Security Target Lite for CEITEC ePassport Module CTC21001 with EAC

Version 2.0 – 12/Dec/2016

Document History

1.0	First version
2.0	Clarifications to section 7.1

Table of contents

1 Introduction

1.1 ST Lite reference and TOE reference

ST Lite identification:	CEITECSA 5.410.052, version 2.0
Author:	Product and Business Development Department (DP&N), CEITEC S.A.
Date:	12 December 2016
TOE identification:	CEITEC ePassport Module, CTC21001, version 1.0
Applicant:	CEITEC S.A., Porto Alegre, Brazil
Compliant to:	BSI-CC-PP-0056, “Machine Readable Travel Document with ‘ICAO Application’, Extended Access Control” [1]
Assurance level:	EAL4 augmented by ALC_DVS.2 and AVA_VAN.5
Keywords:	ePassport, MRTD, machine readable travel document, EAC, extended 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. The Inspection System is required to perform the Extended Access Control (EAC) procedure in order to be allowed to read the optional passport holder biometric 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. The Inspection System is required to perform the Basic Access Control (BAC) authentication procedure in order to be allowed to read the passport holder data and the Extended Access Control (EAC) authentication procedure in order to be allowed to read the optional passport holder biometric data. EAC and all subsequent communication takes place over a secure channel established by BAC.

The traveler presents a MRTD to the Inspection System to prove his or her identity. 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 Extended Access Control Mechanism. This ST addresses the Chip Authentication described in [3] as an alternative to the Active Authentication stated in [2].

The TOE implements Chip Authentication defined in [3]. Chip Authentication prevents data traces described in [2], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The TOE implements Extended Access Control as defined in [3]. Extended Access Control consists of two parts (i) the Chip Authentication Protocol and (ii) the Terminal Authentication Protocol. The Chip Authentication Protocol (i) authenticates the MRTD's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication can only be performed if Chip Authentication has been successfully executed. The Terminal Authentication Protocol consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification of the authentication public keys of Document Verifiers who create Inspection System Certificates.

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/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 Extended Access Control according to [3].

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; and
- 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.

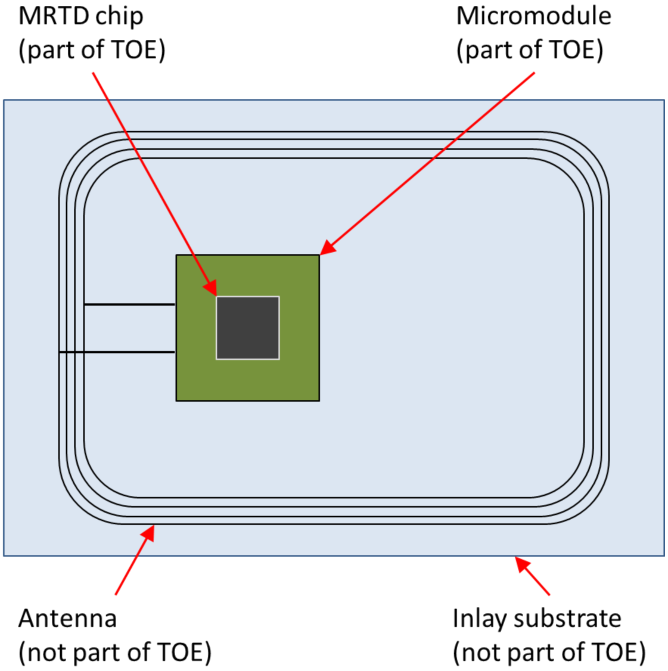


Figure 1 – Parts of the TOE and additional physical parts

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 before the TOE will grant the access rights for the Personalization Agent to create and write the user data files.

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 (i.e. EAC).

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 and EAC procedures are 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 and EAC 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. 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 [4], 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.

(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. Activity (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (a) the digital MRZ data (EF.DG1), (b) the digitized portrait (EF.DG2), and (c) 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 5: It is not possible to add data to the MRTD application data groups during the “Operational Use” phase.

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 [5]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002 [6]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003 [7]

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”, Extended Access Control, BSI-CC-PP-0056, Version 1.10, 25th March 2009 [1].

2.3 Package conformance

This ST claims conformance to assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 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 required by 'ICAO Doc 9303' [2] the TOE described in this ST implements a BAC mechanism 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.

