T · · Systems ·

# Specification of the Security Target TCOS ID Version 2.0 Release 1-BAC/P60D145

## Version: 2.0.1/20190117

| | |
|---|---|
| Dokumentenkennung: | CD.TCOS.ASE |
| Dateiname: | ASE TCOS ID 2.0.1-BAC (NXP).docx |
| Stand: | 17.01.2019 |
| Version: | 2.0.1 |
| Hardware Basis: | P60D145 |
| Autor: | Ernst-G. Giessmann |
| Geltungsbereich: | TeleSec Entwicklungsgruppe |
| Vertraulichkeitsstufe: | **Öffentlich** |

## History

| Version | Date | Remark |
|---|---|---|
| 2.0.1 | 2019-01-17 | Final Version |
| | | |
| | | |
| | | |

# Contents

# 1 ST Introduction

1 This section provides document management and overview information that are required a potential user of the TOE to determine, whether the TOE fulfils her requirements.

## 1.1 ST Reference

2

| | |
|---|---|
| Title: | Specification of the Security Target TCOS ID Version 2.0 Release 1-BAC/P60D145 |
| TOE: | TCOS ID Version 2.0 Release 1-BAC/P60D145 |
| Sponsor: | T-Systems International GmbH |
| Editor(s): | Ernst-G. Giessmann, Markus Blick, T-Systems International GmbH |
| CC Version: | 3.1 (Revision 5) |
| Assurance Level: | EAL4 augmented. |
| General Status: | Final |
| Version Number: | 2.0.1 |
| Date: | 2019-01-17 |
| Certification ID: | BSI-DSZ-CC-1103 |
| Keywords: | TCOS Passport, MRTD, BAC |

3 The TOE is a ready for Personalization contact-less chip with an initialized file system according to [BACPassPP] based like the TCOS Identity Cards on the Operation System TCOS developed at T-Systems.

## 1.2 TOE Reference

4 The Security Target refers to the Product “TCOS ID Version 2.0 Release 1-BAC//P60D145” (TOE), of T-Systems for CC evaluation.

## 1.3 TOE Overview

5 The Target of Evaluation (TOE) addressed by this Security Target is the electronic Passport Card or electronic Residence Permit Card representing a contactless smart card programmed according to the Logical Data Structure (LDS) or Technical Guideline TR-03110 ([EACTR] and providing the Extended Access Control according to ICAO document [ICAO9303-1] and an authentication mechanism according to the technical report [EACTR]. The hardware bases on a NXP chip P60D145 with the TCOS operating system. For CC evaluation the following application of the corresponding product will be considered:

6 the Passport Application1 (ePassport) containing the related user data2 (incl. biometric data) as well as the data needed for authentication (incl. MRZ); this application the TOE is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). Therefore in the following the Passport or Residence Permit Card will be considered as an MRTD only. According to the Technical Guideline TR-03110 (cf. [EACTR, part 1, 2.1]) the ePassport and Residence Permit Card Application supports Passive Authentication, Password Authenticated Connection Establishment (PACE), Terminal and Chip Authentication and also Basic Access Control (BAC).

7 In this Security Target only Basic Access Control (BAC) is considered for evaluation.

8 The ePassport application must be accessed through the contact-less interface of the TOE according to [EACTR].

9 The cryptographic algorithms used by the TOE are defined outside the TOE in the Public Key Infrastructure. The TOE supports Elliptic Curve Cryptography, though this is not relevant for this ST. According to [ICAO9303-1] for Basic Access Control (BAC) only TDES and SHA-1 are required (cf. Cryptographic Operation (FCS_COP) on p. 31).

10 The MRTD is integrated into a plastic, optically readable part of the Passport. This is not part of the TOE.

11 If in some context the hardware base is relevant, the TOE will be identified in more detail as the "TCOS ID Version 2.0 Release 1-BAC/P60D145", otherwise the notion "TCOS ID Version 2.0 Release 1-BAC" will be used, indicating that this context applies to any realization regardless which hardware base is used. Note that that the hardware base is identified as P60D145, but it applies also to its derivates, differing in the memory layout.

12 The TOE follows the composite evaluation aspects ([AIS36]). The Security Target of the underlying platform ([HWST]) claims conformance to Smartcard IC Platform Protection Profile ([ICPP]).

13 This composite ST is based on the ST of the underlying platform ([HWST]). The compatibility of the Life Cycle Model of the Protection Profile [BACPassPP] and the Life Cycle Model required by [ICPP] will be shown in 1.3.1.

### 1.3.1 TOE security features for operational use

14 The following TOE security features are the most significant for its operational use:

- terminals gets the authorization to read the logical MRTD under the Basic Access Control only by optical reading the MRTD or other parts of the passport book providing this information
- verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the service provider connected,
- Averting of inconspicuous tracing of the MRTD,
- Self-protection of the TOE security functionality and the data stored inside.

1 as specified in [EACTR, sec. 3.1.1], see also [ICAO9303-1]

2 according to [EACTR, sec. 3.1.1]; see also Glossary below for definitions

### 1.3.2 TOE Definition

15 The TOE comprises of

- the circuitry of the contactless chip including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (operating system)
- at least the ePassport application and
- the associated guidance documentation

16 The components of the TOE are therefore the hardware (IC), the operating system TCOS (OS) and the dedicated filesystem for the ePassport application in a file system. A detailed description of the parts of TOE will be given in other documents.

