# cv act ePasslet/EACv1 v1.8

# Security Target

## BSI-DSZ-CC-0797

**Common Criteria / ISO 15408**

**EAL 4+**

**Document Version 1.05 • 2012-08-17**

cv cryptovision GmbH • Munscheidstr. 14 • 45886 Gelsenkirchen • Germany
www.cryptovision.com • info@cryptovision.com • +49-209-167-2450

# Content

## Version Control

| Version | Date | Author | Changes to Previous Version |
|---|---|---|---|
| 0.1 | 2010-10-21 | Thomas Zeggel | Initial version |
| 0.2 | 2010-10-26 | Benjamin Drisch | Corrections |
| 0.3 | 2010-11-01 | Thomas Zeggel | Added chapter 5 and 6. |
| 0.4 | 2010-11-05 | Thomas Zeggel | Added chapter 7.<br>Additional corrections and refinements. |
| 0.5 | 2010-11-12 | Benjamin Drisch | Minor corrections |
| 0.51 | 2010-11-23 | Thomas Zeggel | Added tables and other insertions; correction of augmented packages in section 1.3. |
| 0.52 | 2010-11-29 | Thomas Zeggel | Complete renewal of chapter 7.1. Change of the internal structure of chapter 1 and 2. Other small changes based on the result of discussions with NXP. |
| 0.6 | 2010-12-13 | Thomas Zeggel | Chapter 7 extended. |
| 0.61 | 2010-12-20 | Thomas Zeggel | Change of the TOE efinition in chapter 1. Changes and additions to chapter 7. |
| 0.62 | 2011-01-06 | Thomas Zeggel | Small corrections. |
| 0.7 | 2011-01-07 | Benjamin Drisch, Thomas Zeggel | Internal review version with minor corrections. |
| 0.8 | 2011-01-21 | Thomas Zeggel | Small corrections and changes in chapter 1 after review by NXP. |
| 0.9 | 2011-08-24 | Benjamin Drisch | Changes from TÜViT review of BAC-ST included |
| 0.91 | 2011-08-25 | Benjamin Drisch | Internal review – minor changes |
| 0.93 | 2011-08-29 | Thomas Zeggel | Internal review – minor changes |
| 0.94 | 2011-09-27 | Thomas Zeggel | Internal review – minor changes |
| 0.95 | 2011-10-10 | Thomas Zeggel | Changes according to TüvIT OR and refinement of the lifecycle description according to the discussion about the ALC documentation. |
| 0.96 | 2011-11-10 | Benjamin Drisch, Thomas Zeggel | Changes according to the results of the BSI evaluation kick-off meeting and the remarks in the TüvIT observation report to the SSCD ST. |
| 0.97 | 2011-12-09 | Thomas Zeggel | Changed product name in ePasslet/EACv1 v1.8.<br>Jusitification 4 in chapter 6.4.2 deleted.<br>Residual content regarding active authentication deletd.<br>Key lengths adjusted according to latest JCOP ST.<br>Comments in SFR mappings of chapter 2.2 added.<br>Reference for BAC Security Target added.<br>Text before application note 9 corrected. |

| | | | |
|---|---|---|---|
| | | | Change of name of chapter 1.1.<br>FDP_UCT.1.1, FDP_UIT.1.2, FIA_UAU.2, FPT_EMSEC.1 modified according to evaluator's comments. |
| 0.98 | 2011-12-12 | Thomas Zeggel | Minor correction of product name in section 1.1 |
| 0.99 | 2011-12-12 | Thomas Zeggel | Minor corrections |
| 1.00 | 2012-02-27 | Thomas Zeggel | Changes and corrections, based on comments by the BSI:<br>• Added certification ID of platform, crypto lib and hardware in section 1.3.2<br>• Added remarks about EC parameters from JCOP (with according reference)<br>• Included remark on PP conformance claim in section 2.1 |
| 1.01 | 2012-03-01 | Benjamin Drisch | • Corrected Certification ID of underlying hardware platform for P5CD080 |
| 1.02 | 2012-03-15 | Benjamin Drisch | • Added missing mapping between FIA_UAU.5 and TSF_Auth in table 13<br>• Clarified life cycle of the TOE according to ALC in section 1.3.5<br>• Added clarification of MIFARE functionality in section 1.3.2 |
| 1.03 | 2012-04-16 | Benjamin Drisch | • Clarified TOE definition and life-cycle description |
| 1.04 | 2012-08-16 | Benjamin Drisch | Revised TOE definition<br>• corrected references to underlying certificates for Crypto Library and HW platform in 1.3.2<br>• explicitely stated contact-based interface<br>Corrected reference to Guidance Manual and ePasslet/BAC Security Target |
| 1.05 | 2012-08-17 | Thomas Zeggel | Corrected date of BAC Security Target in the references |

# 1 Introduction

## 1.1 ST/TOE Identification

| | |
|---|---|
| Title: | cv act ePasslet/EACv1 v1.8 Security Target |
| Version: | v1.05 |
| Origin: | cv cryptovision GmbH |
| Compliant to: | Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control (BSI-CC-PP0056) [PP0056] |
| Product identification: | cv act ePasslet/EACv1 v1.8 |
| ROM identification value: | P5Cx081UA: 8F80EC<br>P5Cx080UA: 7C1970<br>P5Cx040UA: F39353 |
| Javacard OS platform: | NXP JCOP 2.4.1 R3 [ZertJCOP080], [ZertJCOP040], [ZertJCOP081] |
| Security controller: | [ZertIC080], [ZertIC040], [ZertIC081] |
| TOE identification: | cv act ePasslet/EACv1 v1.8 |
| TOE documentation: | Administration and user guide [Guidance] |

## 1.2 ST overview

The aim of this document is to describe the Security Target for MRTD chips based on the EAC application of the cv act ePassslet Suite. The cv act ePasslet Suite is a set of Javacard applications intended to be used exclusively on the NXP JCOP Javacard OS platform, which is certified according to CC EAL 5+ [ZertJCOP080], [ZertJCOP040], [ZertJCOP081]. The cv act ePasslet Suite as well as the NXP JCOP operating system are provided within the ROM mask of a smart card chip based on the NXP P5CD security controller, which is itself certified according to CC EAL 5+ [ZertIC080], [ZertIC040], [ZertIC081].

This security target claims strict conformance to the Protection Profile *Machine Readable Travel Document with "ICAO Application", Extended Access Control (*BSI-CC-PP0056) [PP0056].

The main objectives of this ST are:

- to introduce TOE and the MRTD application,
- to define the scope of the TOE and its security features,
- to describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- to describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- to specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functionalities.

The assurance level for the TOE is CC EAL4+.

## 1.3 TOE overview

### 1.3.1 Overview of cv act ePasslet Suite

The cv act ePasslet Suite is a modular multi-application solution for eID documents based on Java Card.

It provides the following applications:

| Application name | Function | Standard |
|---|---|---|
| cv act ePasslet/BAC | Basic Access Control | ICAO Doc 9303 |
| cv act ePasslet/EACv1 | Extended Access Control, V1.11 | BSI TR03110, V1.11 |
| cv act ePasslet/EACv2-SAC | Extended Access Control, V2.05 | BSI TR03110, V2.05 |
| cv act ePasslet/GeID | German eID card | BSI TR03127, BSI TR03110 |
| cv act ePasslet/ePKI | IAS with own PKCS#15 profile | PKCS#15 |
| cv act ePasslet/IDL | International Driving License | ISO 18013 |
| cv act ePasslet/eHIC | European Health Insurance | CWA 15974 |
| cv act ePasslet/EuCCB | European Citizen Card - Base Profile | CEN/TS 15480 |
| cv act ePasslet/EuCCF | European Citizen Card - French Profile | GIXEL IAS-ECC V1.01 |
| cv act ePasslet/eVR | Electronic Vehicle Registration | EU Council Directive 1999/37/EC |
| cv act ePasslet/NIDS | Combination of EAC V1.11 and ePKI | BSI TR03110, V1.11, PKCS#15 |

*Table 1: Customer view of the available applications in the cv act ePasslet Suite.*

These applications are realized by configurations of one or more predefined applets; while each application has a distinct configuration, different applications might use the same underlying applet. For details on the relation between applets and applications please refer to Figure 1.

While the whole applet code resides in ROM, the applets providing the different applications are instantiated into EEPROM. Multiple applications can be present at the same time by instantiating multiple applets with their distinct configurations with some restrictions detailed below. A common combination could be an EACv1 applet and an ePKI applet providing a travel application with LDS data and EAC authentication together with a signature application (offered as own standard product configuration “NIDS” as listed in Table 1, Figure 1 and Figure 2).

The cv act ePasslet Suite is available in two variants:

**Variant 1**

- available on P5Cx081 and P5Cx041
- covering all applications provided in Table 1
- certified products (on P5Cx081 only):
  - BAC certified according to PP0055
  - EACv1 certified according to PP0056
  - EACv2-SAC certified according to SAC/PACE-PP
  - ePKI certified as Secure Signature Creation Device (SSCD) according to PP0059 (contact and contactless with PACE)

The following Figure 1 gives an overview of the available applications and actual applets in variant 1.

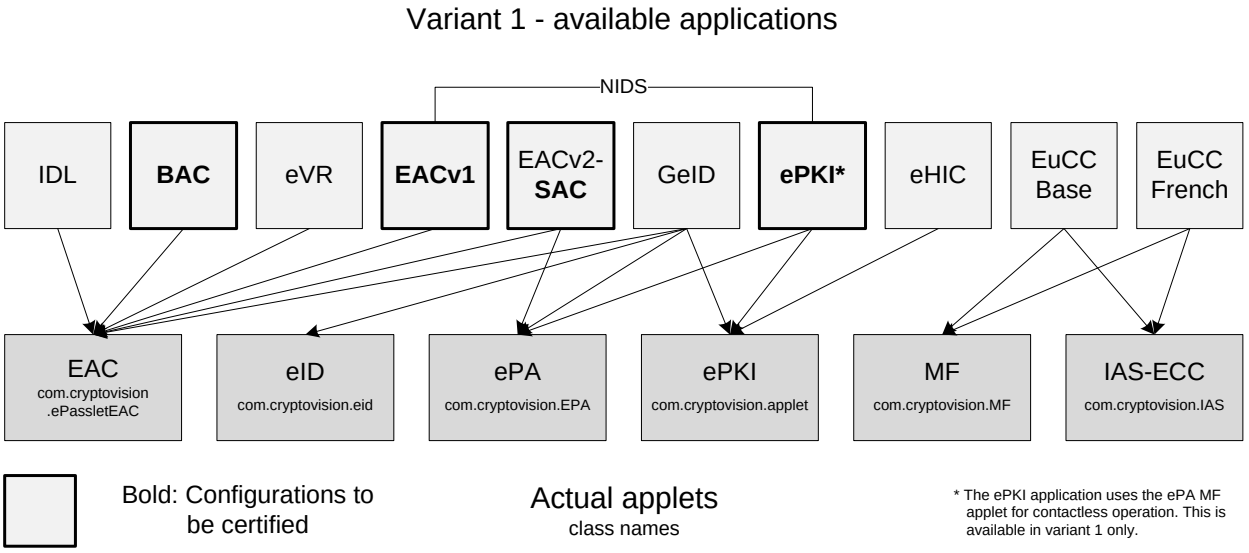



*Figure 1: Available applications and actual applets in variant 1.*

The other version (variant 2) contains a subset of these applications:

**Variant 2**

- available on P5Cx080 and P5Cx040
- Contains the applets and applications indicated in Figure 2
- certified products:
  - BAC certified according to PP0055
  - EACv1 certified according to PP0056
  - ePKI certified as Secure Signature Creation Device (SSCD) according to PP0059 (contact interface only)

The following Figure 2 gives an overview of the available applications and actual applets in variant 2.