Access to the following sensitive User Data is granted by the TOE only for Extended Inspection Systems that successfully perform the EAC mechanism:

- 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 6: 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 and the encoded finger image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, and (iv) signing the Document Security Object defined in [2].

Country Verifying Certification Authority

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

Document Verifier

The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.

Terminal

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

Inspection System (IS)

A technical system used by the border control officer of the receiving State (i) 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.

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 manipulate the logical MRTD without authorization t, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or (iii) to forge a genuine MRTD.

Application Note 7: Note that an attacker trying to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD) is not considered by this ST since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys that is covered by [1]. The same holds for the confidentiality of the user data EF.DG1, EF.DG2, EF.DG5 to EF.DG16 as well as EF.SOD and EF.COM.

Application Note 8: 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 CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [2]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

A.Signature_PKI PKI for Passive Authentication

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

Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

A.Auth_PKI PKI for Inspection Systems

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

3.3 Threats

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

Application Note 9: The threats T.Chip_ID and T.Skimming (cf. [1]) are averted by the mechanisms described in the BAC PP [1] (cf. P.BAC-PP) which cannot withstand an attack with high attack potential thus these are not addressed here. T.Chip_ID addresses the threat of tracing the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. T.Skimming addresses the threat of imitating the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Both attacks are conducted by an attacker who cannot read the MRZ or who does not know the physical MRTD in advance.

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

T.Read_Sensitive_Data Read the sensitive biometric reference data

Adverse action An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [1]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well. MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

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

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

T.Forgery *Forgery of data on MRTD’s chip*

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

Asset Authenticity of logical MRTD data.

T.Counterfeit *MRTD’s chip*

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

Threat agent Having high attack potential, being in possession of one or more legitimate MRTDs.

Asset Authenticity of logical MRTD data.

The TOE shall avert the threat as specified below.

T.Abuse-Func Abuse of Functionality

Adverse action An attacker may use functions of the TOE which shall not be used in 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 high attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Information_Leakage Information Leakage from MRTD's chip

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

Threat agent Having high attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality logical MRTD and TSF data.

T.Phys_Tamper Physical Tampering

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

i. to disclose TSF Data; or

ii. to disclose/reconstruct the MRTD's chip Embedded Software.

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

i. modify security features or functions of the MRTD's chip;

ii. modify security functions of the MRTD's chip Embedded Software;

iii. modify User Data; or

iv. modify TSF data.

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

Threat agent Having high attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Malfunction Malfunction due to Environmental Stress

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

i. deactivate or modify security features or functions of the TOE; or

ii. circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

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

Threat agent Having high attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

3.4 Organizational security policies (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.BAC-PP Fulfillment of the Basic Access Control Protection Profile.

The issuing State or Organization ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the 'ICAO Doc 9303' [2] defines[1] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [1]in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

Application Note 10: The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [2] is addressed by the [1](cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG3 and EF.DG4 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [2]). The TOE shall protect the sensitive biometric reference data in EF.DG3 and EF.DG4 against attacks with high attack potential. Due to the different resistance the protection of EF.DG3 and EF.DG4 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 are addressed separated protection profiles, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates (cf. also to application note 1).

P.Sensitive_Data Privacy of sensitive biometric reference data

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

P.Manufact Manufacturing of the MRTD's chip

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

Application Note 11: The following deviations from P.Manufact shall be followed in this ST to take into account the specific TOE life-cycle as described in Sect. 1.4:

[1] Word ´defines´ added to correct an obvious typing/grammatical error in BSI-CC-PP-0056.

1. Instead of the IC Manufacturer, the Initialization Data is written by the Module manufacturer upon receiving the wafers from the IC Manufacturer and producing the modules on which the TOE is initialized and pre-personalized; and
2. The Pre-personalization Data is written on the TOE by the Module Manufacturer prior to the delivery of the TOE to the MRTD Manufacturer as modules.

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.

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. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Application Note 12: 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 the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

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

OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification and Pre-personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. The storage of the Pre-personalization Data includes writing of the Personalization Agent Key(s).

OT.Chip_Auth_Proof *Proof of MRTD’s chip authenticity*

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD’s chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [3]. The authenticity proof provided by MRTD’s chip shall be protected against attacks with high attack potential.

Application Note 13: The OT.Chip_Auth_Proof implies the MRTD’s chip to have (i) a unique identity as given by the MRTD’s Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD’s chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD’s chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [2] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

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 14: 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 IC 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 15: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that 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.Auth_Key_MRTD MRTD Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

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

OE.BAC_PP Fulfillment of the Basic Access Control Protection Profile.