17 Since contactless interface parts (e.g. antenna) may have impact on specific aspects of vulnerability assessment and, thus, be security relevant, these parts are considered in this ST as part of the TOE. The decision upon this was made by the certification body in charge. Further details are considered in the ALC documentation.

### 1.3.3 File System of the TOE

18 The TOE is configured with one of the dedicated file systems during life cycle phase 2 “Manufacturing”.

19 The available Major Configurations of the file system related to this ST are described in detail in other documents [TCOSCONF]. They do not differ in security-relevant ways. For example, the product configured as Passport provides the same security functionality of an electronic travel document as the product configured as Residence Permit. Though the latter can be used as a Qualified Signature Creation Device, this has no impact on the security functionality of a Passport, not providing this functionality.

20 The two Major Configurations of the TOE in this Security Target, which differ only in the description of the object system, are:

- Passport: user data stored in an ICAO-compliant ePass application.
- Residence Permit: user data stored in an ICAO-compliant ePass application. Additional user data are stored in [EACTR-2] conformant eID and [SSCDPP] conformant eSign Applications, and are protected by EAC2.

21 Depending on the Configuration additionally the eSign Application can be already activated by a Certification Service Provider. The user data of the eSign Application are protected by PACE/EAC2.

### 1.3.4 Life Cycle Phases Mapping

22 Following the protection profile PP0084 [ICPP, sec. 1.2.3] the life cycle phases of a TCOS Passport device can be divided into the following seven phases:

Phase 1: IC Embedded Software Development

Phase 2: IC Development

Phase 3: IC Manufacturing

Phase 4: IC Packaging

Phase 5: Composite Product Integration

Phase 6: Personalization

Phase 7: Operational Use

23 According to the PP [BACPassPP] the TOE life cycle is described in terms of the four life cycle phases[3].

**Life cycle phase 1 "Development"**

24 The TOE is developed in phase 1. The IC developer (i.e. the Platform Developer according to [AIS36]) develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

25 The software developer (i.e. the Application Developer according to [AIS36]) 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 dedicated applications and the guidance documentation associated with these TOE components.

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

27 This life cycle phase 1 covers Phase 1 and Phase 2 of [ICPP], which are called *steps* in the PP [BACPassPP].

**Life cycle phase 2 "Manufacturing"**

28 In a first step the TOE integrated circuit is produced containing the TOE's Dedicated Software and the parts of the Embedded Software in the non-volatile memories (ROM and EEPROM). 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 (note that both of these roles may be assigned to different entities).

29 The inlay holding the chip as well as the antenna and the plastic with optical readable part, (holding the e.g. the printed MRZ) are necessary to represent a complete passport, nevertheless they are not inevitable for the secure operation of the TOE.

30 The MRTD manufacturer

(i) add the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary,

(ii) creates the ePassport application, i.e. the MF and the ICAO.DF,

(iii) equips TOE's chip with Pre-personalization Data and

(iv) packs the IC with hardware for the contactless interface in the MRTD.

31 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.

3 Note that this corresponds to the life cycle phases defined in the [BACPassPP] as well.

32 This life cycle phase 2 corresponds to Phase 3 and Phase 4 of [ICPP] and may include for flexibility reasons Phase 5 and some production processes from Phase 6 as well. Depending on the requirements of the following Personalization life cycle phase 3 some restrictions for the file system may also be fixed already in this phase. Despite of that they all could be made also during Personalization, i.e. they are not changing the TOE itself, such an approach of delivering the TOE with different configurations is useful for issuing states or organizations. The mentioned restrictions never change the structure of the file system, but affect only the pre-allocation of maximal available memory and the a priori appearance of elementary files (EFs) for data groups to be allocated and filled up during Personalization. Note that any other file parameter including the access rules cannot be changed.

33 For the TOE two pre-configured major configurations apply. A detailed description of the sub-phases and the system configurations, including the assigned maximal available memory sizes can be found in the Administrator Guidance [TCOSCONF].

34 The product is finished after initialization, after testing the OS and creation of the dedicated file system with security attributes and readymade for the import of User Data. This corresponds to the end of the life cycle phase 2 of the Protection Profile [EACPassPP]. The TOE may also be pre-configured during manufacturing which leads to different configurations for delivering. A more detailed description of the production processes in Phases 5 and 6 of PP0084 [ICPP] is given in the Administrator Guidance document [TCOSADM]. Note that the physical interface (i.e. the antenna) is out of the scope of the PP0084. Therefore it is not considered in the life cycle phases mapping.

**Life cycle phase 3 “Personalization of the travel document”**

35 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 plastic cover of the physical MRTD,

(iv) the writing of TOE User Data and TSF Data into the logical MRTD and

(v) configuration of the TSF if necessary (not applicable for the TOE).

36 The step (iv) is performed by the Personalization Agent.

37 The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

38 This life cycle phase corresponds to the remaining initialization and personalization processes not covered yet from Phase 6 of the [ICPP].