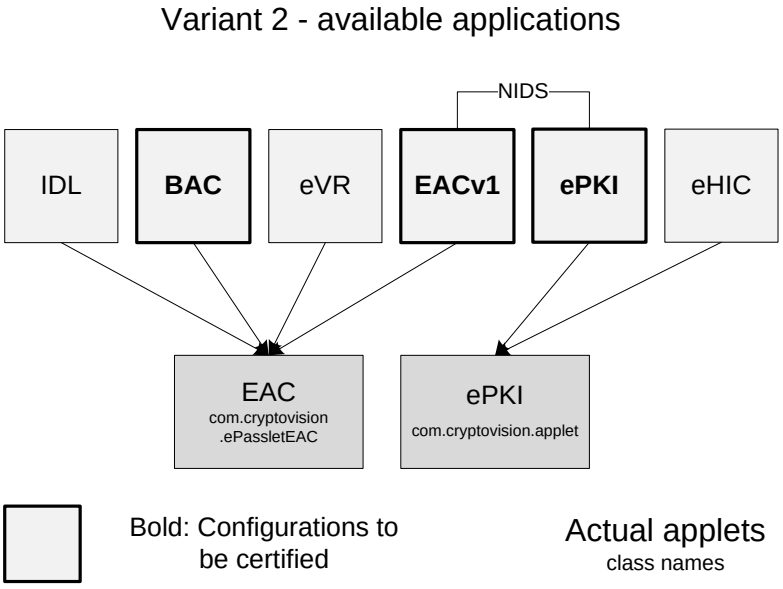



*Figure 2: Available applications and actual appletsin variant 2.*

Combinations of certified and non-certified applications are possible (as long as these applications use one of the above applets instantiated from ROM).

Via configuration the instanciated applets can be tied to the contactless and/or the contact interface, respectively. BAC, EACv1, EACv2-SAC require exclusive access to the contactless interface. Hence, if one of these applications is used (in certified configuration), further (certified or non-certified) applications have to be bound to the contact interface.

These additional applications have to be instanciated from the ROM mask. That especially excludes additional applet code being loaded and installed into EEPROM.

### 1.3.2 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip containing components for a machine readable travel document (MRTD chip). After instantiation and configuration of the cv act ePasslet/EACv1 application it can be programmed according to the Logical Data Structure (LDS) [ICAODoc] and providing the Basic Access Control and the Extended Access Control according to the ICAO document [ICAODoc] and the technical report [TR-03110].

The TOE consists of

- the circuitry of the MRTD's chip (the integrated circuit, IC) including the contact-based interface with hardware for the contactless interface including contacts for the antenna,
- the platform with the Java Card operation system JCOP 2.4.1R3 by NXP, in the variants
    - JxA081, A, B1, B4, Certification ID BSI-DSZ-CC-0675-2011 ([ST_JCOP081], [ZertJCOP81]) with crypto library version 2.7, Certification ID BSI-DSZ-CC-0633-2010 ([ST_CL081], [ZertCL081]) and hardware P5Cx081V1A, Certification ID BSI-DSZ-CC-0555-2009 ([ST_IC081], [ZertIC081]),
    - J2A080, Certification ID BSI-DSZ-CC-0674-2011 ([ST_JCOP080], [ZertJCOP80]) with crypto library version 2.6, Certification ID BSI-DSZ-CC-0709-2010 ([ST_CL080], [ZertCL080]) and hardware P5Cx080V0B , Certification ID BSI-DSZ-CC-0410-2010 ([ST_IC080], [ZertIC080]),
    - JxA040, A, B1, B4, Certification ID BSI-DSZ-CC-0730-2011 ([ST_JCOP040], [ZertJCOP40]) with crypto library version 2.6, Certification ID BSI-DSZ-CC-0710-2010 ([ST_CL040], [ZertCL040]) and hardware P5Cx040VOB, Certification ID BSI-DSZ-CC-0404-2007 ([ST_IC040], [ZertIC040]).
- cv act ePasslet/EACv1 v1.8 as the only application that has access to the contactless interface,
- the associated guidance documentation Administrator and User Guidance [Guidance].

The TOE's functionality claimed by this Security Target is realized by the cv act ePasslet/EACv1 v1.8 application **only**.

Some of the underlying platform variants of this composite TOE provide MIFARE functionality; please note that this functionality is out of scope of the TOE's security functionality claimed by this Security Target.

### 1.3.3 TOE usage and security features for operational use

This paragraph is directly based on the corresponding paragraph in the protection profile [PP0056].

A state or organisation issues a MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity.

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

tactless machine reading. The authentication of the traveller 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) biometrics using the reference data stored in the MRTD.

The issuing state or organization ensures the authenticity of the data of genuine MRTD's. The receiving state trusts a genuine MRTD of an issuing state or organization.

Within this security target the MRTD is viewed as a unit of

- 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.
- the logical MRTD as data of the MRTD holder stored according to the Logical Data Structure [ICAODoc] as specified by ICAO on the contactless integrated circuit. Via the contactless interface of the integrated circuit, the following data including (but not limited to) personal data of the MRTD holder are accessible:
  (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  (2) the digitized portraits (EF.DG2),
  (3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both2
  (4) the 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 passport book and the MRTD's chip is uniquely identified by the document number.

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

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

The ICAO 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 biometrics as optional security measure in the ICAO Technical Report [ICAODoc]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism and the Extended Access Control Mechanism. This security target addresses the Chip Authentication described in [TR-03110] as an alternative to the Active Authentication stated in [ICAODoc].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this security target as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfill the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP0055]. Due to the fact that [PP0055] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately. The evaluation and certification process will be carried out simultaneously to the current process according to the security target in hand.

**PP application note 1:** As explained in the protection profile [PP0056] there is a separate Security Target for BAC [ST_BAC].

For BAC, the inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAODoc], normative appendix 5.

The security target requires the TOE to implement the Chip Authentication defined in [TR-03110]. The protocol provides evidence of the MRTD's chip authenticity and prevents data traces described in [ICAODoc], Annex G, section G.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 a 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. it could apply the Chip Authentication Private Key corresponding to the Chip Authentication Public Key for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The security target requires the TOE to implement the Extended Access Control as defined in [TR-03110]. The Extended Access Control consists of two parts (i) a Terminal Authentication Protocol to authenticate the inspection system as entity authorized by the Issuing State or Organization through the receiving State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. It requires the Chip Authentication of the MRTD's chip to the inspection system and uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

### 1.3.4 Major security features of the TOE

The TOE provides the following TOE security functionalities:

- TSF_Access manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data.
- TSF_Admin manages the storage of manufacturing data, pre-personalization data and personalization data.
- TSF_Secret ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These mechanisms are mainly provided by TSF_OS.
- TSF_Crypto performs high level cryptographic operations. The implementation is mainly based on the Security Functionalities provided by TSF_OS. The supported crypto mechanisms are:
    - the Diffie-Hellman key derivation Protocol with cryptographic key sizes between 512 and 2048 bit (in steps of 64 bit), and ECDH compliant to ISO 15946 with cryptographic key sizes between 128 and 320 bit,
    - digital signature verification in accordance with RSA and cryptographic key sizes between 512 and 2048 bit (in steps of 64 bit), and ECDSA with cryptographic key sizes between 128 and 320 bit,

  - Terminal Authentication Protocol, Secure messaging in MAC-ENC mode, and Symmetric Authentication Mechanism based on Triple-DES.

- TSF_SecureMessaging realizes a secure communication channel with MACs and encryption based on Triple-DES (112 bit key length).
- TSF_Auth realizes different authentication mechanisms: TSF_Auth_Term (Terminal Authentication), TSF_Auth_3DES used for BAC and symmetric authentication based on pre-shared keys used for personalization and TSF_Auth_Chip to manage the capability of the TOE to authenticate itself to the terminal using the Chip Authentication Protocol (EAC).
- TSF_Integrity protects the integrity of internal applet data like the Access control lists.
- TSF_OS contains all security functionalities provided by the certified platform (IC, crypto library, Javacard operation system). Besides some minor additions, the cryptographic operations are provided by this platform.

### 1.3.5 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases. This paragraph is directly based on the corresponding paragraph in the protection profile [PP0056].

#### 1.3.5.1 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.

(Step 2) The software developer[1] uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

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

#### 1.3.5.2 Phase 2: Manufacturing

(Step 3) In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the nonvolatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

**The TOE delivery according to CC is the delivery of the IC (with the application code in ROM) from the IC manufacturer to the MRTD manufacturer.**

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

(Step 4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

(Step 5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD's chips with pre-personalization Data.

[1] Please note that in this ST the role software developer of the protection profile is subdivided into two separate roles: the operating system is developed by the OS software developer, and the MRTD application by the (MRTD) software developer.

**PP application note 2:** Creation of the application implies applet instantiation.

**In this step the final (but not yet personalized) MRTD is generated from the certified components according to the binding initialization and pre-personalization guidelines provided in [Guidance].**

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

#### 1.3.5.3 Phase 3: Personalisation of the MRTD

(Step 6) The personalization of the MRTD includes (i) the survey of the MRTD holder 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 and their secure transfer to the personalisation agent, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) the writing the TSF Data into the logical MRTD and configuration of the TSF if necessary. The step (iv) is performed by the Personalisation Agent and includes but is not limited to the creation of (i) the digital MRZ data (DG1), (ii) the digitised portrait (DG2), and (iii) the Document security object.

The signing of the Document security object by the Document signer [ICAODoc] 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.

**PP application note 3:** <Information only – no action required>

**PP application note 4:** As in the PP this ST distinguishes between the roles „personalization agent“ and „doument signer“

#### 1.3.5.4 Phase 4: Operational use

(Step 7) The TOE is used as MRTD’s chip by the traveller and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the Issuing State or Organization and used according to the security policy of the Issuing State but they can never be modified.

**PP application note 5:** The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.

**PP application note 6:** The intention of the underlying PP [PP0056] is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the “Operational Use” (phase 4) have to be considered in the product evaluation process under AGD assurance class.

**Remark:** This ST considers only phase 1 and parts of phase 2 (steps 1 - 3) as part of CC evaluation under ALC.

### 1.3.6 Non-TOE hardware/software/firmware required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are

needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

# 2 Conformance claims

## 2.1 CC conformance

This security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009, version 3.1 revision 3, [CC_1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, July 2009, version 3.1 revision 3, [CC_2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, July 2009, version 3.1 revision 3, [CC_3],

as follows:

- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC_3].

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [CC_4]

has to be taken into account.

This security target claims strict conformance to the Protection Profile *Machine Readable Travel Document with "ICAO Application", Extended Access Control* (BSI-CC-PP0056) [PP0056][2]. No extensions have been made.

The evaluation of the TOE uses the result of the CC evaluation of the P5CD chip claiming conformance to the PP [PP0035]. The hardware part of the composite evaluation is covered by the certification report [ZertIC080], [ZertIC040], [ZertIC081]. In addition, the evaluation of the TOE uses the result of the CC evaluation of the JCOP 2.4.1R3 Javacard OS claiming conformance to the PP [PP_Javacard]. The Javacard OS part of the composite evaluation is covered by the certification report [ZertJCOP080], [ZertJCOP040], [ZertJCOP081].

**PP application note 7:** <Information only – no action required>.

## 2.2 Statement of Compatibility concerning Composite Security Target

### 2.2.1 Assessment of the Platform TSFs

The following Table 2 lists all Security Functionalities of the underlying Platform ST and shows, which Security Functionalities of the Platform ST are relevant for this Composite ST and which are irrelevant. The first column addresses specific Security Functionality of the underlying platform, which is assigned to Security Functionalities of the Composite ST in the second column. The last column provides additional information on the correspondence if necessary.

[2] PP Application Note 7: information only – no action required

| Relevant Platform TSF-group | Correspondence in this ST | References/Remarks |
|---|---|---|
| SF.AccessControl | TSF_Access | |
| SF.Audit | TSF_Admin | |
| SF.CryptoKey | TSF_Secret | |
| SF.CryptoOperation | TSF_Crypto | |
| SF.I&A | TSF_Access | |
| SF.SecureManagement | TSF_Admin, TSF_Integrity | |
| SF.Transaction | TSF_Integrity | |
| SF.Hardware | TSF_OS | Implicitly used via JCOP (TSF_OS)* |
| SF.CryptoLib | TSF_OS | Implicitly used via JCOP (TSF_OS)* |

*Table 2: Relevant platform TSF-groups and their correspondence*

*** Remark:** The Platform TSF-groups "SF.Hardware" and "SF.CryptoLib" are not directly used by Security Functionalities of the TOE, they are (implicitly) invoked by calls to the JCOP operating system, though. These OS calls are grouped in the TSF_OS.