It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [1]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

Receiving State or Organization

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

OE.Exam_MRTD Examination of the MRTD passport book

The Inspection System of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [2]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the receiving State uses the Inspection System to verify the traveler as MRTD Holder. The Inspection Systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing CA Public Key and the Document Signer Public Key maintaining their authenticity and availability in all Inspection Systems.

OE.Prot_Logical_MRTD Protection of data from the logical MRTD

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

Application Note 16: The figure 2.1 in [3] supposes that the GIS and the EIS follow the order (i) running the Basic Access Control Protocol, (ii) reading and verifying only those parts of the logical MRTD that are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key), (iii) running the Chip Authentication Protocol, and (iv) reading and verifying the less-sensitive data of the logical MRTD after Chip Authentication. The supposed sequence has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. The inspection system will prevent additionally eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. Note that reading the less sensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this PP. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

OE.Ext_Insp_Systems Authorization of Extended Inspection Systems

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

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

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

Table 3 - security objectives coverage

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

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

The OSP P.Personalization “Personalization of the MRTD by issuing State or Organization only” addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment OE.Personalization “Personalization of logical MRTD”, and (ii) the access control for the user data and TSF data as described by the security objective OT.AC_Pers “Access Control for Personalization of logical MRTD”. Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to OT.Identification “Identification and Authentication of the TOE”. The security objective OT.AC_Pers limits the management of TSF data and management of TSF to the Personalization Agent.

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

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

The threat T.Counterfeit “MRTD’s chip” addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by OT.Chip_Auth_Proof “Proof of MRTD’s chip authentication” using a authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by OE.Auth_Key_MRTD “MRTD Authentication Key”. According to OE.Exam_MRTD “Examination of the MRTD passport book” the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD’s chip.

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

The threats T.Information_Leakage “Information Leakage from MRTD’s chip”, T.Phys-Tamper “Physical Tampering” and T.Malfunction “Malfunction due to Environmental Stress” are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives OT.Prot_Inf_Leak “Protection against Information Leakage”, OT.Prot_Phys-Tamper “Protection against Physical Tampering” and 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” which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD’s chip. The security objectives for the TOE environment OE.Prot_Logical_MRTD “Protection of data from the logical MRTD” require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

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

The assumption A.Auth_PKI “PKI for Inspection Systems” is covered by the security objective for the TOE environment OE.Authoriz_Sens_Data “Authorization for use of sensitive biometric reference data” requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organizations only. The

Document Verifier of the receiving State is required by OE.Ext_Insp_Systems “Authorization of Extended Inspection Systems” to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organization has to establish the necessary public key infrastructure.

5 Extended Components Definition

This ST uses components defined as extensions to CC part 2. Some of these components are defined in [8], 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.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 FIA_API

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

Application Note 17: The other families of the Class FIA describe only the authentication verification of users’ identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter “Explicitly stated IT security requirements

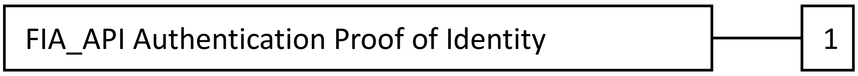
(APE_SRE)") from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behavior

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component leveling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

5.4 Definition of the Family FMT_LIM

The family FMT_LIM describes the functional requirements for the Test Features of the TOE.

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

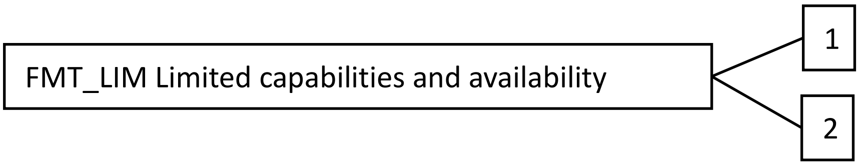
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

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.

5.5 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 [6].

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**[2] with the capability to store the **IC Identification Data**[3] in the audit records.

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

6.1.2 Class Cryptographic Support (FCS)

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*

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 **based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3**[4], and specified cryptographic key sizes **1024 bit**[5] that meet the following: [3]**, Annex A.1**[6].

Application Note 20: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [3], sec. 3.1 and Annex A.1. This protocol is based on the

[2] [assignment: authorized users]
[3] [assignment: list of audit information]
[4] [selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946]
[5] [assignment: cryptographic key sizes]
[6] [assignment: list of standards]

Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [9]). The shared secret value is used to derive the Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [2], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC.