39 *Application Note 1*: Note that from hardware point of view the life cycle phase “Issuing/Personalization” is already an operational use of the composite product and no more a personalization of the hardware. The hardware’s “Personalization” (cf. [HWST]) ends with the initialization and pre-personalization of the TOE and should not be confused with the Personalization described in the Administrator Guidance [TCOSADM].

**Life cycle phase 4 “Operational Use”**

40 The TOE is used as MRTD’s chip by the MRTD holder and the terminals in the “Operational Use” phase.

41 This life cycle phase corresponds to the Phase 7 of the [ICPP].

42 The security environment for the TOE and the ST of the underlying platform match, the Phases up to 6 are covered by a controlled environment as required in [HWCR, p. 41]. In Phase 7 (Operational Use) no restrictions apply.

### 1.3.5 Non-TOE hardware/software/firmware

43 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 travel document; nevertheless these parts are not inevitable for the secure operation of the TOE.

### 1.3.6 TOE Boundaries

#### 1.3.6.1 TOE Physical Boundaries

44 Smart card as used in this ST means an integrated circuit containing a microprocessor, (CPU), a coprocessor for special (cryptographic) operations, a random number generator, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier. The integrated circuit is a single chip incorporating CPU and memory which include RAM, ROM, and EEPROM.

45 The chip is embedded in a module which provides the capability for standardized connection to systems separate from the chip through contactless interface in accordance with ISO standards.

46 The physical constituents of the TOE are the operating system, the data in elementary files of the dedicated file of the ICAO application (EEPROM), and temporary data used during execution of procedures associated to that dedicated file.

#### 1.3.6.2 TOE Logical Boundaries

47 All card accepting devices (Host Applications) will communicate through the I/O interface of the operating system by sending and receiving octet strings. The logical boundaries of the TOE are given by the complete set of commands of the TCOS operating system for access, reading, writing, updating or erasing data.

48 The input to the TOE is transmitted over the physical interface as an octet string that has the structure of Command Application Protocol Data Unit (CAPDU).

49 The output octet string from the TOE has the structure of a Response Application Protocol Data Unit (RAPDU).

50 The Application Protocol Data Units or TCOS commands that can be used in the operating systems are described in more detail in another document.

# 2 Conformance Claim

## 2.1 CC Conformance Claims

51 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017,

Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017,

Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

1 as follows:

Part 2 extended,

Part 3 conformant.

2 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 ([CC]) has to be taken into account. The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations.

## 2.2 PP Claims

3 This ST claims *strict* conformance to 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application" Basic Access Control', Version 1.10, BSI-CC-PP-0055 issued by Bundesamt für Sicherheit in der Informationstechnik (BSI) [BACPassPP].

## 2.3 Package Claims

4 The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [HWCR]. The IC hardware platform and its primary embedded software are evaluated at level EAL 6+.

5 The evaluation assurance level of the TOE is EAL4 augmented with ALC_DVS.2, as defined in [CC].

## 2.4 Conformance Rationale

6 Since the ST is not claiming conformance to any other protection profile and the PP [BACPassPP] is not claiming conformance to another PP, no rationale is necessary here.

# 3 Security Problem Definition

## 3.1 Introduction

### Assets

7 The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the Appendix Glossary for the term definitions)

| Object No. | Asset | Definition | Generic security property to be maintained by the current security policy |
|---|---|---|---|
| 1 | user data stored on the TOE | All data (being not authentication data) stored in the context of the ePassport application of the MRTD as defined in [EACTR] and being allowed to be *read out* or *written* by a terminal (in the sense of [EACTR, part 2, 2.2]).<br>This data consists of Personal Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16), the Chip Authentication Public Key in EF.DG14, Active Authentication Public Key in EF.DG15, Document Security Object ($SO_D$) in EF.SOD, Common data in EF.COM and Sensitive biometric reference data (EF.DG3, EF.DG4). | Confidentiality<br>Integrity<br>Authenticity |
| 2 | user data transferred between the TOE and the terminal connected | All data (being not authentication data) being transferred in the context of the ePassport application between the TOE and a terminal (in the sense of [EACPassPP, sec. 3.2].<br>User data can be received and sent. | Confidentiality<br>Integrity<br>Authenticity |
| 3 | MRTD tracing data | Technical information about the current and previous locations of the MRTD gathered by inconspicuous (for the MRTD holder) recognizing the TOE not knowing the MRZ.<br>TOE tracing data can be provided / gathered. | Unavailability[4] |

**Table 1: Primary assets**

8 All these primary assets represent User Data in the sense of the CC.

9 The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

| Object No. | Asset | Definition | Property to be maintained by the current security policy |
|---|---|---|---|
| 4 | Accessibility to the TOE functions and data only for authorized subjects | Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only. | Availability |
| 5 | Genuineness of the TOE | Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way.<br>This asset covers the 'Authenticity of the MRTD's chip' in [BACPassPP]. | Availability |

4 represents a prerequisite for anonymity of the MRTD holder

| Object No. | Asset | Definition | Property to be maintained by the current security policy |
|---|---|---|---|
| 6 | TOE immanent secret cryptographic keys | Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality. | Confidentiality<br>Integrity |
| 7 | TOE immanent non-secret cryptographic keys | Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Card/Chip and Document Security Objects $SO_C$ and $SO_D$, respectively, containing digital signatures) used by the TOE in order to enforce its security functionality. | Integrity<br>Authenticity |

**Table 2: Secondary assets**

10 *Application Note 2*: Please note that the MRZ is not transmitted to the TOE.

