request of random numbers, after cryptographic operations**[80] to demonstrate the correct operation of **the TSF**. [81]
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of **TSF data**. [82]
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of **stored TSF executable code**. [83]

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

FPT_PHP.3 *Resistance to physical attack*

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist **physical manipulation and physical probing** [84] to **the TSF** [85] by responding automatically such that the SFRs are always enforced.

[79] [assignment: list of types of failures in the TSF]
[80] [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur]]
[81] [selection: [assignment: parts of TSF], the TSF]
[82] [selection: [assignment: parts of TSF data], TSF data]
[83] [selection: [assignment: parts of TSF], TSF].
[84] [assignment: physical tampering scenarios]
[85] [assignment: list of TSF devices/elements]

6.2 Security Assurance Requirements for the TOE

The 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 component:

ALC_DVS.2.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					
FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_RND.1	x	x	x					
FIA_UID.1			x	x				
FIA_AFL.1			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4	x	x	x					
FIA_UAU.5	x	x	x					
FIA_UAU.6	x	x	x					
FDP_ACC.1	x	x	x					
FDP_ACF.1	x	x	x					
FDP_UCT.1	x	x	x					
FDP_UIT.1	x	x	x					
FMT_SMF.1	x	x	x					
FMT_SMR.1	x	x	x					
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA				x				
FMT_MTD.1/INI_DIS				x				
FMT_MTD.1/KEY_WRITE	x	x	x					

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FMT_MTD.1/KEY_READ	x	x	x					
FPT_EMSEC.1	x				x			
FPT_TST.1					x		X	
FPT_FLS.1	x				x		X	
FPT_PHP.3	x				x	x		

Table 6- Coverage of Security Objective for the TOE by SFR

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 FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent (FIA_UAU.5) is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5.

The Personalization Agent (FIA_UAU.5.2 stage 1) can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [13] by using the symmetric authentication mechanism (FCS_COP.1/ AUTH).

In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially 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 of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). 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 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 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

The security objective OT.Data_Int “Integrity of personal data” requires the TOE to ensure that the Inspection System is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

The security objective OT.Data_Conf “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys). The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/ MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

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.

Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 “Operational Use”. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (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 SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD’s chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application note 30). In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

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 features 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/or 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/or – 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, and (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

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.

The table below shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction,	Fulfilled by FCS_COP.1/ENC and 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	Fulfilled by FCS_CKM.1,

SFR	Dependencies	Support of the Dependencies
	attributes, or FCS_CKM.1 Cryptographic key generation]	
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/ENC	[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/AUTH	[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 2 for non-satisfied dependencies justification 2 for non-satisfied dependencies
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_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1

SFR	Dependencies	Support of the Dependencies
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a
FIA_UAU.6	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 3 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 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_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
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/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.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
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 7 – Dependencies between the SFR for the TOE

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

No. 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither key generation (FCS_CKM.1) nor key import (FDP_ITC.1/2) is necessary.

No. 2: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus it is not necessary to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

No. 3: 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.

No. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS. There is no need for 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.

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 component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements.

Dependencies ALC_DVS.2:

No dependencies.

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 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-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 sections 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

This section provides a description of the TOE's security functions and mechanisms and the corresponding SFRs that are met by each function or mechanism.

7.1 SF.AC_Pers: Access Control for Personalization

During the Phase 3, "Personalization" the Personalization Agent is identified and authenticated cryptographically using random numbers meeting the AIS-31 PTG.2 quality requirements (FCS_RND.1) for challenge-response authentication as well as a symmetric key mechanism 3DES (FCS_COP.1/AUTH) and message authentication codes (FCS_COP.1/MAC) for the authentication.

The Personalization Agent receives the TOE in a Locked state from the MRTD Manufacturer (who in turn receives the TOE in a Locked state from the Module Manufacturer). The Personalization Agent must complete an authentication procedure with the TOE in order to unlock the TOE and perform the personalization (FIA_UAU.5).

The authentication procedure involves both parties generating a symmetric session key (FCS_CKM.1) with a SHA-1 hash function (FCS_COP.1/SHA) and using that session key for encrypting and authenticating subsequent exchanges (FCS_COP.1/ENC). Upon completion of the Personalization of the TOE, the session key used for secure messaging is destroyed (FCS_CKM.4). The secure messaging channel ensures that the data communicated between the TOE and the Personalization Agent is protected from unauthorized disclosure (FDP_UCT.1).

The mechanism ensures that reuse of authentication data from previous sessions is prevented (FIA_UAU.4) as each session key is unique (based on a unique challenge and unique RNDs). Only commands communicated to the TOE via a secure channel (FCS_COP.1/ENC) and with a correct message authentication code (FCS_COP.1/MAC) are executed by the TOE (FIA_UAU.6). The security function is implement in a rigorous manner so that any TSF failure shall not expose the TOE into an insecure state (FPT_FLS.1) and that attempts of physical manipulation of the TOE (FPT_PHP.3) or reading of electromagnetic emanations during the personalization (FPT_EMSEC.1) shall not provide the attacker with an advantage which could be practically turned into a successful attack against the TOE.