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

FCS_CKM.4 Cryptographic key destruction - MRTD

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**[7] that meets the following: **none**[8].

Application Note 21: The TOE shall destroy the BAC Session Keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip Authentication Protocol. The TOE shall destroy the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

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 by MRTD

Hierarchical to: No other components.

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

FCS_COP.1.1/SHA The TSF shall perform hashing in accordance with a specified cryptographic algorithm **SHA-1**[9] and cryptographic key sizes **none**[10] that meet the following: **FIPS 180-4**[11] [10].

[7] [assignment: cryptographic key destruction method]
[8] [assignment: list of standards]
[9] [selection: SHA-1 or other approved algorithms]

Application Note 22: For the purposes of this ST, SHA-1 concerns with the Chip Authentication Protocol.

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

Hierarchical to: No other components.

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

FCS_COP.1.1/SYM The TSF shall perform **secure messaging – 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 meet the following: **TR-03110** [3][15].

FCS_COP.1/MAC Cryptographic operation –MAC

Hierarchical to: No other components.

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

FCS_COP.1.1/MAC The TSF shall perform **secure messaging – message authentication code**[16] in accordance with a specified cryptographic algorithm **Retail MAC**[17] and cryptographic key sizes **112 bit**[18] that meet the following: **TR-03110** [3][19].

Application Note 23: The TOE implements cryptographic primitives for secure messaging with encryption (3DES) and message authentication (Retail MAC) of transmitted data. The key is agreed upon by Chip Authentication Protocol.

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

Hierarchical to: No other components.

[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]
[15] [assignment: list of standards]
[16] [assignment: list of cryptographic operations]
[17] [assignment: cryptographic algorithm]
[18] [assignment: cryptographic key sizes]
[19] [assignment: list of standards]

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

FCS_COP.1.1/SIG_VER The TSF shall perform **digital signature verification**[20] in accordance with a specified cryptographic algorithm **RSA**[21] and cryptographic key sizes **1024-bit modulus**[22] that meet the following: [11][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] [12].

6.1.3 Class FIA Identification and Authentication

Application Note 24: The table below provides an overview on the authentication mechanisms used.

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4
Chip Authentication Protocol	FIA_API.1, FIA_UAU.5, FIA_UAU.6
Terminal Authentication Protocol	FIA_ UAU.5

Table 4 – Authentication Mechanisms

Note the Chip Authentication Protocol as defined in this ST includes

- the BAC authentication protocol as defined in 'ICAO Doc 9303' [2] in order to gain access to the Chip Authentication Public Key in EF.DG14;

[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]

- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol; and
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

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

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 establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
3. to carry out the Chip Authentication Protocol[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

1. to establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
3. to identify themselves by selection of the authentication key,

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

4. to carry out the Chip Authentication Protocol[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. Terminal Authentication Protocol,
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. Terminal Authentication Protocol,
2. Secure messaging in MAC-ENC mode,
3. Symmetric Authentication Mechanism based on Triple-DES[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 the Terminal Authentication Protocol with Personalization Agent Keys.
2. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.

[29] [assignment: list of TSF-mediated actions]
[30] [assignment: identified authentication mechanism(s)]
[31] [assignment: list of multiple authentication mechanisms]

3. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism[32].

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 after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS**[33].

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2).

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a **Chip Authentication Protocol according to** [3][34] to prove the identity of the **TOE**[35].

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

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the **Access Control SFP** [36] 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**[37].

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

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

[34] [assignment: authentication mechanism]

[35] [assignment: authorized user or role]

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

FDP_ACF.1 *Security attribute based access control*

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 **Access Control SFP**[38] to objects based on the following:

1. Subjects:
a. Personalization Agent,
b. Extended Inspection System,
c. Terminal,

2. Objects:
a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
b. data EF.DG3 and EF.DG4 of the logical MRTD,
c. data in EF.COM,
d. data in EF.SOD,

3. Security attributes
a. authentication status of terminals.
b. Terminal Authorization[39].

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

1. **the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,**
2. **the successfully authenticated Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD,**
3. **the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate**

[36] [assignment: access control SFP]
[37] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[38] [assignment: access control SFP]
[39] [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]

holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD[40].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**[41]

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

1. **A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,**
2. **A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,**
3. **A terminal authenticated as DV is not allowed to read data in the EF.DG3,**
4. **A terminal authenticated as DV is not allowed to read data in the EF.DG4,**
5. **Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,**
6. **Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read the EF.DG3 to EF.DG4 of the logical MRTD**[42].