11 The secondary assets represent TSF and TSF-data in the sense of the CC.

## Subjects and external entities

12 This ST considers the following subjects:

| External Entity | Subject | Role | Definition |
|---|---|---|---|
| 1 | 1 | MRTD holder | A person for whom the MRTD issuer has personalized the MRTD.<br>This entity is commensurate with 'MRTD Holder' in [BACPassPP].<br>Please note that an MRTD holder can also be an attacker (s. below). |
| 2 | – | MRTD presenter | A person presenting the MRTD to a terminal[5] and claiming the identity of the MRTD holder.<br>This subject is commensurate with 'Traveler' in [BACPassPP].<br>Please note that an MRTD holder can also be an attacker (s. below). |
| 3 | 2 | Terminal | A terminal is any technical system communicating with the TOE through the contactless interface.<br>The role 'Terminal' is the default role for any terminal being recognized by the TOE ('Terminal' is used by the MRTD presenter). |
| 4 | 3 | Basic Inspection System with BAC (BIS-BAC) | A technical system being used by an authority[6] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the MRTD presenter as the MRTD holder (for *ePassport*: by comparing the real biometrical data of the MRTD presenter with the stored biometrical data of the MRTD holder).<br>BIS-BAC is supporting/applying the Passive Authentication. BIS-BAC is equivalent to the Basic Inspection System (BIS) as defined in [BACPassPP]. |
| 5 | – | Document Signer (DS) | An organization enforcing the policy of the CSCA and signing the Card/Chip and Document Security Objects stored on the MRTD for passive authentication.<br>A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate ($C_{DS}$), see [EACTR, part 1, 1.1] and [ICAO9303-1].<br>This role is usually delegated to a Personalization Agent.<br>This entity is commensurate with the respective external entity #9 in [PACEPassPP]. |

5 in the sense of [EACTR]

6 concretely, by a control officer

| External Entity | Subject | Role | Definition |
|---|---|---|---|
| 6 | – | Country Signing Certification Authority (CSCA) | An organization enforcing the policy of the MRTD Issuer with respect to confirming correctness of user and TSF data stored in the MRTD. The CSCA represents the country specific root of the PKI for the MRTDs and creates the Document Signer Certificates within this PKI.<br>The CSCA also issues the self-signed CSCA Certificate ($C_{CSCA}$) having to be distributed by strictly secure diplomatic means, see. [ICAO9303-1], 5.1.1.<br>The Country Signing Certification Authority issuing certificates for Document Signers (cf. [ICAO9303-1]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [EACTR, part 3, 2.1]. |
| 7 | 4 | Personalization Agent | An organization acting on behalf of the MRTD Issuer to personalize the MRTD for the MRTD holder by some or all of the following activities: (i) establishing the identity of the MRTD holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder, (iii) writing a subset of these data on the physical Passport (optical personalization) and storing them in the MRTD (electronic personalization) for the MRTD holder as defined in [EACTR], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Card/Chip Security Object and the Document Security Object (ePassport) defined in [ICAO9303-1] (in the role of DS).<br>Please note that the role 'Personalization Agent' may be distributed among several institutions according to the operational policy of the MRTD Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role. |
| 8 | 5 | Manufacturer | Generic term for the IC Manufacturer producing integrated circuit and the MRTD Manufacturer completing the IC to the MRTD. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and MRTD Manufacturer using this role Manufacturer. |
| 9 | – | Attacker | A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. |

**Table 3: Subjects and external entities**[7]

## 3.2 Threats

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

**T.Chip_ID Identification of MRTD's chip**

14 An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. The attacker has enhanced basic attack potential, not knowing

7 This table defines external entities and subjects in the sense of [CC]. Subjects can be recognized by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC]). From this point of view, the TOE itself does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognized by the TOE.

the optically readable MRZ data printed on the MRTD data page in advance. The asset is the anonymity of the MRTD holder.

**T.Skimming** **Skimming MRTD/Capturing Card–Terminal Communication**

15 An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker having enhanced basic attack potential cannot read and does not know the correct value of the optically readable MRZ data printed on the MRTD data page in advance. The asset is the confidentiality of logical MRTD data.

**T.Eavesdropping** **Eavesdropping on the communication between the TOE and a inspection system**

16 An attacker is listening to a communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance. The attacker having enhanced basic attack potential does not know the optically readable MRZ data printed on the MRTD data page in advance. The asset is the confidentiality of logical MRTD data.

**T.Forgery** **Forgery of Data**

17 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. The attacker having enhanced basic attack potential is in possession of one or more legitimate MRTDs. The asset is the authenticity of logical MRTD data.

18 The following threats shall be averted by the TOE as specified below.

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

19 An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder. The attacker having enhanced basic attack potential, is in possession of a legitimate

MRTD. The asset is the confidentiality and authenticity of logical MRTD and TSF data, and the correctness of TSF.

**T.Information_Leakage Information Leakage from MRTD**

20 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). The attacker, having enhanced basic attack potential, is in possession of a legitimate MRTD. The asset is the confidentiality of logical MRTD and TSF data.