### 2.2.2 Assessment of the Platform SFRs

The following Table 3 provides an assessment of all relevant Platform SFRs.

| Relevant Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| FAU: Security Audit | | |
| FAU_ARP.1/JCS | FPT_PHP.3 | Internal counter for security violations complement JCOP mechanisms |
| FAU_SAA.1 | FPT_PHP.3 | Internal counter for security violations complement JCOP mechanisms |
| FAU_SAS.1 | FAU_SAS.1 | Fullfillment of the platform SFR leads directly to the SFR of this ST. |
| FCS: CRYPTOGRAPHIC SUPPORT | | |
| FCS_CKM.1 | FCS_CKM.1 | The requirements are equivalent: EC keys and RSA keys of the platform SFR correspond to the Diffie-Hellman and ECDH keys of this ST. |
| FCS_CKM.2 | No correspondence | Out of scope (managed within JCOP)<br>No contradiction to this ST |
| FCS_CKM.3 | No correspondence | Out of scope (managed within JCOP)<br>No contradiction to this ST |
| FCS_CKM.4 | FCS_CKM.4 | The requirements are equivalent (physically overwriting the keys with zeros). |
| FCS_COP.1 | FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER | The requirements are equivalent: FCS_COP.1/SHA of this ST corresponds to the platform SFR FCS_COP.1/SHA-1, FCS_COP.1/SHA-224 and |

| Relevant Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| | | FCS_COP.1/SHA-256; FCS_COP.1/SYM corresponds to the platform SFR FCS_COP.1/TDES_MRTD; FCS_COP.1/MAC corresponds to the platform SFR FCS_COP.1/MAC_MRTD; FCS_COP.1/SIG_VER corresponds to the platform SFR FCS_COP.1/ECSignature and FCS_COP.1/RSASignaturePKCS#1. |
| FCS_RNG.1 | FCS_RND.1 | Fullfillment of the platform SFR leads directly to the SFR of this ST. |
| FDP: User Data Protection | | |
| FDP_ACC.1/CMGR | No correspondence | Refers to LC state before Applet instantiation<br>No contradiction to this ST |
| FDP_ACC.1/SCP | No correspondence | Out of scope (JCOP memory management)<br>No contradiction to this ST |
| FDP_ACC.2/FIREWALL | No correspondence | Out of scope (JCOP firewall mechanism)<br>No contradiction to this ST |
| FDP_ACF.1/FIREWALL | No correspondence | Out of scope (JCOP access control mechanisms)<br>No contradiction to this ST |
| FDP_ACF.1/CMGR | No correspondence | Out of scope (JCOP access control mechanisms)<br>No contradiction to this ST |
| FDP_ACF.1/SCP | No correspondence | Out of scope (JCOP access control mechanisms)<br>No contradiction to this ST |
| FDP_ETC.1 | No correspondence | Out of scope (JCOP data control mechanisms)<br>No contradiction to this ST |
| FDP_IFC.1/JCVM | No correspondence | Out of scope (refers to Virtual Machine)<br>No contradiction to this ST |
| FDP_IFC.1/SCP | No correspondence | No contradiction to this ST |
| FDP_IFF.1/JCVM | No correspondence | Out of scope (refers to Virtual Machine)<br>No contradiction to this ST |
| FDP_ITC.1 | No correspondence | Out of scope (JCOP data control mechanisms) |

| Relevant Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| | | No contradiction to this ST |
| FDP_ITT.1/SCP | No correspondence | Out of scope (platform internal data transfer)<br>No contradiction to this ST |
| FDP_RIP.1 | FCS_CKM.4 | Relied on for key deletion<br>No contradiction to this ST |
| FDP_ROL.1/FIREWALL | No correspondence | Out of scope (refers to Virtual Machine)<br>No contradiction to this ST |
| FDP_SDI.2 | No correspondence | Out of scope (JCOP internal data integrity protection)<br>No contradiction to this ST |
| FIA: Identification and Authentication | | |
| FIA_AFL.1/PIN | No correspondence | Out of scope (no PINs used within applet)<br>No contradiction to this ST |
| FIA_AFL.1/CMGR | No correspondence | Out of scope (refers to card manager)<br>No contradiction to this ST |
| FIA_ATD.1/AID | No correspondence | Out of scope (JCOP AID management)<br>No contradiction to this ST |
| FIA_UAU.1 | FIA_UAU.1 | The SFR in this ST extends the allowed actions of the platform SFR. No contradiction to this ST. |
| FIA_UAU.3/CMGR | No correspondence | Refers to LC state before Applet instantiation<br>No contradiction to this ST |
| FIA_UAU.4/CMGR | No correspondence | Refers to LC state before Applet instantiation<br>No contradiction to this ST |
| FIA_UID.1/CMGR | No correspondence | Refers to LC state before Applet instantiation<br>No contradiction to this ST |
| FIA_UID.2/AID | No correspondence | Out of scope (JCOP AID management)<br>No contradiction to this ST |
| FIA_USB.1 | No correspondence | Out of scope (JCOP applet management)<br>No contradiction to this ST |
| FMT: Security Management | | |
| FMT_LIM.1 | FMT_LIM.1 | The SFR of this St is refinement of the platform SFR. No contradictions to this ST. |

| Relevant Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| FMT_LIM.2 | FMT_LIM.2 | The SFR of this St is refinement of the platform SFR. No contradictions to this ST. |
| FMT_MSA.1/JCRE | No correspondence | Out of scope (JCOP firewall mechanism)<br>No contradiction to this ST |
| FMT_MSA.1/CMGR | No correspondence | Out of scope (JCOP firewall mechanism)<br>No contradiction to this ST |
| FMT_MSA.2/JCRE | No correspondence | Out of scope (JCOP object handling)<br>No contradiction to this ST |
| FMT_MSA.3/FIREWALL | No correspondence | Out of scope (JCOP firewall mechanism)<br>No contradiction to this ST |
| FMT_MSA.3/CMGR | No correspondence | Out of scope (JCOP firewall mechanism)<br>No contradiction to this ST |
| FMT_MSA.3/SCP | No correspondence | Out of scope (JCOP firewall mechanism)<br>No contradiction to this ST |
| FMT_MTD.1/JCRE | No correspondence | Out of scope (modyfing list of registered applets' AID).<br>No contradiction to this ST |
| FMT_MTD.3 | No correspondence | Out of scope (JCOP LF state handling)<br>No contradiction to this ST |
| FMT_SMF.1 | FMT_SMF.1 | Fullfillment of the platform SFR is used for fulfillment of the SFR of this ST. |
| FMT_SMR.1/JCRE | No correspondence | Out of scope (JCOP specific roles)<br>No contradiction to this ST |
| FMT_SMR.1/CMGR | No correspondence | Out of scope (JCOP specific roles)<br>No contradiction to this ST |
| FPR: Privacy | | |
| FPR_UNO.1 | No correspondence | Out of scope (JCOP package separation)<br>No contradiction to this ST |
| FPT: Protection of the TSF | | |
| FPT_EMSEC.1 | FPT_EMSEC.1 | FPR_EMSEC.1.1 is equivalent, FPT_EMSEC.1.2 is more restricted in this ST. No contradiction. |
| FPT_FLS.1/JCS | FPT_FLS.1 | Internal countermeasures for detecting security violations complement JCOP |

| Relevant Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| | | mechanisms<br>No contradiction to this ST |
| FPT_FLS.1/SCP | FPT_FLS.1 | Internal countermeasures for detecting security violations complement JCOP mechanisms |
| FPT_ITT.1/SCP | No correspondence | Out of scope (platform internal data transfer)<br>No contradiction to this ST |
| FPT_PHP.1 | No correspondence | Out of scope (hardware mechanism)<br>No contradiction to this ST |
| FPT_PHP.3/SCP | FPT_PHP.3 | The SFRs are identical. |
| FPT_RCV.3/SCP | No correspondence | No contradiction to this ST |
| FPT_RCV.4/SCP | No correspondence | No contradiction to this ST |
| FPT_TDC.1 | No correspondence | Refers to LC state before Applet instantiation<br>No contradiction to this ST |
| FPT_TST.1 | FPT_TST.1 | The SFR is equivalent. No contradiction to the ST. |
| FRU: Resource Utilisation | | |
| FRU_FLT.2/SCP | No correspondence | Out of scope (JCOP internal)<br>No contradiction to this ST |
| FTP: Trusted Path/Channels | | |
| FTP_ITC.1/CMGR | No correspondence | Out of scope (JCOP internal)<br>No contradiction to this ST |

*Table 3: Relevant platform SFRs and their correspondence*

### 2.2.3 Assessment of the Platform Objectives

The following table provides an assessment of all relevant Platform objectives.

| Relevant Platform Oberctive | Correspondence in this ST | References/Remarks |
|---|---|---|
| O.PROTECT_DATA | OT.Data_Int, OT.Sens_Data_Conf | |
| O.SIDE_CHANNEL | OT.Prot_Inf_Leak | |
| O.OS_DECEIVE | No correspondence | |
| O.FAULT_PROTECT | OT.Prot_Malfunction | |
| O.PHYSICAL | OT.Prot_Phys-Tamper | |
| O.IDENTIFICATION | OT.Identification | |
| O.RND | No correspondence | Out of scope<br>No contradiction to this ST |
| O.SID | No correspondence | Out of scope |

| Relevant Platform Oberctive | Correspondence in this ST | References/Remarks |
|---|---|---|
| | | No contradiction to this ST |
| O.MF_FW | No correspondence | Out of scope<br>No contradiction to this ST |
| O.OPERATE | No correspondence | Out of scope<br>No contradiction to this ST |
| O.RESOURCES | No correspondence | Out of scope<br>No contradiction to this ST |
| O.FIREWALL | No correspondence | Out of scope<br>No contradiction to this ST |
| O.REALLOCATION | No correspondence | Out of scope<br>No contradiction to this ST |
| O.SHRD_VAR_CONFID | No correspondence | Out of scope<br>No contradiction to this ST |
| O.SHRD_VAR_INTEG | No correspondence | Out of scope<br>No contradiction to this ST |
| O.ALARM | No correspondence | Out of scope<br>No contradiction to this ST |
| O.TRANSACTION | No correspondence | Out of scope<br>No contradiction to this ST |
| O.CIPHER | No correspondence | Out of scope<br>No contradiction to this ST |
| O.PIN-MNGT | No correspondence | Out of scope<br>No contradiction to this ST |
| O.KEY-MNGT | No correspondence | Out of scope<br>No contradiction to this ST |
| O.CARD-MANAGEMENT | No correspondence | Out of scope<br>No contradiction to this ST |
| O.SCP.RECOVERY | No correspondence | Out of scope<br>No contradiction to this ST |
| O.SCP.SUPPORT | No correspondence | Out of scope<br>No contradiction to this ST |
| O.SCP.IC | No correspondence | Out of scope<br>No contradiction to this ST |

Table 4: Relevant platform objectives and their correspondence

### 2.2.4 Assessment of Platform Threats

The following Table 5 provides an assessment of all relevant Platform objectives.

| Relevant Platform Oberctive | Correspondence in this ST | References/Remarks |
|---|---|---|
| T.ACCESS_DATA | T.Read_Sensitive_Data | |
| T.OS_OPERATE | No correspondence | Out of scope<br>No contradiction to this ST |
| T.OS_DECEIVE | No correspondence | Out of scope<br>No contradiction to this ST |
| T.LEAKAGE | T.Information_Leakage | |
| T.FAULT | T.Malfunction | |
| T.RND | No correspondence | Out of scope<br>No contradiction to this ST |
| T.PHYSICAL | T.Phys-Tamper | |
| T.CONFID-JCSCODE | No correspondence | Out of scope<br>No contradiction to this ST |
| T.CONFIDAPPLI-DATA | T.Information_Leakage | |
| T.CONFID-JCSDATA | No correspondence | Out of scope<br>No contradiction to this ST |
| T.INTEG-APPLICODE | No correspondence | Out of scope<br>No contradiction to this ST |
| T.INTEG-JCSCODE | No correspondence | Out of scope<br>No contradiction to this ST |
| T.INTEG-APPLIDATA | T.Forgery | |
| T.INTEG-JCSDATA | No correspondence | Out of scope<br>No contradiction to this ST |
| T.SID.1 | No correspondence | Out of scope<br>No contradiction to this ST |
| T.SID.2 | No correspondence | Out of scope<br>No contradiction to this ST |
| T.EXE-CODE.1 | No correspondence | Out of scope<br>No contradiction to this ST |
| T.EXE-CODE.2 | No correspondence | Out of scope<br>No contradiction to this ST |
| T.RESOURCES | No correspondence | Out of scope<br>No contradiction to this ST |

*Table 5: Relevant platform thretas and their correspondence*

### 2.2.5 Assessment of Platform Organisational Security Policies

The platform ST contains only the Organisational Security Policy “OSP.PROCESS-TOE” referring to accurate identification of each TOE instance. This policy will be fulfilled by a distinct product code for the platform and for the composite TOE each. This policy does not contradict to the policies of this ST.