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]

FDP_UCT.1.1 The TSF shall enforce the **Access Control SFP**[43] to be able to **transmit and receive**[44] user data in a manner protected from unauthorized disclosure **after Chip Authentication**[45].

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

[40] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[41] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
[42] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[43] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[44] [selection: transmit, receive]
[45] Refinement as per BSI-CC-PP-0056

FDP_UIT.1 *Data exchange integrity*

Hierarchical to: No other components.

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

FDP_UIT.1.1 The TSF shall enforce the **Access Control SFP** [46] to be able to **transmit and receive**[47] user data in a manner protected from **modification, deletion, insertion and replay**[48] errors **after Chip Authentication**[49].

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** [50] has occurred **after Chip Authentication**[51].

Rationale for Refinement: The refinement follows the wording of BSI-PP-CC-0056 [13].

6.1.5 Class FMT Security Management

Application Note 25: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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[52].

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

[46] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[47] [selection: transmit, receive]
[48] [selection: modification, deletion, insertion, replay]
[49] Refinement as per BSI-CC-PP-0056
[50] [selection: modification, deletion, insertion, replay]
[51] refinement
[52] [assignment: list of management functions to be provided by the TSF]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifying Certification Authority,
4. Document Verifier,
5. domestic Extended Inspection System,
6. foreign Extended Inspection System[53].

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

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 manipulated,
2. Sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated,
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks[54].

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.

[53] [assignment: the authorized identified roles]
[54] [assignment: Limited capability and availability policy]

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 manipulated,
2. Sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated,
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks[55].

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**[56] the **Initialization Data and Pre-personalization Data**[57] to **the Manufacturer**[58].

Application Note 26: The Manufacturer refers to the Module Manufacturer.

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**[59] the **Initialization Data**[60] to **the Personalization Agent**[61].

[55] [assignment: Limited capability and availability policy]
[56] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[57] [assignment: list of TSF data]
[58] [assignment: the authorized identified roles]
[59] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[60] [assignment: list of TSF data]
[61] [assignment: the authorized identified roles]

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to **write**[62] the
1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date[63]
to **the Manufacturer**[64].

Application Note 27: The Manufacturer is the Module Manufacturer.

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to **update**[65] the
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate[66]
to **Country Verifying Certification Authority**[67].

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/DATE The TSF shall restrict the ability to **modify**[68] the **Current date**[69] to
1. Country Verifying Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System[70].

[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]
[68] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[69] [assignment: list of TSF data]
[70] [assignment: the authorized identified roles]

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**[71] the **Document Basic Access Keys** [72] to **the Personalization Agent**[73].

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **create**[74] the **Chip Authentication Private Key**[75] to **the Manufacturer**[76].

Application Note 28: The Manufacturer is the Module Manufacturer.

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read**[77] the
1. Document Basic Access Keys,
2. Chip authentication Private Key,
3. Personalization Agent Keys[78]
to **none**[79].

FMT_MTD.3 *Secure TSF data*

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

[71] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[72] [assignment: list of TSF data]
[73] [assignment: the authorized identified roles]
[74] [selection: create, load]
[75] [assignment: list of TSF data]
[76] [assignment: the authorized identified roles]
[77] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[78] [assignment: list of TSF data]
[79] [assignment: the authorized identified roles]

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain**[80] are accepted for **TSF data of the Terminal Authentication Protocol and the Access Control**[81].

Refinement[82]: The certificate chain is valid if and only if

(1) the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,

(2) the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

(3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying of the Country Verifying Certification Authority is not before the Current Date of the TOE.

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

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

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.

[80] Refinement as per BSI-CC-PP-0056
[81] [assignment: list of TSF data]
[82] As per BSI-CC-PP-0056

Dependencies: No Dependencies.

FPT_EMSEC.1.1 The TOE shall not emit **electromagnetic fields and power consumption information**[83] in excess of **non-useful information**[84] enabling access to **Personalization Agent Key(s) and Chip Authentication Private Key**[85] and **data stored in EF.COM, EF.SOD, EF.DG1 to EF.DG16**[86].