**T.Phys-Tamper Physical Tampering**

21 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. The attacker having enhanced basic attack potential, is in possession of a legitimate MRTD. The asset is the confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

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

22 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. The attacker having enhanced basic attack potential is in possession of a legitimate MRTD. The asset is the confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

## 3.3 Organizational Security Policies

23 The TOE and/or its environment shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

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

24 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.

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

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

**P.Personal_Data** **Personal data protection policy**

26 The biographical data and its summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)3 and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO9303-1].

27 *Application Note 3*: The organizational security policy P.Personal_Data is drawn from the ICAO Doc 9303 [ICAO9303-1]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

## 3.4 Assumptions

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

29 The PP ([BACPassPP]) includes the assumption **A.MRTD_Manufact**. It is covered in this ST by ALC_DVS.2. Therefore it will not be repeated here.

30 The PP ([BACPassPP]) includes the assumption **A.MRTD_Delivery**. It is covered in this ST by ALC_DEL.1. Therefore it will not be repeated here.

31 *Application note 4:* Assumptions A.MRTD_Manufact and A.MRTD_Delivery from [BACPassPP] address manufacturing, testing and delivery aspects. Fulfillment of such assumptions is a necessary condition for a 'pass' judgment by applying the chosen assurance components ALC_DVS.2 and ALC_DEL.1, respectively. It means that if the components ALC_DVS.2 and ALC_DEL.1 have positively been judged, the fulfillment of these assumptions is 'automatically' ensured: the manufacturer is required and

responsible for applying all the related procedures with respect to the TOE. Therefore, the assumptions A.MRTD_Manufact and A.MRTD_Delivery are implicitly included into the BAC PP ([BACPassPP]) by choosing the assurance components ALC_DVS.2 and ALC_DEL.1.

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

32 The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

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

33 The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO9303-1]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

34 *Application Note 5*: According to [ICAO9303-1] the support of the Passive Authentication mechanism is mandatory whereas the BAC is optional. Nevertheless for this ST the Basic Access Control is mandatory.

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

35 The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the ICAO Doc 9303 [ICAO9303-1], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

36 *Application Note 6*: When assessing the MRZ data or the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

# 4 Security Objectives

37 This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

## 4.1 Security Objectives for the TOE

38 The following TOE security objectives address the protection provided by the TOE *independent* of the TOE environment.

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

39 The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO9303-1] 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.DG 3 to EF.DG16 are added.

40 *Application Note 7*: The OT.AC_Pers implies that the data of the LDS groups written during personalization for MRTD holder cannot be changed by write access after personalization. The Personalization Agents may add (fill in) data into the LDS data groups not written yet, and update and sign the Document Security Object accordingly. Adding data in the “Operational Use” phase is not supported.

**OT.Data_Int Integrity of Data**

41 The TOE must ensure the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

**OT.Data_Conf Confidentiality of Data**

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

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

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

44 *Application Note 8*: The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and/or to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the MRTD”. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 “Operational Use” the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

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

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

46 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.

**OT.Prot_Inf_Leak Protection against Information Leakage**

47 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,
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

48 *Application Note 9:* This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

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

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

- measuring through galvanic contacts representing a direct physical probing on the chip’s 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 electrical charges (using tools used in solid-state physics research and IC failure analysis),

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

with a prior

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

**OT.Prot_Malfunction Protection against Malfunctions**

50 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.

51 *Application Note 10:* 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

### I. MRTD issuer (State or Organization) as the general responsible

52 The MRTD issuer as the general responsible for the global security policy related will implement the following security objectives of the TOE environment:

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

53 An appropriate functionality testing of the TOE shall be used in life cycle phases 4 to 6. During all manufacturing and test operations, security procedures shall be used to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

**OE.MRTD_Delivery Protection of the MRTD Delivery**

54 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.

55 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 proce-

dure for delivery got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

**OE.Personalization Personalization of the logical MRTD**

56 The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

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

57 The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO9303-1].

**OE.BAC-Keys Chip Authentication Key**

58 The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the ICAO Doc 9303 [ICAO9303-1] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

## II. Terminal's PKI (receiving) branch

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

**OE.Exam_MRTD Authentication of rightful terminals**

60 The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO9303-1].

**OE.Passive_Auth_Verif Terminal operating**

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

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

62 The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

## 4.3 Security Objective Rationale

63 The following table provides an overview for security objectives coverage (TOE and its environment). It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

| | OT.AC_Pers | OT.Data_Int | OT.Data_Conf | OT.Identication | OT.Prot_Abuse-Func | OT.Prot_Inf_Leak | OT.Prot_Phys-Tamper | OT.Prot_Malfunction | OE.MRTD_Manufact | OE.MRTD_Delivery | OE.Personalization | OE.Pass_Auth_Sign | OE.BAC-Keys | OE.Exam_MRTD | OE.Passive_Auth_Verif | OE.Prot_Logical_MRTD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.Chip_ID | | | | x | | | | | | | | | x | | | |
| T.Skimming | | | x | | | | | | | | | | x | | | |
| T.Eavesdropping | | | x | | | | | | | | | | | | | |
| T.Forgery | x | x | | | | | x | | | | | x | | x | x | |
| T.Abuse-Func | | | | | x | | | | | | x | | | | | |
| T.Information_Leakage | | | | | | x | | | | | | | | | | |
| T.Phys-Tamper | | | | | | | x | | | | | | | | | |
| T.Malfunction | | | | | | | | x | | | | | | | | |
| P.Manufact | | | | x | | | | | | | | | | | | |
| P.Personalization | x | | | x | | | | | | | x | | | | | |
| P.Personal_Data | | x | x | | | | | | | | | | | | | |
| A.MRTD_Manufact | | | | | | | | | x | | | | | | | |
| A.MRTD_Delivery | | | | | | | | | | x | | | | | | |
| A.Pers_Agent | | | | | | | | | | | x | | | | | |
| A.Insp_Sys | | | | | | | | | | | | | | x | | x |
| A.BAC-Keys | | | | | | | | | | | | | x | | | |