### 2.2.6 Assessment of Platform Operational Environment

#### 2.2.6.1 Assessment of Platform Assumptions

In the first column, the following table lists all significant assumptions of the Platform ST. The last column provides an explanation of relevance for the Composite TOE.

| Significant Platform Assumption | Relevance for Composite ST |
|---|---|
| A.USE_DIAG | A.USE_DIAG is required in the Platform ST to cover secure communication.<br>There is no corresponding assumption in the Composite ST. Secure communication is enforced by TSF_Access and hence supports this assumption directly. |

*Table 6: Significant assumptions of the platform ST.*

#### 2.2.6.2 Assessment of Platform Security Objectives and SFRs for the Operational Environment

There are no significant Platform Security Objectives and no Platform SFRs for the Operational Environment to be considered.

# 3 Security problem definition

This chapter has been taken from [PP0056] with minor modifications.

## 3.1 Introduction

### 3.1.1 Assets

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

#### 3.1.1.1 Logical MRTD sensitive User Data

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

**PP application note 8:** Due to interoperability reasons the 'ICAO Doc 9303' [ICAODoc] requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG16. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [PP0055]).

#### 3.1.1.2 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.

### 3.1.2 Subjects

This security target considers the following subjects:

#### 3.1.2.1 Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

#### 3.1.2.2 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 of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object.

#### 3.1.2.3 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.

#### 3.1.2.4 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.

#### 3.1.2.5 Terminal

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

#### 3.1.2.6 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.

#### 3.1.2.7 MRTD Holder

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

#### 3.1.2.8 Traveler

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

#### 3.1.2.9 Attacker

A threat agent trying (i) to manipulate the logical MRTD without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or (iii) to forge a genuine MRTD. 57

**PP Application note 9:** 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 security target since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys that is covered by [PP0055]. 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.

**PP Application note 10:** 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.

### 3.2.1 A.MRTD_Manufact MRTD manufacturing on steps 4 to 6

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

### 3.2.2 A.MRTD_Delivery MRTD delivery during steps 4 to 6

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

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

### 3.2.3 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.

### 3.2.4 A.Insp_Sys Inspection Systems for global interoperability

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

### 3.2.5 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.

### 3.2.6 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.

**PP Application note 11:** The threats T.Chip_ID and T.Skimming (cf. [PP0055]) are averted by the mechanisms described in the BAC PP [PP0055] (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.

### 3.3.1 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. [PP0055]) 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. |
| 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. |

### 3.3.2 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 writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD 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. |

### 3.3.3 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 threats as specified below.

### 3.3.4 T.Abuse-Func Abuse of Functionality

| | |
|---|---|
| Adverse action: | An attacker may use functions of the TOE which shall not be used in "Operational Use" phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder. |
| Threat agent: | having high attack potential, being in possession of a legitimate MRTD |
| Asset: | confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF |

### 3.3.5 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 of logical MRTD and TSF data |

### 3.3.6 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) to 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 |

### 3.3.7 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

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 [CC_1], section 3.2).

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

The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the 'ICAO Doc 9303' [ICAODoc] 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' [PP0055] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

**PP Application note 12:** The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [ICAODoc] is addressed by the [PP0055] (cf. P.BAC-PP). The confidentiality of the personal data oth-

er 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. [PP0055]). 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 on the other side are addressed in separated protection profiles and security targets, which results in technically separated evaluations (at least for classes ASE and VAN) and certificates (cf. also PP application note 1).

### 3.4.2 P.Sensitive_Data Privacy of sensitive biometric reference data

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

### 3.4.3 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.

### 3.4.4 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.

### 4.1.1 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 [ICAODoc] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and 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.

**PP Application note 13:** The OT.AC_Pers implies that

(1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,

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

### 4.1.2 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.

### 4.1.3 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.

### 4.1.4 OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile 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).

### 4.1.5 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 [TR-03110]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

**PP application note 14:** 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 [ICAODoc] 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.

### 4.1.6 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.

### 4.1.7 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.

**PP application note 15:** 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.

### 4.1.8 OT.Prot_Phys-Tamper Protection against Physical Tampering

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

### 4.1.9 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.

**PP application note 16:** A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

## 4.2 Security Objectives for the Operational Environment

### 4.2.1 Issuing State or Organization

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

#### 4.2.1.1 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.

#### 4.2.1.2 OE.MRTD_ Delivery Protection of the MRTD delivery

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

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

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

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

#### 4.2.1.3 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.

#### 4.2.1.4 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 to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAODoc].

#### 4.2.1.5 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.

#### 4.2.1.6 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.

#### 4.2.1.7 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' [PP0055]. 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.

### 4.2.2 Receiving State or Organization

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

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

#### 4.2.2.2 OE.Passive_Auth_Verif Verification by Passive Authentication

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

#### 4.2.2.3 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.

**PP application note 17**: The figure 2.1 in [TR03110] 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 lesssensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this ST. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

#### 4.2.2.4 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_Malfuntion | 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 | | | | | | | | | | | | | | | |

| | 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_Malfuntion | 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.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.Personalisation | 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 7: Overview of the 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 the management of TSF to the Personalization Agent.

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

ing appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems”.

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

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

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

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

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

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

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

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

the TOE environment **OE.Prot_Logical_MRTD** “Protection of data from the logical MRTD” require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

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

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

# 5 Extended Components Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [PP0002], other components are defined in the protection profile [PP0056]. This chapter has been taken from [PP0056] with minor modifications.

## 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.

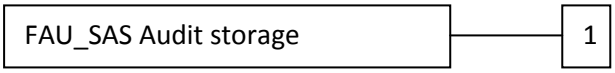
The family “Audit data storage (FAU_SAS)” is specified as follows.

**FAU_SAS Audit data storage**

Family behavior

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

Component leveling




| | |
|---|---|
| FAU_SAS.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 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.

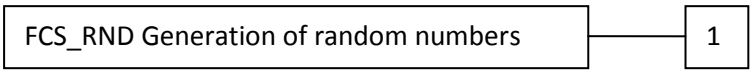
The family “Generation of random numbers (FCS_RND)” is specified as follows.

**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 | The 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.

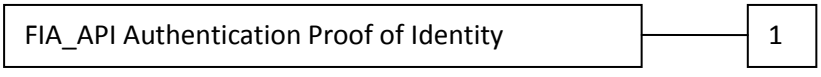
**PP application note 18**: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common 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.

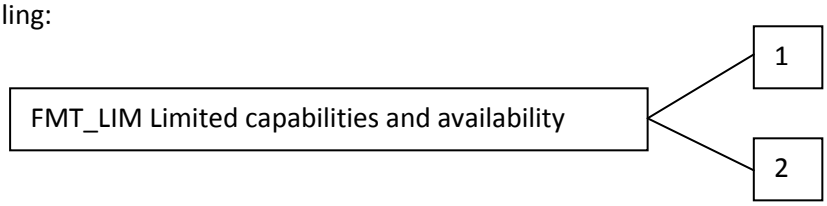
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

**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*]. |

**PP application note 19:** 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

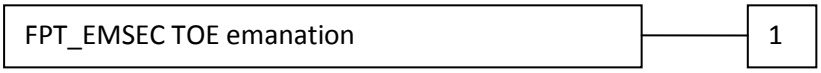
The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena 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 [CC_2].

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:




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<br>There are no management activities foreseen. |
| Audit: | FPT_EMSEC.1<br>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

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 [CC_1] of the CC. Each of these operations is used in this ST and the underlying PP.

Operations already performed in the underlying PP [PP0056] are uniformly marked by ***bold italic*** font style; for further information on details of the operation, please refer to [PP0056].

Operations performed within this Security Target are marked by **bold underlined** font style; further information on details of the operation is provided in foot notes.

## 6.1 Security Definitions

Definition of security attributes:

| Security Attribute | Values | Meaning |
|---|---|---|
| Terminal Authentication Status | none (any Terminal) | default role (i.e. without authorisation after start-up) |
| | CVCA | roles defined in the certificate used for authentication (cf. [TR-03110], A.5.1); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA |
| | DV (domestic) | roles defined in the certificate used for authentication (cf. [TR-03110], A.5.1); Terminal is authenticated as domestic Document Verifier after successful CA and TA |
| | DV (foreign) | roles defined in the certificate used for authentication (cf. [TR-03110], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA and TA |
| | IS | roles defined in the certificate used for authentication (cf. [TR-03110], A.5.1); Terminal is authenticated as Extended Inspection System after successful CA and TA |
| Terminal Authorization | none | |
| | DG4 (Iris) | Read access to DG4: (cf. [TR-03110], A.5.1) |
| | DG3 (Fingerprint) | Read access to DG3: (cf. [TR-03110], A.5.1) |
| | DG3 (Iris) / DG4 (Fingerprint) | Read access to DG3 and DG4: (cf. [TR-03110], A.5.1) |

*Table 8: Definition of security attributes.*

The following table provides an overview of the keys and certificates used:

| Name | Abbreviation | Description |
|---|---|---|
| Country Verifying Certification Authority Private Key | $SK_{CVCA}$ | The Country Verifying Certification Authority (CVCA) holds a private key ($SK_{CVCA}$) used for signing the Document Verifier Certificates. |
| Country Verifying Certification Authority Public Key | $PK_{CVCA}$ | The TOE stores the Country Verifying Certification Authority Public Key ($PK_{CVCA}$) as part of the TSF data to verify the Document Verifier Certificates. The $PK_{CVCA}$ has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of |

| Name | Abbreviation | Description |
|---|---|---|
| | | a domestic Document Verifier Certificate. |
| Country Verifying Certification Authority Certificate | $C_{CVCA}$ | The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [PP0055] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key ($PK_{CVCA}$) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes. |
| Document Verifier Certificate | $C_{DV}$ | The Document Verifier Certificate $C_{DV}$ is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key ($PK_{DV}$) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes. |
| Inspection System Certificate | $C_{IS}$ | The Inspection System Certificate ($C_{IS}$) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key ($PK_{IS}$), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes. |
| Chip Authentication Public Key Pair | | The Chip Authentication Public Key Pair ($SK_{ICC}$, $PK_{ICC}$) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946. |
| Chip Authentication Public Key | $PK_{ICC}$ | The Chip Authentication Public Key ($PK_{ICC}$) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment. |
| Authentication Private Key | $SK_{ICC}$ | The Chip Authentication Private Key ($SK_{ICC}$) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data. |
| Country Signing Certification Authority Key Pair | | Country Signing Certification Authority of the Issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by Receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key. |
| Document Signer Key Pairs | | Document Signer of the Issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the Receiving State or organization with the Document Signer Public Key. |
| Document Basic Access Keys | | The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and the key agreement for secure messaging between |

| Name | Abbreviation | Description |
|---|---|---|
| | | the MRTD's chip and the Inspection System. |
| BAC Session Keys | | Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol. |
| Chip Session Key | | Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol. |

*Table 9: Overview of the keys and certificates.*

**PP application note 20:** The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization.

## 6.2 Security Functional Requirements for the TOE

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

### 6.2.1 Class FAU Security Audit

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

**FAU_SAS.1 Audit storage**

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

**PP Application note 21:** The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

### 6.2.2 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 Diffie-Hellman key derivation Protocol compliant to PKCS#3** with cryptographic key sizes **of 1976 - 2048 bit, or ECDH compliant to ISO 15946[3]** with cryptographic key sizes **of 224 and 256 bit[4]** that meet the following: ***[TR-03110] , Annex A.1***.[5] |

**PP Application note 22:** The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [TR-03110], sec. 3.1 and Annex A.1. The shared secret value is used to derive the AES or Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [ICAODoc], 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**

| | |
|---|---|
| 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 **physically overwriting the keys with zeros[6]** that meets the following: **none[7]**. |

**PP Application note 23:** The TOE shall destroy the BAC Session Keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip Authentication Protocol. The TOE shall destroy the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

### 6.2.2.1 Cryptographic operation (FCS_COP.1)

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

[3] Please also note the remark in the JCOP user guidance manual [JCOP_UGM], section 2.2.1 on EC domain parameters.

[4] [assignment: cryptographic key generation algorithm]

[5] The combination of the two cryptographic algorithms with an „or" is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

[6] [assignment: cryptographic key destruction method]

[7] [assignment: list of standards]

**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<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>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, SHA-224, SHA-256**[8] and cryptographic key sizes (***none***) that meet the following: **FIPS 180-2**[9]. |

**PP application note 24:** <applied>

**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<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/SYM | The TSF shall perform ***secure messaging – encryption and decryption*** in accordance with a specified cryptographic algorithm: **Triple-DES in CBC mode**[10] and cryptographic key size **112 bit**[11] that meets the following: **FIPS 46-3**[12] ***and [TR-03110]***. |

**PP application note 25:** This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol according to the FCS_CKM.1. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

**FCS_COP.1/MAC Cryptographic operation – MAC**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |

[8] [assignment: cryptographic algorithms]

[9] [assignment: list of standards]

[10] [assignment: cryptographic algorithm]

[11] [assignment: cryptographic key sizes]

[12] [assignment: list of standards]

FCS_COP.1.1/MAC The TSF shall ***perform secure messaging – message authentication code*** in accordance with a specified cryptographic algorithm: **Retail MAC**[13] and cryptographic key size **112 bit**[14] that meets the following: ***[TR-03110]***.