FPT_EMSEC.1.2 The TSF shall ensure **any users**[87] are unable to use the following interface **smart card circuit contacts**[88] to gain access to **Personalization Agent Key(s) and Chip Authentication Private Key**[89] and **data stored in EF.COM, EF.SOD, EF.DG1 to EF.DG16**[90].

Application Note 29: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card.
The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1[91].

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.

[83] [assignment: types of emissions]
[84] [assignment: specified limits]
[85] [assignment: list of types of TSF data]
[86] [assignment: list of types of user data]
[87] [assignment: type of users]
[88] [assignment: type of connection]
[89] [assignment: list of types of TSF data]
[90] [assignment: list of types of user data]
[91] [assignment: list of types of failures in the TSF]

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 conditions request of random numbers and after cryptographic operations**[92] to demonstrate the correct operation of **the TSF**[93].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of **TSF data**[94].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of **stored TSF executable code**[95].

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**[96] to the **TSF**[97] by responding automatically such that the SFRs are always enforced.

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 components:

ALC_DVS.2 and AVA_VAN.5.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

[92] [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]]
[93] [selection: [assignment: parts of TSF], the TSF]
[94] [selection: [assignment: parts of TSF], TSF data]
[95] [selection: [assignment: parts of TSF], TSF]
[96] [assignment: physical tampering scenarios]
[97] [assignment: list of TSF devices/elements]

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1				X					
FCS_CKM.1	X	X	X		X				
FCS_CKM.4	X	X	X						
FCS_COP.1/SHA	X	X	X		X				
FCS_COP.1/SYM	X	X	X		X				
FCS_COP.1/MAC	X	X	X		X				
FCS_COP.1/SIG_VER	X		X						
FCS_RND.1	X		X						
FIA_UID.1	X	X	X						
FIA_UAU.1	X	X	X						
FIA_UAU.4	X	X	X						
FIA_UAU.5	X	X	X						
FIA_UAU.6	X	X	X						
FIA_API.1					X				
FDP_ACC.1	X	X	X						
FDP_ACF.1	X	X	X						
FDP_UCT.1			X						
FDP_UIT.1		X							
FMT_SMF.1	X	X							
FMT_SMR.1	X	X							
FMT_LIM.1						X			
FMT_LIM.2						X			
FMT_MTD.1/INI_ENA				X					
FMT_MTD.1/INI_DIS				X					
FMT_MTD.1/CVCA_INI			X						
FMT_MTD.1/CVCA_UPD			X						
FMT_MTD.1/DATE			X						
FMT_MTD.1/KEY_WRITE	X								
FMT_MTD.1/CAPK		X	X		X				
FMT_MTD.1/KEY_READ	X	X	X		X				
FMT_MTD.3			X						
FPT_EMSEC.1	X						X		
FPT_TST.1							X		X
FPT_FLS.1							X		X
FPT_PHP.3							X	X	

Table 5 - 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 FIA_UID.1, FUI_UAU.1, FDP_ACC.1 and FDP_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. If the Personalization Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1, FCS_COP.1/SHA (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6 (for the re-authentication). If the Personalization Terminal wants to authenticate itself to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/SYM (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMSEC.1 the 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 in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6. The SFR FIA_UAU.6 and FDP_UIT.1 requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1 (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

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

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

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

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

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

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

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

The security objective OT.Chip_Auth_Proof “Proof of MRTD’s chip authenticity” is ensured by the Chip Authentication Protocol provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1 is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol [3] requires additional TSF according to FCS_COP.1/SHA (for the derivation of the session keys), FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging).

The security objective OT.Prot_Abuse-Func “Protection against Abuse of Functionality” is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other 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/SYM 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 attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1,
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	justification 1 for non-satisfied dependencies,

SFR	Dependencies	Support of the Dependencies
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/SYM	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1, Fulfilled by FCS_CKM.4
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1, Fulfilled by FCS_CKM.4
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1, Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 2 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 3 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path],	justification 3 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	[FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	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_SMR.1 Fulfilled by FMT_SMF.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1 Fulfilled by FMT_SMF.1
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 6 - 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 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 attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

No. 3: The SFR FDP_UCT.1 and FDP_UIT.1 require the use of secure messaging between the MRTD and the GIS. 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.

No. 4: The TOE consists of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

6.3.3 Security Assurance Requirements Rationale

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

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

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

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description;
- ADV_FSP.2 Security-enforcing functional specification;
- ADV_TDS.3 Basic modular design;
- ADV_IMP.1 Implementation representation of the TSF;
- AGD_OPE.1 Operational user guidance; and
- AGD_PRE.1 Preparative procedures.