**Table 4:Security Objective Rationale**

64 A detailed justification required for suitability of the security objectives to coup with the security problem definition is given in the Protection Profile ([BACPassPP]). Hence there is no need to duplicate it here.

65 For the Composite Evaluation the following Security Objectives for the Hardware Platform are relevant too. They are listed here for the sake of completeness only. The detailed analysis of the Security Objectives derived from the hardware platform ST [HWST] and the environment of the Hardware Platform is made separately in a the chapter 7.8 (Statement of Compatibility).

66 The following Security Objectives for the Hardware Platform are based on [ICPP]:

| | |
|---|---|
| O.Leak-Inherent | (Protection against Inherent Information Leakage) |
| O.Phys-Probing | (Protection against Physical Probing) |
| O.Malfunction | (Protection against Malfunctions) |
| O.Phys-Manipulation | (Protection against Physical Manipulation) |
| O.Leak-Forced | (Protection against Forced Information Leakage) |
| O.Abuse-Func | (Protection against Abuse of Functionality) |
| O.Identification | (TOE Identification) |

67 They are all relevant and do not contradict Security Objectives of the TOE. They can be mapped to corresponding objectives of the TOE.

68 The remaining objective O.RND is covered by Security Objectives OT.Data_Integrity, and OT.Data_Confidentiality. These Security Objectives of the TOE address the integrity and confidentiality of transmitted data, based on the protocols of Terminal and Chip Authentication, depending on a high cryptographic quality of random number generation. Therefore this objective is supported by Security Objectives of the TOE.

# 5 Extended Components Definition

69 This protection profile uses components defined as extensions to CC part 2. All these extended components are drawn from Definitions of chapter 5 of [BACPassPP].

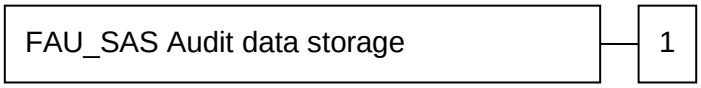
## 5.1 FAU_SAS Audit data storage

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

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.

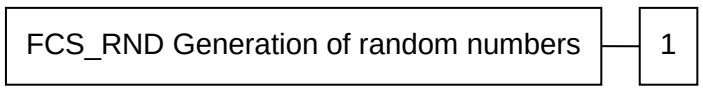
## 5.2 FCS_RND Generation of random numbers

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

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*].

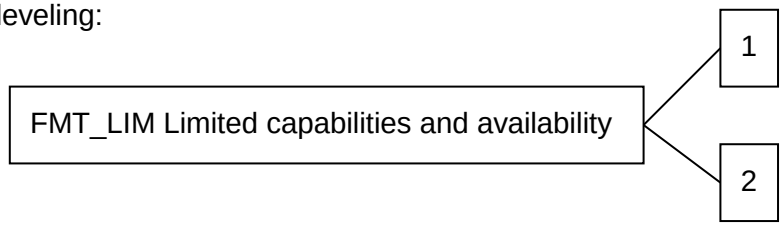
## 5.3 FMT_LIM Limited capabilities and availability

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

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 require that the TSF is built to provide only the capabilities (perform action, gather information) which are 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.

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

**FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.2 Limited availability.

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

**FMT_LIM.2 Limited availability**

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].

Dependencies: FMT_LIM.1 Limited capabilities.

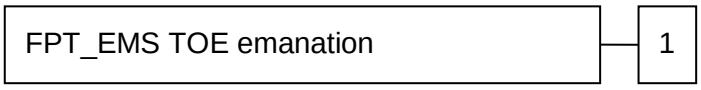
## 5.4 Definition of the Family FPT_EMS

The family “TOE Emanation (FPT_EMS)” is specified as follows. Due to TLA[8] restrictions in CC documents and to conform to EACPassPP the family FPT_EMSEC defined in the BACPassPP is renamed in this ST.

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:




FPT_EMS.1 TOE emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

8 TLA = three letter acronym

There are no actions defined to be auditable.

**FPT_EMS.1 TOE Emanation**

Hierarchical to: No other components.

FPT_EMS.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_EMS.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*].

Dependencies: No other components.

# 6 Security Requirements

73 This part of the PP defines the detailed security requirements that shall be satisfied by the TOE. The statement of **TOE security requirements** shall define the *functional* and *assurance* security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

74 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in section 8.1 of Part 1 of the Common Criteria [CC]. Each of these operations is used in this ST.

75 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~.

76 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections made by the ST author appear *slanted and underlined*.