**PP application note 26:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol according to the FCS_CKM.1. The Retail-MAC as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 (cf. [PP0055]) is DES resp. two-key Triple-DES base.

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/SIG_VER | The TSF shall perform ***digital signature verification*** in accordance with a specified cryptographic algorithm: **RSA**[15] and cryptographic key sizes **of 1976 - 2048 bit**[16] that meet the following: **RSASSA-PKCS#1-v1_5**[17], or **ECDSA**[12] [18] and cryptographic key sizes **of 224 and 256 bit**[13] that meet the following: **ISO15946**[14]**.**[19] |

**PP application note 27:** <applied>

### 6.2.2.2 Random Number Generation (FCS_RND.1)

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

**FCS_RND.1 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 **the AIS20 Class K3 quality metric**[20]**.** |

[13] [assignment: cryptographic algorithm]

[14] [assignment: cryptographic key sizes]

[15] [assignment: cryptographic algorithm]

[16] [assignment: cryptographic key sizes]

[17] [assignment: list of standards]

[18] Please also note the remark in the JCOP user guidance manual [JCOP_UGM], section 2.2.1 on EC domain parameters.

[19] The combination of the two cryptographic algorithms with an „or" is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

[20] [assignment: a defined quality metric]

**PP application note 28:** This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

### 6.2.3 Class FIA Identification and Authentication

**PP application note 29:** The following Table 10 gives 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<br>FIA_UAU.5<br>FIA_UAU.6 |
| Terminal Authentication Protocol | FIA_UAU.5 |

*Table 10: Overview on authentication SFR*

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

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

The BAC mechanism does not provide a security function on its 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<br>1. ***to establish the communication channel***,<br>2. ***to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS***<br>3. ***to carry out the Chip Authentication Protocol*** 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. |

**PP application note 30:** In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the Document Basic Access Keys, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Basic Inspection System (cf. PP MRTD BAC [PP0055]) is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to run the BAC Authentication Protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol (i.e. the BAC mechanism is not seen as an independent mechanism in this security target, it is a mandatory part within the Chip Authentication Protocol, and thus noted here for reasons of completeness). After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or (ii) if necessary and available by symmetric authentication as Personalization Agent (using the Personalization Agent Key).

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<br>1. ***to establish the communication channel***,<br>2. ***to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS***,<br>3. ***to identify themselves by selection of the authentication key***<br>4. ***to carry out the Chip Authentication Protocol***<br>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<br>1. ***Terminal Authentication Protocol***,<br>2. ***Authentication Mechanism based on*** **Triple-DES**[21] |

[21] [assignment: identified authentication algorithms]

**PP application note 31:** The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

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<br>1. ***Terminal Authentication Protocol***,<br>2. ***Secure messaging in MAC-ENC mode***,<br>3. ***Symmetric Authentication Mechanism based on*** **Triple-DES**[22]<br>to support user authentication. |
| FIA_UAU.5.2 | The TSF shall authenticate any user's claimed identity according to the ***following rules***:<br>***1. The TOE accepts the authentication attempt as Personalization Agent by*** **the Symmetric Authentication Mechanism with Personalization Agent Key**[23]***.***<br>***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.***<br>***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.*** |

**PP application note 32:** Depending on the authentication methods used the Personalization Agent holds (i) a key for the Symmetric Authentication Mechanism or (ii) an asymmetric key pair for the Terminal Authentication Protocol (e.g. provided by the Extended Access Control PKI in a valid card verifiable certificate with appropriate encoded access rights). The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

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

[22] [assignment: identified authentication algorithms]

[23] [selection: the Symmetric Authentication Mechanism with Personalization Agent Key]

**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***. |

**PP application note 33:** The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [ICAODoc] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on CMAC, Retail-MAC or EMAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE reauthenticates the user for each received command and accepts only those commands received from the previously authenticated user.

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

**FIA_API.1 Authentication Proof of Identity**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_API.1.1 | The TSF shall provide a ***Chip Authentication Protocol according to [TR-03110]*** to prove the identity of the ***TOE***. |

**PP application note 34:** This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [TR03110]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAODoc], normative appendix 5, A5.1. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

### 6.2.4 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*** 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***. |

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<br>FMT_MSA.3 Static attribute initialization |
| FDP_ACF.1.1 | The TSF shall enforce the ***Access Control SFP*** to objects based on the following:<br>***1. Subjects:***<br>***a. Personalization Agent,***<br>***b. Extended Inspection System***<br>***c. Terminal,***<br>***2. Objects:***<br>***a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,***<br>***b. data EF.DG3 and EF.DG4 of the logical MRTD***<br>***c. data in EF.COM,***<br>***d. data in EF.SOD,***<br>***3. Security attributes:***<br>***a. authentication status of terminals,***<br>***b. Terminal Authorization.*** |
| FDP_ACF.1.2 | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:<br>***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,***<br>***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.***<br>***3. the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD.*** |
| FDP_ACF.1.3 | The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***none***. |
| FDP_ACF.1.4 | The TSF shall explicitly deny access of subjects to objects based on the ***rule***:<br>***1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,***<br>***2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,***<br>***3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,***<br>***4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,***<br>***5. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,***<br>***6. Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD.*** |

**PP application note 35:** The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [TR03110], Annex A.5.1, table A.8. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

**PP application note 36:** Note that the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG16 of the logical MRTD. According to P.BAC-PP these security features of the MRTD are not subject of this security target.

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**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FTP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path]<br>[FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control] |
| FDP_UCT.1.1 | The TSF shall enforce the ***Access Control SFP*** to be able to ***transmit and receive*** user data in a manner protected from unauthorized disclosure ***after Chip Authentication***. |

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

**FDP_UIT.1 Data exchange integrity**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>[FTP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path] |
| FDP_UIT.1.1 | The TSF shall enforce the ***Access Control SFP*** to be able to ***transmit and receive*** user data in a manner protected from ***modification, deletion, insertion and replay*** errors ***after Chip Authentication***. |
| FDP_UIT.1.2 | The TSF shall be able to determine on receipt of user data, whether ***modification, deletion, insertion and replay*** has occurred ***after Chip Authentication***. |

**Rationale for Refinement in the PP:** Note that the Access Control SFP (cf. FDP_ACF.1.2) allows the Extended Inspection System (as of [ICAODoc] and [PP0055]) to access the data EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD. Nevertheless there is explicitly no rule for preventing access to these data. More over their data integrity (cf. FDP_UIT.1) and confidentiality (cf. FDP_UCT.1) is ensured by the BAC mechanism being addressed and covered by [PP0055]. The fact that the BAC mechanism is not part of the security target in hand is addressed by the refinement "after Chip Authentication".

**PP application note 37:** FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication to the General Inspection System. The authentication mechanism as part of Basic Access Control Mechanism and the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

### 6.2.5 Class FMT Security Management

**PP application note 38:** 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:<br>***1. Initialization ,***<br>***2. Pre-personalization ,***<br>***3. Personalization.*** |

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

**FMT_SMR.1 Security roles**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification. |
| FMT_SMR.1.1 | The TSF shall maintain the roles<br>***1. Manufacturer ,***<br>***2. Personalization Agent ,***<br>***3. Country Verifying Certification Authority,***<br>***4. Document Verifier,***<br>***5. domestic Extended Inspection System***<br>***6. foreign Extended Inspection System.*** |
| FMT_SMR.1.2 | The TSF shall be able to associate users with roles. |

**PP application note 39**: Note that the MRTD also maintains the role Basic Inspection System due to a direct consequence of P.BAC-PP resp. OE.BAC-PP. Nevertheless this role is not explicitly listed in FMT_SMR.1.1, above since the TSF cannot maintain the role with respect to the assumed high attack potential due to the known weaknesses of the Document Basic Access Keys.

**PP application note 40**: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

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

**FMT_LIM.1 Limited capabilities**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.2 Limited availability. |
| FMT_LIM.1.1 | The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced:<br>***Deploying Test Features after TOE Delivery does not allow,***<br>***1. User Data to be manipulated,***<br>***2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,***<br>***3. TSF data to be disclosed or manipulated***<br>***4. software to be reconstructed and***<br>***5. substantial information about construction of TSF to be gathered which may enable other attacks*** |

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

**FMT_LIM.2 Limited availability**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.1 Limited capabilities. |
| FMT_LIM.2.1 | The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced:<br>***Deploying Test Features after TOE Delivery does not allow***<br>***1. User Data to be manipulated,***<br>***2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,***<br>***3. TSF data to be disclosed or manipulated***<br>***4. software to be reconstructed and***<br>***5. substantial information about construction of TSF to be gathered which may enable other attacks.*** |

**PP application note 41:** The formulation of “Deploying Test Features …” in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term “software” in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

**PP application note 42:** The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

The TOE shall meet the requirement “Management of TSF data (FMT_MTD.1)” as specified below (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 Prepersonalization 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 ***the Initialization Data and Prepersonalization Data*** to ***the Manufacturer***. |

**PP application note 43:** The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

**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*** the ***Initialization Data*** to ***the Personalization Agent***. |

**PP application note 44:** According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Prepersonalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMF.1 Specification of management functions |
| | FMT_SMR.1 Security roles |
| FMT_MTD.1.1/CVCA_INI | The TSF shall restrict the ability to write the<br>***1. initial Country Verifying Certification Authority Public Key,***<br>***2. initial Country Verifying Certification Authority Certificate,***<br>***3. initial Current Date***<br>to **the Personalization Agent**[24]**.** |

[24] [assignment: the authorized identified roles]

**PP application note 45:** <applied>

**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*** the |
| | ***1. Country Verifying Certification Authority Public Key,*** |
| | ***2. Country Verifying Certification Authority Certificate*** |
| | to ***Country Verifying Certification Authority.*** |

**PP application note 46:** The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [TR03110], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [TR03110], sec. 2.2.3 and 2.2.4).

**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*** the ***Current date*** to |
| | ***1. Country Verifying Certification Authority,*** |
| | ***2. Document Verifier,*** |
| | ***3. Domestic Extended Inspection System.*** |

**PP application note 47**: The authorized roles are identified in their certificate (cf. [TR03110], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [TR03110], annex A.3.3, for details).

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMF.1 Specification of management functions |
| | FMT_SMR.1 Security roles |
| FMT_MTD.1.1/KEY_WRITE | The TSF shall restrict the ability to ***write*** the ***Document Basic Access Keys*** to ***the Personalization Agent***. |

**PP application note 48:** The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMF.1 Specification of management functions |
| | FMT_SMR.1 Security roles |
| FMT_MTD.1.1/CAPK | The TSF shall restrict the ability to **load**[25] the ***Chip Authentication Private Key*** to **the Personalization Agent**[26]**.** |

**PP application note 49:** <applied>

**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 the |
| | ***1. Document Basic Access Keys,*** |
| | ***2. Chip Authentication Private Key,*** |
| | ***3. Personalization Agent Keys*** |
| | to: ***none***. |

The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below (Common Criteria Part 2):

**FMT_MTD.3 Secure TSF data**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_MTD.1 Management of TSF data |
| FMT_MTD.3.1 | The TSF shall ensure that only secure values **of the certificate chain** are accepted for ***TSF data of the Terminal Authentication Protocol and the Access Control***. |

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

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

[25] [selection: create, load]

[26] [assignment: the authorised identified roles]

**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.**

**PP application note 50:** The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.

### 6.2.6 Class FPT Protection of the Security Functions

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

The TOE shall meet the requirement "TOE Emanation (FPT_EMSEC.1)" as specified below (Common Criteria Part 2 extended):

**FPT_EMSEC.1 TOE Emanation**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No Dependencies. |
| FPT_EMSEC.1.1 | The TOE shall not emit **variations in power consumption or timing during command execution**[27] in excess of **non-useful information**[28] enabling access to ***Personalization Agent Keys and Chip Authentication Private Key***[29]***and*** **none**[30]. |
| FPT_EMSEC.1.2 | The TSF shall ensure ***any users*** are unable to use the following interface: **smart card circuit contacts or contactless interface**[31] to gain access ***to Personalization Agent Key(s) and Chip Authentication Private Key***[32] ***and*** **none**[33]. |

**PP application note 51:** <applied>

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

[27] [assignment: types of emissions]

[28] [assignment: specified limits]

[29] [assignment: list of types of user data]

[30] [assignment: list oftypes of user data].