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

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

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

The dependency analysis in section 6.3.2 Dependency Rationale 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

The authentication protocol for personalization, together with corresponding access control (FDP_ACC.1, FDP_ACF.1) and security management features, ensure that only a legitimate Personalization Agent (FMT_SMR.1) is granted access to the Personalization functions of the TOE. All protocol messages are protected against violations of confidentiality and integrity to ensure that unauthentic parties shall not succeed in reading or modifying the protocol messages during personalization.

This security function concerns with the confidentiality of the personalization data of the MRTD. The security measures are largely overlapping with the security measures for the security function concerning with the integrity of the personal data of MRTD holders (SF.Data_Int) and confidentiality of the MRTD holder´s biometric data (SF.Sens_Data_Conf).

The TOE implents a rich set of mechanisms and cryptographic operations (FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SIG_VER, FCS_RND.1) to identify and authenticate the Personalization Agent (FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FMT_MTD.3), to establish a secure communication channel with the Persoanlization Agent, and to allow the Personalization Agent to recognize the TOE as authentic (FIA_API.1) using the private key stored on the TOE by the Module Manufacturer (FMT_MTD.1/CAPK).

Only the Personalization Agent is allowed to disable read access to the initialization data stored during the TOE initialization (FMT_MTD.1/INI_DIS) and write the Document Basic Access Keys (FMT_MTD.1/KEY_WRITE). The initialization and pre-personalization data, including the IC identification data, can only be written by the Manufacturer (specifically, the Module Manufacturer) (FAU_SAS.1, FMT_MTD/INI_ENA). Initialization, pre-personalization and personalization are well defined management functions (FMT_SMF.1) and Manufacturer and Personalization Agent are well defined TOE user roles (FMT_SMR.1). Reading of the initialization data is allowed prior to identification and authentication of users unless disabled by the Personalization Agent (FIA_UID.1, FIA_UAU.1).

Once the private keys Document Basic Access Key, Chip Authentication Private Key, or Personalization Agent Keys are written to the TOE during initialization, manufacturing or personalization, nobody is allowed to read them (FMT_MTD.1/KEY_READ).

The access control restrictions together with the communication between the TOE and the reader ensure that any communication between the TOE and a Terminal is protected for confidentiality and integrity (FDP_UIT.1, FDP_UCT.1). All cryptographic computations by the TOE are implemented in such a manner that no intelligible emanations are emitted in quantities which could be used for constituting successful cryptoanalytical attacks against the TOE and that probing of the TOE contacts does not allow an attacker to harvest information in sufficient quantities as to facilitate successful attacks against the TOE (FPT_EMSEC.1).

7.2 SF.Data_Int: Integrity of Personal Data

This security function concerns with the integrity of the MRTD Holder´s personal data during personalization. This is achieved by using the authentication protocol por personalization and subsequent secure channels for any communication between the TOE and the (authenticated) Personalization Agent. These measures are largely overlapping with the measures implemented to achieve confidentiality of the personalization data. They specifically prevent violations of integrity of the protocol messages (FDP_UIT.1).

The TOE maintains a well-defined set of roles and only allows an authorized Personalization Agent (FMT_SMR.1) to personalize the TOE (FMT_SMF.1) and only allows the Module Manufacturer (FMT_SMR.1) to write the private key used for chip authentication protocol (FMT_MTD.1/CAPK). This ensures that no unauthorized party can violate the integrity of the MRTD by successfully injecting unauthentic personal data on the MRTD. No party is allowed to read the cryptographic keys stored on the TOE (FMT_MTD.1/KEY_READ) and the TOE measures ensure that the TOE resists attacks which would allow user data to be manipulated or allow deployment of features disabled when the TOE is moved to subsequent life-cycle stages (FMT_LIM.1, FMT_LIM.2). Hence, only after a successful cryptoanalytical attack would an unauthentic party succeed in masquerading as a legitimate Personalization Agent which may not occur in practice as the TOE uses random number generators of good quality, recognized cryptographic primitives and key derivation techniques, and ensures that all residual key material is erased once no longer used.