The TOE maintains a role Personalization Agent and the authentication mechanism allows the TOE to establish the identity and determine legitimacy of the Personalization Agent (FMT_SMR.1) and make available to the Personalization Agent the functions required for the Personalization of the TOE (FMT_SMF.1).

7.2 SF.Data_Int: Integrity of Personal Data

Prior to being shipped to the MRTD Manufacturer and, subsequently, to the Personalization Agent, the TOE is only manipulated by the Manufacturer (specifically, the Module Manufacturer). The Module Manufacturer initializes and pre-personalizes the TOE in secure premises. Upon completing the initialization and pre-personalization of the TOE, the TOE is set to a Locked mode and all subsequent accesses require a successful authentication procedure to establish the user of the TOE as a Personalization Agent or Basic Inspection System (FMT_SMR.1).

Initialization of the TOE concerns with the writing of the TOE software on the module and pre-personalization concerns with the downloading of the TSF Data on the TOE.

Personalization is only allowed upon successful authentication of the Personalization Agent (FIA_UAU.5). There are no other TOE management functions (FMT_SMF.1).

The TOE only allows an authorized Personalization Agent (FMT_SMR.1) to write the data elements containing the personal data and Document Basic Access Keys as part of TOE Personalization through a well-defined management function (FMT_SMF.1, FMT_MTD.1/KEY_WRITE). No party is allowed to read the BAC keys (FMT_MTD.1/KEY_READ). The Personalization Agent is authenticated and a secure messaging channel established between the TOE and the Personalization Agent (FCS_CKM.1, FCS_RND.1, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_CKM.4, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1). Writing to these data groups is not allowed after the Personalization phase as shall be discussed in the following.

During the “Operational Use” phase, a Basic Inspection System is only allowed to read data from the TOE after being successfully authenticated by a BAC mechanism using the MRZ data and deriving the BAC keys from that data (FCS_CKM.1, FCS_RND.1, FCS_COP.1/MAC, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_CKM.4, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1).

The Basic Inspection System must generate the 3DES key from the optically readable data on the ePassport data page (the travel document serial number and the personal data of the traveler). The TOE generates the same key from the logical data stored on the TOE. The two parties (Basic Inspection System and the TOE) now use this key to complete the BAC authentication.

This allows the TOE to establish the authenticity and assign a role of the Basic Inspection System to the user (FMT_SMR.1). Upon successful authentication and role establishment, the TOE shall enforce a role based access control rules to ensure that only legitimate accesses are allowed to the Basic Inspection System (FDP_ACC.1, FDP_ACF.1) and that only reading of data is allowed.

The secure messaging channel between the the TOE and the Basic Inspection System ensures that the data communicated between the TOE and the Basic Inspection System is protected from unauthorized disclosure (FDP_UCT.1) and modification (FDP_UIT.1).

7.3 SF.Data_Conf: Confidentiality of personal Data

Data confidentiality is enforced by the TOE:

1. By ensuring cryptographic quality of the BAC secrets and the subsequent secure channel used for communicating any data between the TOE and the Basic Inspection System as described under SF.Data_Int (Sect.7.2) covering SFR´s FCS_RND.1, FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/AUTH FDP_UIT.1 and FDP_UCT.1;
2. by restricting access to functions available before user identification and authentication at different life-cycle stages (FIA_UID.1, FIA_UAU.1);

3. by ensuring that rigorous authentication functions are implemented as described under SF.AC_Pers (Sect.7.1) and SF.Data_Int (Sect.7.2) covering SFRs FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6;
4. by ensuring that only well-defined accesses are allowed based on the role of the user (FDP_ACC.1, FDP_ACF.1) which prevents violations of confidentiality and integrity of data stored on the TOE; and
5. by only allowing TOE management via well-defined management functions (FMT_SMF.1) to the systems acting in specific authorized roles (FMT_SMR.1) so that unauthorized reading and writing of BAC keys is prevented (FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ).

7.4 SF.Auth: Identification and Authentication

The TOE allows the Manufacturer to write the IC Identification and Pre-personalization data, including the personalization Agent Key during Phase 2 “Manufacturing” (FAU_SAS.1, FMT_MTD.1/INI_ENA). The IC Identification can be read by the Personalization Agent during Phase 3 “Personalization of the MRTD”. Upon completion of the personalization of the TOE, the Personalization Agent removes any initialization data thus disables any read access to the initialization data and the TOE ensures that only the personalization agent is allowed to remove the initialization data (FMT_MTD.1/INI_DIS).