[31] [assignment: type of connection]

[32] [assignment: list of types of TSF data]

[33] [assignment: list oftypes of user data].

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:<br>***1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,***<br>***2. Failure detected by TSF according to FPT_TST.1.*** |

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

**FPT_TST.1 TSF testing**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No Dependencies. |
| FPT_TST.1.1 | The TSF shall run a suite of self tests **during initial start-up**[34] to demonstrate the correct operation of ***the TSF***. |
| FPT_TST.1.2 | The TSF shall provide authorised users with the capability to verify the integrity of ***TSF data***. |
| FPT_TST.1.3 | The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. |

**PP application note 52:** <applied>

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 to the TSF*** by responding automatically such that the SFRs are always enforced. |

**PP application note 53:** The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response"

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

means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

**PP application note 54**: The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

## 6.3 Security Assurance Requirements for the TOE

The requirements 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**.

**PP application note 55:** The TOE shall protect the assets against high attack potential under the assumption that the inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol (OE.Prot_Logical_MRTD). Otherwise the confidentiality of the standard data shall be protected against attacker with at least Enhanced-Basic attack potential (AVA_VAN.3).

## 6.4 Security Requirements Rationale

### 6.4.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements 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_Malfuntion |
|---|---|---|---|---|---|---|---|---|---|
| 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 | | | | | | |

| | 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_Malfuntion |
|---|---|---|---|---|---|---|---|---|---|
| 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 11: Overview of the security functional requirements coverage.*

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

handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control.

The 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 [TR-03110] 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.

### 6.4.2 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 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 | Fulfilled by FCS_COP.1/SYM, and |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| | FCS_COP.1 Cryptographic operation],<br>FCS_CKM.4 Cryptographic key destruction | FCS_COP.1/MAC,<br><br>Fulfilled by FCS_CKM.4 |
| FCS_CKM.4 | [FDP_ITC.1 Import of user data without security attributes,<br>FDP_ITC.2 Import of user data with security attributes, or<br>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,<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | justification 1 for non-satisfied dependencies<br><br>Fulfilled by FCS_CKM.4 |
| FCS_COP.1/SYM | [FDP_ITC.1 Import of user data without security attributes,<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | Fulfilled by FCS_CKM.1,<br><br>Fulfilled by FCS_CKM.4 |
| FCS_COP.1/MAC | [FDP_ITC.1 Import of user data without security attributes,<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | Fulfilled by FCS_CKM.1<br><br>Fulfilled by FCS_CKM.4 |
| FCS_COP.1/SIG_VER | [FDP_ITC.1 Import of user data without security attributes,<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation],<br>FCS_CKM.4 Cryptographic key destruction | Fulfilled by FCS_CKM.1,<br><br>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 identfication | 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. |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FIA_API.1 | No dependencies | n.a. |
| FDP_ACC.1 | FDP_ACF.1 Security attribute based access control | Fulfilled by FDP_ACF.1 |
| FDP_ACF.1 | FDP_ACC.1 Subset access control,<br>FMT_MSA.3 Static attribute initialization | Fulfilled by FDP_ACC.1,<br>justification 2 for non-satisfied dependencies |
| FDP_UCT.1 | [FTP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path],<br>[FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control] | justification 3 for non-satisfied dependencies<br>Fulfilled by FDP_ACC.1 |
| FDP_UIT.1 | [FTP_ITC.1 Inter-TSF trusted channel, or<br>FTP_TRP.1 Trusted path],<br>[FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control] | justification 3 for non-satisfied dependencies<br>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,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/INI_DIS | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/CVCA_INI | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/CVCA_UPD | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/DATE | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/KEY_WRITE | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/CAPK | FMT_SMF.1 Specification of management functions, | Fulfilled by FMT_SMF.1 |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| | FMT_SMR.1 Security roles | Fulfilled by FMT_SMR.1 |
| FMT_MTD.1/KEY_READ | FMT_SMF.1 Specification of management functions,<br>FMT_SMR.1 Security roles | Fulfilled by FMT_SMF.1<br>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_TST.1 | No dependencies | n.a. |
| FPT_FLS.1 | No dependencies | n.a. |
| FPT_PHP.3 | No dependencies | n.a. |

*Table 12: Overview of the dependencies between the SFR of 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 a key generation (FCS_CKM.1) nor an 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 attribute (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 secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

### 6.4.3 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
- AGD_PRE.1 Preparative procedures

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

### 6.4.4 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 (ASE_TSS)

## 7.1 Security Functionality

### 7.1.1 TSF_Access: Access rights

This security functionality manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data. Access control for initialization and pre-personalization in Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying JCOP Java Card platform (SF.AccessControl, SF.I&A).

Access is granted (or denied) in accordance to access rights that depend on appropriate identification and authentication mechanisms.

TSF_Access covers the following SFRs:

- FIA_UID.1.1 requires that the TSF shall allow to establish the communication channel, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, and to carry out the Chip Authentication Protocol on behalf of the user to be performed before the user is identified. FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.1.1 requires that the TSF shall allow to establish the communication channel, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to identify themselves by selection of the authentication key, and to carry out the Chip Authentication Protocol on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.4 requires that the TSF shall prevent reuse of authentication data related to Terminal Authentication Protocol, and the Authentication Mechanism based on Triple-DES. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.5.1 requires that the TSF shall provide Terminal Authentication Protocol, Secure messaging in MAC-ENC mode, and Symmetric Authentication Mechanism based on Triple-DES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user's claimed identity according to specified rules. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.6 requires that the TSF shall re-authenticate the user under the condition that each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS. TSF_Access realizes the appropriate control of the access rights.
- FDP_ACC.1 requires that the TSF shall enforce the Access Control SFP 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. TSF_Access realizes the appropriate control of the access rights.
- FDP_ACF.1: FDP_ACF.1.1 requires that the TSF shall enforce the Access Control SFP to objects based on subjects (Personalization Agent, Extended Inspection System, Terminal), objects (data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, data EF.DG3 and EF.DG4 of the logical MRTD, data in EF.COM, data in EF.SOD), and security attributes (authentication status of terminals, Terminal Authorization). FDP_ACF.1.2 requires that 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, and (3.) the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD. FDP_ACF.1.3 requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. FDP_ACF.1.4 requires that he TSF shall explicitly deny access of subjects to objects based on the rules: (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 any of the EF.DG3 to EF.DG4 of the logical MRTD. TSF_Access realizes the appropriate control of the access rights.

- FDP_UCT.1: FDP_UCT.1.1 requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure after Chip Authentication. TSF_Access realizes the appropriate control of the access rights.
- FDP_UIT.1: FDP_UIT.1.1 requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication. FDP_UIT.1.2 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred after Chip Authentication. TSF_Access realizes the appropriate control of the access rights.
- FMT_SMR.1: FMT_SMR.1.1 requires that the TSF shall maintain the roles (1.) Manufacturer , (2.) Personalization Agent , (3.) Country Verifying Certification Authority, (4.) Document Verifier, (5.) domestic Extended Inspection System, and (6.) foreign Extended Inspection System. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. TSF_Access realizes the appropriate control of the access rights.
- FMT_LIM.1 requires that 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. This is realized by TSF_Access.
- FMT_LIM.2 requires that 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. This is realized by TSF_Access.
- FMT_MTD.1.1/CVCA_INI requires that the TSF shall restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Date to the Personalization Agent. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/CVCA_UPD requires that the TSF shall restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority. TSF_Access realizes the appropriate control of the access rights.

- FMT_MTD.1.1/DATE requires that the TSF shall restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/CAPK requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the (1.) Document Basic Access Keys, the (2.) Chip Authentication Private Key, and the (3.) Personalization Agent Keys to none. TSF_Access realizes the appropriate control of the access rights.

### 7.1.2 TSF_Admin: Administration

This Security Functionality manages the storage of manufacturing data, pre-personalization data and personalization data. This storage area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Management of manufacturing and pre-personalization data in Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying JCOP Java Card platform (SF.SecureManagement); also Audit functionality is based on JCOP functionality (SF.Audit). During Operational Use phase, read access is only possible after successful authentication.

TSF_Admin covers the following SFRs:

- FAU_SAS.1: FAU_SAS.1 requires that the TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records. This is realized by TSF.Admin.
- FMT_SMF.1: FMT_SMF.1.1 requires that the TSF shall be capable of performing the following management functions: (1.) Initialization , (2.) Pre-personalization , (3.) Personalization. This is realized within TSF_Admin.
- FMT_SMR.1: FMT_SMR.1.1 requires that the TSF shall maintain the roles (1.) Manufacturer , (2.) Personalization Agent , (3.) Country Verifying Certification Authority, (4.) Document Verifier, (5.) domestic Extended Inspection System, and (6.) foreign Extended Inspection System. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. This is realized within TSF_Admin.
- FMT_LIM.1 requires that 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. This is realized by TSF_Admin.
- FMT_LIM.2 requires that 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. This is realized by TSF_Admin.
- FMT_MTD.1.1/CVCA_INI requires that the TSF shall restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Date to the Personalization Agent. This is realized within TSF_Admin.

- FMT_MTD.1.1/CVCA_UPD requires that the TSF shall restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority. This is realized within TSF_Admin.
- FMT_MTD.1.1/DATE requires that the TSF shall restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System. This is realized within TSF_Admin.
- FMT_MTD.1.1/CAPK requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. This is realized within TSF_Admin.
- FMT_MTD.1/KEY_WRITE: FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent. This is realized within TSF_Admin.

### 7.1.3 TSF_Secret: Secret key management

This Security Functionality ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These functions make use of SF.CryptoKey of the underlying JCOP Java Card OS.

TSF_Secret covers the following SFRs:

- FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent. This is realized within TSF_Secret.
- FMT_MTD.1.1/CAPK requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. This is realized by TSF_Admin, TSF_Access and TSF_OS. This is realized within TSF_Secret.
- FMT_MTD.1/KEY_READ: FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the (1.) Document Basic Access Keys, the (2.) Chip Authentication Private Key, and the (3.) Personalization Agent Keys to none. This is realized within TSF_Secret.

### 7.1.4 TSF_Crypto: Cryptographic operations

This Security Functionality performs high level cryptographic operations. The implementation is based on the Security Functionalities provided by TSF_OS.

TSF_Crypto covers the following SFRs:

- FCS_CKM.1: FCS_CKM.1.1 requires that the TSF shall generate cryptographic keys based on the Diffie-Hellman key derivation Protocol compliant to PKCS#3 with cryptographic key sizes of 1976 - 2048 bit, and ECDH compliant to ISO 15946 with cryptographic key sizes of 224 and 256 bit, meeting [TR-03110], Annex A.1. This is realized within TSF_Crypto (Diffie-Hellman) and TSF_OS (ECDH).
- FCS_CKM.4: FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys with zeros by method (e.g. clearKey of [Java_RES]) or automatically on applet deselection. This is realized in the security functionalities provided by TSF_OS and TSF_Secret. The only exceptions are the CMAC Sub-Keys (for Secure Messaging), where the security functionality is provided by TSF_Crypto.
- FCS_COP.1.1/MAC requires that the TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm: retail MAC and cryptographic key size 112 bit that meets the following: TR-03110. This is realized within TSF_Crypto.
- FCS_COP.1/SIG_VER requires that the TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm: RSA and cryptographic key sizes of 1976 - 2048 bit that meet the following: RSASSA-PKCS#1-v1_5, and ECDSA and cryptographic key sizes of 224 and 256 bit that meet the following: ISO15946. This is realized within TSF_Crypto (and TSF_OS).

- FIA_UAU.5.1 requires that the TSF shall provide Terminal Authentication Protocol, Secure messaging in MAC-ENC mode, and Symmetric Authentication Mechanism based on Triple-DES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user's claimed identity according to specified rules. TSF_Crypto adds parts of the cryptographic implementation.

### 7.1.5 TSF_ SecureMessaging: Secure Messaging

This Security Functionality realizes a secure communication channel after successful authentication for personalization and BAC during operational use.

TSF_SecureMessaging covers the following SFRs:

- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide Terminal Authentication Protocol, Secure messaging in MAC-ENC mode, and Symmetric Authentication Mechanism based on Triple-DES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user's claimed identity according to specified rules. TSF_SecureMessaging provides the secure messaging mechanism.
- FDP_UIT.1: FDP_UIT.1.1 requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication. FDP_UIT.1.2 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred after Chip Authentication. TSF_SecureMessaging provides the protected communication.