7.3 SF.Sens_Data_Conf: Confidentiality of Sensitive Biometric Reference Data

The confidentiality of the sensitive biometric reference data is protected by the TOE by numerous means:

1. Access to the biometric reference data (EF.DG3 and EF.DG4) is only granted to a legitimate Extended Inspection System after successful authentication of the terminal as such (FDP_ACF.1, FDP_ACC.1). Any terminal not successfully authenticated as Extended Inspection System shall not be granted access to the biometric reference data. Terminals authenticated as Country Verification Certification Authorities (CVCA) or Document Verifiers (DV) are not granted access to the biometric reference data (FDP_ACF.1, FDP_ACC.1, FMT_SMR.1).The access control rules specifically ensure that any data communicated between the TOE and a terminal after successful terminal authentication is protected from disclosure to unauthorized parties (FDP_UCT.1).;
2. All inspection systems must be identified and authenticated prior to the establishment of the secure sessions between the terminal and the TOE and the TOE restricts the functions available to the terminals not identified and authenticated only to the basic accesses required for identification and authentication (FIA_UID.1, FIA_UAU.1);
3. A rich set of authentication mechanisms is implemented by the TOE to authenticate various parties as described in Sect. 7.1. Only upon successful Chip Authentication and Terminal Authentication shall a Terminal be assigned to a role Extended Inspection System and granted a read access to the biometric reference data (FDP_ACF.1, FDP_ACC.1, FMT_SMR.1). The role Extended Inspection System is further divided into

domestic and foreign based on the Document Verified Certificate. The Extended Inspection System is domestic if the Document Verified Certificate belongs to the same State as the Country Verifying Certification Authority and foreign if the Document Verifier Certificate does not belong to the same state is the Country Verifying Certification Authority. From the MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization;

4. All communication between the TOE and the Extended Inspection System is protected against violations of confidentiality and integrity so that any party eavesdropping the communication shall fail in learning the sensitive biometric reference data of Travelers.
5. The credentials for users to enter roles CVCA or DV (incl. the original date) are initially written on the TOE by the Manufacturer (FMT_MTD.1/CVCA_INI) and can only be updated by the CVCA (FMT_MTD.1/CVCA_UPD);
6. Only the successfully authenticated Country Verifying Certification Authority, Document Verifier, or domestic Extended Inspection System is allowed to modify the Current Date stored on the TOE (FMT_MTD.1/DATE); and
7. Given that the security objectives of the environment of the TOE concerning with issuing states and organizations only granting certificates giving access to the sensitive biometric data are only issued to legitimate parties (OE.Authoriz_Sens_Data and OE.Ext_Insp_Systems), the measures implemented by the TOE under SF.Sens_Data_Conf are sufficient to prevent disclosure of biometric reference data to unauthentic parties.

7.4 SF.Identification: Identification and Authentication of the TOE

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 only be read by the Personalization Agent during Phase 3 “Personalization of the MRTD”, but it is not accessible to the Inspection System during Phase 4 “Operational Use” (FMT_MTD.1/INI_DIS) if disabled by the Personalization Agent.

7.5 SF.Chip_Auth_Proof: Proof of MRTD´s Chip Authenticity

The TOE implements a chip authentication protocol to provide a terminal an ability to assert the identity of the TOE (FIA_API.1). The protocol is based in a Diffie-Hellman key exchange (FCS_CKM.1) of keys from which a symmetric session key is derived and used for a symmetric mutual authentication of the terminal and the chip (FCS_COP.1/SYM). The secure messaging channel over which the authentication is performed uses secure hash functions (FCS_COP.1/SHA) and cryptographic message authentication codes (FCS_COP.1/MAC). The chip authentication results are trustworthy as only the Manufacturer is allowed to write the Chip Authentication Private Key used in the Chip authentication protocol (FMT_MTD.1/CAPK) and the TOE ensures that no party is able to read the key (FMT_MTD.1/KEY_READ), hence preventing the possibility of an unauthentic party masquerading as the TOE.

7.6 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).

7.7 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 7.8 and 7.9 (FPT_FLS.1, FPT_TST.1, FPT_PHP.3).

7.8 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.

7.9 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
BAC	Basic Access Control
BIS	Basic Inspection System
BSI	Bundesamt für Sichereit 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
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, “Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)”.

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

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

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

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

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

[9] RSA Laboratories, “PKCS #3: Diffie-Hellman Key-Agreement Standard, Version 1.4,” 1993.

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

[11] RSA Laboratories, “PKCS #1: RSA Cryptography Standard, Version 2.1,” 2002.

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

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

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

[15] CEITEC, Security Target for CEITEC ePassport Module CTC21001 with BAC.

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

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

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

[19] 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.

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

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

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

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

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

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

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