77 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments made by the ST author appear *slanted and underlined*.

78 The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.
For the sake of a better readability, the iteration operation may also be applied to some single components (being not repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

79 The definition of the subjects "Manufacturer", "Personalization Agent", "Basic Inspection System" and "Terminal" used in the following chapter was given in section 3.1. Note that all these subjects are acting for homonymous external entities. All used objects are defined in the Appendix Glossary and Acronyms.

80 Definition of security attributes:

| security attribute | values | meaning |
|---|---|---|
| Terminal authentication status | none (any terminal) | default role (i.e. without authorization after start-up) |
| | Basic Inspection System | Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2. |
| | Personalization Agent | Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2... |

## 6.1 Security Functional Requirements for the TOE

### 6.1.1 Class FAU Security Audit

81 **FAU_SAS.1 Audit storage**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FAU_SAS.1.1 | The TSF shall provide the Manufacturer[9] with the capability to store the IC Identification Data[10] in the audit records. |

82 *Application Note 11*: The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization and/or Pre-personalization Data as TSF-data into the TOE. The audit records are usually write-only-once data of the MRTD (see FMT_MTD.1/INI_DIS).

### 6.1.2 Class FCS Cryptographic Support

#### 6.1.2.1 Cryptographic Key Generation (FCS_CKM)

83 The following iterations are caused by different cryptographic key generation algorithms to be implemented and keys to be generated by the TOE.

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1/ | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Control Key Derivation Algorithm [11] and specified cryptographic key sizes 112 bit[12] that meet the following: [ICAO9303-1], normative appendix 5[13]. |

9 [assignment: *authorized users*]
10 [assignment: *list of audit information*]
11 [assignment: *cryptographic key generation algorithm*]
12 [assignment: *cryptographic key sizes*]
13 [assignment: *list of standards*]

85 *Application Note 12*: The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [ICAO9303-1, normative appendix 5, A.5.2], produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO9303-1, normative appendix A.5.1]. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

86 **FCS_CKM.4 Cryptographic key destruction - MRTD**

Hierarchical to: No other components.

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

FCS_CKM.4.1/ The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with the new key*[14] that meets the following: *none*[15].

87 *Application Note 13*: The TOE destroys the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging after closing the secure channel or power-off.

### 6.1.2.2 Cryptographic Operation (FCS_COP)

88 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.

89 **FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation**

Hierarchical to: No other components.

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

FCS_COP.1.1/ SHA The TSF shall perform hashing[16] in accordance with a specified cryptographic algorithm SHA-1[17] and cryptographic key sizes none[18] that meet the following: FIPS 180-2 [FIPS180][19].

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

90 **FCS_COP.1/ENC Cryptographic operation – Encryption / Decryption Triple DES**

Hierarchical to: No other components.

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

FCS_COP.1.1/ENC: The TSF shall perform secure messaging (BAC) – encryption and decryption[20] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[21] and cryptographic key sizes 112 bit[22] that meet the following: FIPS 46-3 [FIPS46] and [ICAO9303-1, Normative Appendix 5, A5.3][23].

91 **FCS_COP.1/AUTH Cryptographic operation – Authentication**

Hierarchical to: No other components.

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

FCS_COP.1.1/AUTH: The TSF shall perform symmetric authentication – encryption and decryption[24] in accordance with a specified cryptographic algorithm AES[25] and cryptographic key sizes 128 bit[26] that meet the following: FIPS 197 [FIPS197][27].

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

Hierarchical to: No other components.

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

20 [assignment: *list of cryptographic operations*]
21 [assignment: *cryptographic algorithm*]
22 [assignment: *cryptographic key sizes*]
23 [assignment: *list of standards*]
24 [assignment: *list of cryptographic operations*]
25 [assignment: *cryptographic algorithm*]
26 [assignment: *cryptographic key sizes*]
27 [assignment: *list of standards*]

| | |
|---|---|
| FCS_COP.1.1/ MAC | The TSF shall perform secure messaging – message authentication code[28] in accordance with a specified cryptographic algorithm Retail MAC[29] and cryptographic key sizes 112 bit[30] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[31]. |

### 6.1.2.3 Random Number Generation (FCS_RND)

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

94 **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 quality requirements for a DRG.4 generator according to* [AIS31][32]. |

95 *Application Note 14:* This requirement is specified in [AIS31] in more detail. The TOE implements a hybrid deterministic[33] random number generator of the pre-defined class DRG.4 that provides the following security capabilities:

(DRG.4.1) The internal state of the RNG shall *use PTRNG of class PTG.2 as random source*[34].

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy *on condition "session closed or aborted"*[35].

(DRG.4.5) The internal state of the RNG is seeded by *a PTRNG of class PTG.2*[36].

(DRG.4.6) The RNG generates output for which $k > 2^{34}$ strings[37] of bit length 128 are mutually different with probability $1-\varepsilon$, with $\varepsilon < 2^{-16}$ [38].