### 7.1.6 TSF_Auth: Authentication protocols

This security functionality realizes different authentication mechanisms.

#### 7.1.6.1 TSF_Auth_Term

TSF_Auth_Term performs the Terminal Authentication to authenticate the terminal (EAC). TSF_Auth_Term covers the following SFRs:

- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide Terminal Authentication Protocol, Secure messaging in MAC-ENC mode, and Symmetric Authentication Mechanism based on Triple-DES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user's claimed identity according to specified rules. The authentication mechanisms are provided by TSF_Auth_Term.
- FDP_ACC.1 requires that the TSF shall enforce the Access Control SFP 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. The authentication mechanism is provided by TSF_Auth_Term.
- FDP_ACF.1: FDP_ACF.1.1 requires that the TSF shall enforce the Access Control SFP to objects based on subjects (Personalization Agent, Extended Inspection System, Terminal), objects (data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, data EF.DG3 and EF.DG4 of the logical MRTD, data in EF.COM, data in EF.SOD), and security attributes (authentication status of terminals, Terminal Authorization). FDP_ACF.1.2 requires that 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, and (3.) the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD. FDP_ACF.1.3 requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none. FDP_ACF.1.4 re-

quires that he TSF shall explicitly deny access of subjects to objects based on the rules: (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 any of the EF.DG3 to EF.DG4 of the logical MRTD. The authentication mechanism for the Access Control SFP is provided by TSF_Auth_Term.

- FMT_MTD.3.1 requires that the TSF shall ensure that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control. This is realized by TSF_Auth_Term. The refinement to FMT_MTD.3.1 requires that the certificate chain is valid if and only if

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

  In addition, the refinement to FMT_MTD.3.1 requires that

  - 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.

  This is realized by TSF_Auth_Term.

#### 7.1.6.2 TSF_Auth_3DES

TSF_Auth_3DES performs an authentication mechanism based on TDES used for BAC and symmetric authentication based on pre-shared keys used for personalization. TSF_Auth_3DES covers the following SFRs:

- FDP_ACF.1: FDP_ACF.1.1 requires that the TSF shall enforce the Access Control SFP to objects based on subjects (Personalization Agent, Extended Inspection System, Terminal), objects (data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, data EF.DG3 and EF.DG4 of the logical MRTD, data in EF.COM, data in EF.SOD), and security attributes (authentication status of terminals, Terminal Authorization). FDP_ACF.1.2 requires that 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, and (3.) the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD. FDP_ACF.1.3 requires that the TSF shall explicitly author-

ize access of subjects to objects based on the following additional rules: none. FDP_ACF.1.4 requires that he TSF shall explicitly deny access of subjects to objects based on the rules: (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 any of the EF.DG3 to EF.DG4 of the logical MRTD. The authentication mechanism for the Access Control SFP is provided by TSF_Auth_3DES.

- FMT_MTD.1.1/CVCA_INI requires that the TSF shall restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Date to the Personalization Agent. The authentication mechanism is provided by TSF_Auth_3DES.
- FMT_MTD.1.1/CVCA_UPD requires that the TSF shall restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority. The authentication mechanism is provided by TSF_Auth_3DES.
- FMT_MTD.1.1/DATE requires that the TSF shall restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System. The authentication mechanism is provided by TSF_Auth_3DES.
- FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent. The authentication mechanism is provided by TSF_Auth_3DES.
- FMT_MTD.1.1/CAPK requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. The authentication mechanism is provided by TSF_Auth_3DES.

#### 7.1.6.3 TSF_Auth_Chip

This security functionality manages the capability of the TOE to authenticate itself to the terminal using the Chip Authentication Protocol (EAC). TSF_Auth_Chip covers the following SFRs:

- FIA_UID.1: FIA_UID.1.1 requires that the TSF shall allow to establish the communication channel, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, and to carry out the Chip Authentication Protocol on behalf of the user to be performed before the user is identified. FIA_UID.1.2 requires that the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. The authentication mechanism leads to the identification and is provided by TSF_Auth_Chip.
- FIA_UAU.1: FIA_UAU.1.1 requires that the TSF shall allow to establish the communication channel, to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, to identify themselves by selection of the authentication key, and to carry out the Chip Authentication Protocol on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. The authentication mechanism is provided by TSF_Auth_Chip.
- FIA_UAU.6: requires that the TSF shall re-authenticate the user under the condition that each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS. The authentication mechanism is provided by TSF_Auth_Chip.
- FIA_API.1.1 requires that the TSF shall provide a Chip Authentication Protocol according to [TR-03110] to prove the identity of the TOE. This is provided by TSF_Auth_Chip.

- FDP_UCT.1: FDP_UCT.1.1 requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure after Chip Authentication. The authentication mechanism is provided by TSF_Auth_Chip.
- FDP_UIT.1: FDP_UIT.1.1 requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication. FDP_UIT.1.2 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred after Chip Authentication. The authentication mechanism for the Access Control SFP is provided by TSF_Auth_Chip.

### 7.1.7 TSF_Integrity: Integrity protection

This Security Functionality protects the integrity of internal applet data like the Access control lists. This function makes use of SF.SecureManagement and SF.Transaction of the underlying JCOP Java Card OS (cf. the according security targets [ST_JCOP080], [ST_JCOP040], [ST_JCOP081]).

TSF_Integrity covers the following SFRs:

- FPT_FLS.1: FPT_FLS.1.1 requires that 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, and (2) failure detected by TSF according to FPT_TST.1. This is realized within TSF_Integrity.

### 7.1.8 TSF_OS: Javacard OS Security Functionalities

The Javacard operation system (part of the TOE) features the following Security Functionalities. The exact description can be found in the Javacard OS security targets [ST_JCOP080], [ST_JCOP040], [ST_JCOP081]; the realization is partly based on the security functionalities of the certified cryptographic library and the certified IC platform:

- Enforcement of access control (SF.AccessControl)
- Audit functionality (SF.Audit)
- Cryptographic key management (SF.CryptoKey)
- Cryptographic operations (SF.CryptoOperation)
- Identification and authentication (SF.I&A)
- Secure management of TOE resources (SF.SecureManagement)
- Transaction management (SF.Transaction)

Since the applet layer of the TOE is based on the Javacard OS, the realization of all TOE security functionalities and thus the fulfillment of all SFRs has dependencies to TSF_OS. The following items list all SFRs where TSF_OS has an impact above this level:

- FCS_CKM.1: FCS_CKM.1.1 requires that the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes. This is realized within TSF_OS.
- FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method. This is realized in the security functionality provided by TSF_OS. The only exceptions are the CMAC Sub-Keys (for Secure Messaging), where the security functionality is provided by TSF_Crypto.
- FCS_COP.1.1/SHA: FCS_COP.1.1/SHA requires that the TSF shall perform hashing in accordance with a specified cryptographic algorithm. This is realized within TSF_OS.

- FCS_COP.1.1/SYM requires that the TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm: Triple-DES in CBC mode and cryptographic key size 112 bit that meets the following: FIPS 46-3 and TR-03110. This is realized within TSF_OS.
- FCS_COP.1.1/MAC requires that the TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm: retail MAC and cryptographic key size 112 bit that meets the following: TR-03110. This is realized within TSF_OS.
- FCS_COP.1.1/SIG_VER requires that the TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm: RSA and cryptographic key sizes of 1976 - 2048 bit that meet the following: RSASSA-PKCS#1-v1_5, and ECDSA and cryptographic key sizes of 224 and 256 bit that meet the following: ISO15946. This is realized within TSF_Crypto and TSF_OS
- FCS_RND.1: FCS_RND.1.1 requires that the TSF shall provide a mechanism to generate random numbers that meet the AIS 20 Class K3 quality metric. This is realized within TSF_OS.
- FMT_LIM.1 requires that 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. This is realized by TSF_OS.
- FMT_LIM.2 requires that 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. This is realized by TSF_OS.
- FMT_MTD.1.1/INI_ENA requires that the TSF shall restrict the ability to write the Initialization Data and Prepersonalization Data to the Manufacturer. This is realized by TSF_OS.
- FMT_MTD.1.1/INI_DIS requires that the TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent. This is realized by TSF_OS.
- FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the (1.) Document Basic Access Keys, the (2.) Chip Authentication Private Key, and the (3.) Personalization Agent Keys to none. This is realized by TSF_OS.
- FPT_EMSEC.1: FPT_EMSEC.1.1 requires that the TOE shall not emit variations in power consumption or timing during command execution in excess of non-useful information enabling access to Personalization Agent Keys and Chip Authentication Private Key. FPT_EMSEC.1.2 requires that the TSF shall ensure any users are unable to use the following interface: smart card circuit contacts or contactless interface to gain access to Personalization Agent Key(s) and Chip Authentication Private Key. This is mainly realized by appropriate measures in TSF_OS together with the strict following of the security implementation guidelines of the Javacard platform.
- FPT_FLS.1.1 requires that 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, and (2) failure detected by TSF according to FPT_TST.1. This is realized within TSF_OS (together with TSF_Integrity).
- FPT_TST.1.1 requires that the TSF shall run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF. FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data. FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.

- FPT_PHP.3.1 requires that the TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.

## 7.2 TOE summary specification rationale

This summary specification shows that the TSF and assurance measures are appropriate to fulfill the TOE security requirements.

Each TOE security functional requirement is implemented by at least one security functionality. The mapping of TOE Security Requirements and TOE Security Functionalities is given in the following table. If iterations of a TOE security requirement are covered by the same TOE security functionality the mapping will appear only once. The description of the TSF is given in section 7.1.

| | TSF_Access | TSF_Admin | TSF_Secret | TSF_Crypto | TSF_SecureMessaging | TSF_Auth | TSF_Integrity | TSF_OS |
|---|---|---|---|---|---|---|---|---|
| FAU_SAS.1 | | x | | | | | | |
| FCS_CKM.1 | | | | x | | | | x |
| FCS_CKM.4 | | | | x | | | | x |
| FCS_COP.1/SHA | | | | | | | | x |
| FCS_COP.1/SYM | | | | | | | | x |
| FCS_COP.1/MAC | | | | x | | | | x |
| FCS_COP.1/SIG_VER | | | | x | | | | x |
| FCS_RND.1 | | | | | | | | x |
| FIA_UID.1 | x | | | | | x | | |
| FIA_UAU.1 | x | | | | | x | | |
| FIA_UAU.4 | x | | | | | x | | |
| FIA_UAU.5 | x | | | x | x | x | | |
| FIA_UAU.6 | x | | | | | x | | |
| FIA_API.1 | | | | | | x | | |
| FDP_ACC.1 | x | | | | | x | | |
| FDP_ACF.1 | x | | | | | x | | |
| FDP_UCT.1 | x | | | | | x | | |
| FDP_UIT.1 | x | | | | x | x | | |
| FMT_SMF.1 | | x | | | | | | |
| FMT_SMR.1 | x | x | | | | x | | |
| FMT_LIM.1 | x | x | | | | | | x |

| | TSF_Access | TSF_Admin | TSF_Secret | TSF_Crypto | TSF_SecureMessaging | TSF_Auth | TSF_Integrity | TSF_OS |
|---|---|---|---|---|---|---|---|---|
| FMT_LIM.2 | x | x | | | | | | x |
| FMT_MTD.1/INI_ENA | | | | | | | | x |
| FMT_MTD.1/INI_DIS | | | | | | | | x |
| FMT_MTD.1/CVCA_INI | x | x | | | | x | | |
| FMT_MTD.1/CVCA_UPD | x | x | | | | x | | |
| FMT_MTD.1/DATE | x | x | | | | x | | |
| FMT_MTD.1/KEY_WRITE | x | | x | | | | | |
| FMT_MTD.1/CAPK | x | | x | | | x | | |
| FMT_MTD.1/KEY_READ | x | | x | | | | | x |
| FMT_MTD.3 | | | | | | x | | |
| FPT_EMSEC.1 | | | | | | | | x |
| FPT_FLS.1 | | | | | | | x | x |
| FPT_TST.1 | | | | | | | | x |
| FPT_PHP.3 | | | | | | | | x |

*Table 13: Mapping of TOE Security Requirements and TOE Security Functionalities.*

# References

In the following tables, the references used in this document are summarized. The first column lists the internal reference names, the third (last) column – if applicable – the reference numbers to these documents or older versions of these documents in the protection profile PP-0056 [PP0056].