The TOE implements measures to handle failed authentication attempts as expressed in Table 3 (FIA_AFL.1). The TOE implements authentication and access control mechanism to make sure that the TOE and Personalization Agent and the TOE and the Basic Inspection System are mutually authenticated prior to granting any access to the TSF data during the Personalization or Operational Use of the TOE. Only the read accesses required for authentication and establishment of the secure channel are allowed prior to identification and authentication of the Personalization Agent or the Basic Inspection System (FIA_UID.1, FIA_UAU.1). The TOE also allows the Manufacturer (namely, the Module Manufacturer) to read the initialization data written on the TOE during Module Manufacturing to ensure that the TOE can be fully tested prior to shipment to the MRTD Manufacturer.

7.5 SM.Prot_Abuse_Func: Protection against Abuse of Functionality

During the Phase 2, “Manufacturing” the connection to the test interface of the chip is disabled before the chip is mounted onto the module. This prevents the direct access to the chip circuit and functions (FMT_LIM.1 and FMT_LIM.2).

7.6 SM.Prot_Inf_Leak: Protection against Information Leakage

The TOE provides protection against disclosure of confidential TSF data stored and/or processed in the MRTD’s chip by observation of its electromagnetic emanations (FPT_EMSEC.1). Data disclosure by direct physical manipulation of the TOE or by forcing malfunctions is prevented by the features listed in Sect. 7.7 and Sect. 7.8 (FPT_FLS.1, FPT_TST.1, FPT_PHP.3).

7.7 SM.Prot_Phys_Tamper: Protection against Physical Tampering

The TOE provides protection of the confidentiality and integrity of the User Data, the TSF Data, and the IC Embedded Software against direct reading with physical probing or forced disclosure due to perturbation injections (FPT_PHP.3).

The IC of the TOE additionally provides a rich set of hardware countermeasures against physical tampering which prevent construction of intelligible data from any information obtained by physically tampering with the TOE.

7.8 SM.Prot_Malfunction: Protection against Malfunctions

The TOE is protected against malfunctions due to abnormal operation conditions by a set of sensors (FPT_FLS.1) and self-tests (FPT_TST.1).

8 List of abbreviations

AES	Advanced Encryption System
APDU	Application Protocol Data Unit
BAC	Basic Access Control
BIS	Basic Inspection System
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher-Block Chaining
CC	Common Criteria
CDS	DS Public Key Certificate
DES	Data Encryption System
DG	Data Group
DP&N	Desenvolvimento de Produtos e Negócios
DPA	Differential Power Analysis
EAC	Extended Access Control
EAL	Assurance Level
EF	Elementary File
EIS	Extended Inspection System
GIS	General Inspection System
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ICCSN	Integrated Circuit Card Serial Number
IS	Inspection System
LDS	Logical Data Structure
LDS	Logical Data Security
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
MRZ	Machine-Readable Zone
n.a.	Not Applicable
OCR	Optical Character Recognition
OSP	Organization Security Policy
PA	Personalization Agent
PP	Protection Profile
PS	Personalization System

RFID	Radio Frequency Identification
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOD	Document Security Object
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

9 References

[1] Bundesamt für Sicherheit in der Informationstechnik, “Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application”, Basic Access Control,” 2009.

[2] International Civil Aviation Organization, “ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports,” 2006.

[3] Bundesamt für Sicherheit in der Informationstechnik, “Security IC Platform Protection Profile,” 2007.

[4] “Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4,” 2012.

[5] “Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4,” 2012.

[6] “Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 4,” 2012.

[7] Bundesamt für Sicherheit in der Informationstechnik, “PP conformant to Smartcard IC Platform Protection Profile, Version 1.0,” 2001.

[8] U.S. Department Of Commerce/National Institute of Standards and Technology, “Secure Hash Standard (SHS),” 2012.

[9] U.S. Department Of Commerce/National Institute of Standards and Technology, “Data Encryption Standard (DES),” 1999.

[10] ISO, “Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher,” 2011.

[11] Bundesamt für Sicherheit in der Informationstechnik, “Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren,” 2013.

[12] Bundesamt für Sicherheit in der Informationstechnik, “Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)”.

[13] Bundesamt für Sicherheit in der Informationstechnik, “Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0056, Version 1.10,” 25th March, 2009.

[14] U.S. Department Of Commerce/National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” 2001.

[15] ISO, “Identification cards - Integrated circuit cards - Part 2: Cards with contacts - Dimensions and location of the contacts,” 2007.

[16] Bundesamt für Sicherheit in der Informationstechnik, "Technical Guideline TR-03110-1," Bonn, 2012.

[17] G. Ilha, *CTC21001 APDU Specification version 1 (*preliminary*),* 02/apr/2015.

[18] CEITEC SA, *CEITECSA 5.410.028 - ST ePassport Module BAC.*

[19] CEITEC SA, *CEITECSA 5.410.029 - ST ePassport Module EAC.*

[20] CEITEC SA, *Copernicus Architecture Specification Document version 1.0 (*preliminary*),* 2015.

[21] CEITEC SA, *CEITECSA 5.420.014 - Micromodule CTC21001 MM - (*preliminary*).*

[22] International Civil Aviation Organization, Doc 9303 - Machine Readable Travel Documents - Part 1, 6 ed., vol. 2, ICAO, 2006.