## Common Criteria

| | | |
|---|---|---|
| [CC_1] | Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, July 2009; CCMB-2009-07-001. | [1] |
| [CC_2] | Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, July 2009; CCMB-2009-07-002. | [2] |
| [CC_3] | Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, July 2009; CCMB-2009-07-003. | [3] |
| [CC_4] | Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 3, July 2009; CCMB-2009-07-004. | [4] |

## Protection Profiles

| | | |
|---|---|---|
| [PP0056] | Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control, Version 1.10, 25.3.2009, BSI-PP-0056, Bundesamt für Sicherheit in der Informationstechnik. | - |
| [PP0002] | PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001. | [22] |
| [PP0035] | Security IC Platform Protection Profile, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007. | [24] |
| [PP0055] | Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March 2009. | [25] |
| [PP_Javacard] | Java Card System - Minimal Configuration Protection Profile, Version 1.1, May 2006, part of: Java Card Protection Profile Collection, Version 1.1, May 2006. | - |

## TOE and Platform References

| | | |
|---|---|---|
| [Guidance] | cv act ePasslet/EACv1 - cv act ePasslet Suite Java Card applet providing ICAO ePassport application with Extended Access Control, Guidance Manual, Version 2.0.5; cryptovision, June 2012 | - |
| [ST_BAC] | cv act ePasslet/BAC v1.8 Security Target, BSI-DSZ-CC-0798; cryptovision, August 2012. | - |

| | | |
|---|---|---|
| [ZertIC040] | Certification Report BSI-DSZ-CC-0404-2007 for NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification; BSI, July 2007. | - |
| [ZertIC080] | Certification Report BSI-DSZ-CC-0680-2010 for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B, each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH; BSI, November 2010. | - |
| [ZertIC081] | Certification Report BSI-DSZ-CC-0555-2009 for NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A, each with IC dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification; BSI, November 2009. | - |
| [ZertJCOP040] | Certification Report BSI-DSZ-CC-0730-2011 for NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, May 2011. | - |
| [ZertJCOP080], | Certification Report BSI-DSZ-CC-0674-2011 for NXP J3A080 and J2A080 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, March 2011. | - |
| [ZertJCOP081] | Certification Report BSI-DSZ-CC-0675-2011 for NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, April 2011. | - |
| [ZertCL040] | Certification Report BSI-DSZ-CC-0710-2010 for Crypto Library V2.6 on P5CD040V0B /P5CC040V0B / P5CD020V0B / P5CC021V0B /P5CD012V0B from NXP Semiconductors Germany GmbH; BSI, January 2011. | - |
| [ZertCL080] | Certification Report BSI-DSZ-CC-0709-2010 for Crypto Library V2.6 on P5CD080V0B /P5CN080V0B / P5CC080V0B / P5CC073V0B from NXP Semiconductors Germany GmbH; BSI, December 2010. | - |
| [ZertCL081] | Certification Report BSI-DSZ-CC-0633-2010 for Crypto Library V2.7 on P5CD081V1A /P5CC081V1A / P5CN081V1A / P5CD041V1A /P5CD021V1A / P5CD016V1A from NXP Semiconductors Germany GmbH; BSI, November 2010. | - |
| [ST_JCOP040] | Security Target Lite „NXP J3A040 and J2A040 Secure Smart Card Controller Rev. 3“, Rev. 01.03; NXP, 13 May 2011. | - |
| [ST_JCOP080] | Security Target Lite „NXP J3A080 and J2A080 Secure Smart Card Controller Rev. 3“, Rev. 01.02; NXP, December 2010. | - |
| [ST_JCOP081] | Security Target Lite „NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Rev. 3“, Rev. 01.02; NXP, December 2010. | - |
| [ST_CL040] | Security Target Lite “Crypto Library V2.6 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B”, Rev. 2.4; NXP, 14 December 2010. | - |
| [ST_CL080] | Security Target Lite “Crypto Library V2.6 on P5CD080V0B / P5CN080V0B / P5CC080V0B / P5CC073V0B”, NXP, Rev. 2.3; NXP, 12 November 2010. | - |
| [ST_CL081] | Security Target Lite “Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A”, NXP, Rev. 1.2; 9 November 2010. | - |

| | | |
|---|---|---|
| [ST_IC040] | Security Target Lite “P5CD040/P5CC040/P5CD020/P5CC021 V0B”, Rev. 1.0, NXP, 21 March 2007. | - |
| [ST_IC080] | Security Target Lite “P5CD080/P5CN080/P5CC080 V0B”, Rev. 1.0, NXP, 21 March 2007. | - |
| [ST_IC081] | Security Target Lite “NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A”, Rev. 1.3, NXP, 21 September 2009. | - |
| [JCOP_UGM] | NXP JCOP V2.4.1 Revision 3 secure smart card controller, Rev. 3.0--9 March 2011 – User manual, Doc No. 188830 | - |

## ICAO specifications

| | | |
|---|---|---|
| [ICAODoc] | ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization | [5] |

## Cryptography

| | | |
|---|---|---|
| [TR-03110] | Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI), 21.02.2008 | [26] |
| [TR-ECC] | Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006. | [27] |
| [ISO7816-4] | ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004 | [28] |
| [AIS20] | Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2.12.1999 | - |
| [AIS31] | Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik | - |
| [ISO14888-3] | ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999 | [7] |
| [FIPS46-3] | FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Techn logy | [8] |
| [NIST800-20] | NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999 | [9] |
| [FIPS180-2] | Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1 | [10] |
| [FIPS186-2] | Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1 | [11] |
| [FIPS197] | Federal Information Processing Standards Publication 197, ADVANCED | [12] |

| | | |
|---|---|---|
| | ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001 | |
| [ANSIX9.19] | ANSI X9.19, AMERICAN NATIONAL STANDARD, Financial Institution Retail Message Authentication, 1996 | [13] |
| [ANSIX9.62] | AMERICAN NATIONAL STANDARD X9.62-1999: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), September 20, 1998 | [14] |
| [ISO9796-2] | ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002 | [15] |
| [ISO15946-1] | ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002. | [16] |
| [ISO15946-2] | ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002. | [17] |
| [ISO15946-3] | ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002 | [18] |
| [PKCS3] | PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993 | [19] |
| [NIST800-38B] | Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005 | [20] |
| [RFC4493] | Request for Comments: 4493, The AES-CMAC Algorithm, JH. Song et al. University of Washington, Category: Informational, June 2006 | [21] |

# Glossary

| | |
|---|---|
| **Active authentication** | Security mechanism defined in [ICAODoc] by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization. |
| **AES** | The AES (Advanced Encryption Standard) has been defined as a standard for symmetric data encryption. It is a block cipher with a block length of 128 bit and key lengths of 128, 192 and 256 bit. |
| **Application note** | Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE. |
| **Asymmetric cipher** | Encryption procedures employing two different keys (in contrast to a symmetric cipher): one publicly known (public key) for data encryption and one key only known to the message receiver (private key) for decryption. |
| **Audit records** | Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data. |
| **Authentication** | Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures. |
| **BAC** | Basic access control. Security mechanism defined in [ICAODoc] by which means the MTRD's chip proves and the inspection system protects their communication by means of secure messaging. |
| **Basic access keys** | Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [ICAODoc]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book. |
| **Block cipher** | An algorithm processing the plaintext in bit groups (blocks). Its alternative is called stream cipher. |
| **CA** | Certification authority |
| **Certificate** | see digital certificate |
| **Certificate revocation list** | A list of revoked certificates issued by a certificate authority |
| **Certification authority** | An entity responsible for registering and issuing, revoking and generally managing digital certificates |
| **Country signing CA certificate ($C_{CSCA}$)** | Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority. The $C_{CSCA}$ is stored in the inspection system. |
| **Country verifying CA** | The country specific root of the PKI of Inspection Systems. It creates the<br>Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing country or organization in respect to the protection of sensitive biometric data stored in the MRTD. |
| **CRL** | see Certificate Revocation List |
| **Cryptography** | In the classical sense, the science of encrypting messages. Today, this notion comprises a larger field and also includes problems like authentication or digital |

| | |
|---|---|
| | signatures. |
| **Current date** | The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates. |
| **CVCA link certificate** | Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key. |
| **DES** | (Data Encryption Standard) symmetric 64 bit block cipher, which was developed (first under the name Lucifer) by IBM. The key length is 64 bit of which 8 bit serve for a parity check. DES is the classic among the encryption algorithms, which nevertheless is no longer secure due to its insufficient key length. Alternatives are Triple-DES or the successor AES. |
| **Digital certificate** | A data set that identifies the certification authority issuing it, identifies its owner, contains the ower's public key, identifies its operational period, and is digitally signed by the certification authority issuing it. |
| **Digital signature** | The counterpart of a handwritten signature for documents in digital format. A digital signature grants authentication, integrity, and non-repudiation. These features are achieved by using asymmetric procedures. |
| **Document verifier** | Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations |
| **EAC** | Extended access control. Security mechanism identified in [ICAODoc] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. |
| **ECC** | (Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm. |
| **Elliptic curves** | A mathematical construction, in which a part of the usual operations applies, and which has been employed successfully in cryptography since 1985. |
| **Fingerprint (digital)** | Checksum that can be used to easily determine the correctness of a key without having to compare the entire key. This is often done by comparing the hash values after application of a hash function. |
| **Hash function** | A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value. Common hash functions are RIPEMD-160 and SHA-1, each having hash values with a length of 160 bit as well as the MD5, which is still often used today having a hash value length of 128 bit. |
| **Inspection system** | A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and |

| | |
|---|---|
| | (ii) verifying the traveller as MRTD holder. |
| **Integrity** | The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hashfunctions, MACs (Message Authentication Codes) or – with additional functionality – digital signatures. |
| **Javacard** | A smart card with a Javacard operation system. |
| **Key exchange** | The use of symmetric cipher procedures requires that two communication partners decide on one joint key only known to themselves. The difficulty is that for the exchange of such information usually only partially secure channels exist. Additionally, protocols for key exchange must be prepared in such a way that only those pieces of information are exchanged which do not lead to knowledge of the real secret (the key). The most popular protocol of that type is diffie-Hellman, whose presentation in 1976 can be regarded as the birth of public key cryptography. |
| **LDS** | Logical data structure. The collection of groupings of data elements stored in the optional capacity expansion technology, defined in [ICAODoc]. |
| **MAC** | Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy, requires its protection in a suitable way. |
| **MRTD** | Machnine-readable travel document. Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. |
| **MRZ** | Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. |
| **Non-repudiation** | One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered and respective framework conditions need to be provided by pertinent laws. |
| **Passive authentication** | (i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object. |
| **Passphrase** | A long, but memorable character sequence (e.g. short sentences with punctuation) which should replace passwords as they offer more security. |
| **Password** | A secret character sequence whose knowledge is to serve as a replacement for the authentication of a participant. A password is usually short to really ensure that an attacker cannot guess the password by trial and error. |
| **Personalization** | The process by which the portrait, signature and biographical data are applied to the document. |
| **Personalization agent** | The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the |

| | |
|---|---|
| | holder. |
| **PKI** | Cf. Public Key Infrastructure |
| **PP** | Protection Profile |
| **Private key** | Secret key only known to the receiver of a message, which is used in asymmetric ciphers for encryption or generation of digital signatures. |
| **Pseudo random number** | Many cryptographic mechanisms require random numbers (e.g. in key generation). The problem, however, is that it is difficult to implement true random numbers in software. Therefore, so called pseudo-random number generators are used, which then should be initialized with a real random element (the so called *seed*). |
| **Public key** | Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures. |
| **Public key infrastructure (PKI)** | Combination of hardware and software components, policies, and different procedures used to manage digital certificates. |
| **Random numbers** | Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for a software), so called pseudo random numbers are used instead. |
| **Secure messaging** | Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4. |
| **SFR** | Security functional requirement. |
| **Skimming** | Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data. |
| **Smart card** | A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (ROM, EEPROM) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). Therefore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes. |
| **SOD** | Document Security Object (stored in EF.SOD). A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). |
| **ST** | Security Target |
| **Stream cipher** | Symmetric encryption algorithm which processes the plaintext bit-by-bit or byte-by-byte. The other usually employed class of procedures comprises so called block cipher. |
| **Symmetric cipher** | Encryption procedure using the same key for enciphering and deciphering (or, in which these two keys can simply be derived from each other). One distinguishes between block ciphers processing plaintext in blocks of fixed length (mostly 64 or 128 bit) and stream ciphers working on the basis of single characters. |

| | |
|---|---|
| **TOE** | Target of evaluation. |
| **Travel document** | A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel. |
| **TSF** | TOE security functionality. |
| **Verification** | The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. |
| **X.509** | Standard for certificates, CRLs and authentication services. It is part of the X.500 standard of the ITU-T for realization of a worldwide distributed directory service realized with open system. |