---

28 [assignment: *list of cryptographic operations*]
29 [assignment: *cryptographic algorithm*]
30 [assignment: *cryptographic key sizes*]
31 [assignment: *list of standards*]
32 [assignment: *a defined quality metric*]
33 [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]
34 [selection: *use PTRNG of class PTG.2 as random source*, *have* [assignment: *work factor*], *require* [assignment: *guess work*]]
35 [selection: *on demand, on condition* [assignment: *condition*], *after* [assignment: *time*]]
36 [selection: *internal entropy source*, *PTRNG of class PTG.2*, *PTRNG of class PTG.3*, [other selection]]
37 [assignment: *number of strings*]
38 [assignment: *probability*]

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[39], *the NIST and the dieharder*[40] *tests*[41].

96 *Application Note 15*: This SFR requires the TOE to generate random numbers (random nonces) used for the authentication protocols as required by FIA_UAU.4.

### 6.1.3 Class FIA Identification and Authentication

97 *Application Note 16:* The following table provides an overview of the authentication mechanisms used.

| Name | SFR for the TOE | Algorithms and key sizes according to [ICAO9303-1, normative appendix 5], and [EACTR] |
|---|---|---|
| Basic Access Control Authentication Mechanism | FIA_UAU.4, FIA_UAU.6 | Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC) |
| Symmetric Authentication Mechanism for Personalization Agents | FIA_UAU.4 | AES with 128 bit keys (cf. FCS_COP.1/AUTH) |

**Table 5: Overview of authentication SFRs**

#### 6.1.3.1 User Identification (FIA_UID.1)

98 **FIA_UID.1/Rightful_Terminal Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 "Manufacturing"
2. to read the random identifier in Phase 3 "Personalization of the MRTD",
3. to read the random identifier in Phase 4 "Operational Use"[42]

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.

99 *Application Note 17:* The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the

39 [assignment: *additional test suites*]

40 The selected here test suites http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.1.1.zip and http://www.phy.duke.edu/~rgb/General/dieharder/dieharder-3.31.0.tgz are available at NIST and Dieharder web sites. Note that the dieharder tests include Marsaglia's "Diehard battery of tests" and NIST tests.

41 [assignment: *additional test suites*]

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

Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. 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 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System 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 authenticate the user as Basic Inspection System.

100 *Application Note 18:* In the “Operational Use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’s chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more than one RFID. This identifier is selected randomly and contains no user specific information.

#### 6.1.3.2 User Authentication (FIA_UAU)

101 **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 read the Initialization Data in Phase 2 "Manufacturing"<br>2. to read the random identifier in Phase 3 "Personalization of the MRTD",<br>3. to read the random identifier in Phase 4 "Operational Use"[43]<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. |

102 *Application Note 19:* The Basic Inspection System and the Personalization Agent authenticate themselves.

103 **FIA_UAU.4 Single-use authentication mechanisms - Single-use authentication of the Terminals by the TOE**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |

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

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on *Symmetric Authentication Mechanism based on AES-128* [44][45].

104 *Application Note 20:* The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalization Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

105 *Application Note 21:* The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO9303-1]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

106 **FIA_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on *AES*[46] [47]

to support user authentication.

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

1. The TOE accepts the authentication attempt as Personalization Agent one of the following mechanism(s): *Symmetric Authentication Mechanism based on AES-128*[48].
2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys[49].

107 *Application Note 22:* In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [EACPassPP] is

44 [selection: *Triple-DES, AES or other approved algorithms*]
45 [assignment: *identified authentication mechanism(s)*]
46 [selection: Triple-DES, AES]
47 [assignment: *list of multiple authentication mechanisms*]
48 [selection: *the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key,* [assignment *other*]]
49 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

also fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES. The Personalization Agent could be authenticated by using the symmetric AES-based authentication mechanism or other (e.g. the Terminal Authentication Protocol using the Personalization Key, cf. [EACPassPP] FIA_UAU.5.2).

108 *Application Note 23:* 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 may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism[50].

110 *Application Note 24:* The Basic Access Control Mechanism specified in [ICAO9303-1] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

111 *Application Note 25:* Note that in case the TOE fulfills [EACPassPP] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

### 6.1.3.3 Authentication Failure Handling (FIA_AFL)

112 **FIA_AFL.1 Authentication failure handling**

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UAU.1 Timing of authentication |

| | |
|---|---|
| FIA_AFL.1.1 | The TSF shall detect when *2*[51] unsuccessful authentication attempts occur related to *BAC authentication attempts within a single power-on-session*[52]. |
| FIA_AFL.1.2 | When the defined number of unsuccessful authentication attempts has been *met or surpassed*[53], the TSF shall *wait before accepting any other command at least the time which is necessary for re-initialization after power-on*[54]. |

113 *Application Note 26:* These assignments ensure the strength of authentication function for the Basic Access Control. The initialization time after power-off is an upper bound for the time required by an attacker because even if the TOE waits longer, the attacker could enforce the re-start by a shut-down of the Radio Frequency field. On the other side this is sufficient too: If the initialization lasts at least 0.1 seconds then with expected entropy of $2^{56}$ bit the estimated time for a brute force attack will more than 200 million years.

### 6.1.4 Class FDP User Data Protection

#### 6.1.4.1 Access Control Policy (FDP_ACC)

114 **FDP_ACC.1 Subset access control – Terminal Access**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACF.1 Security attribute based access control |

| | |
|---|---|
| FDP_ACC.1.1 | The TSF shall enforce the Basic Access Control SFP [55] on terminals gaining write, read, modification access to data in EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD [56]. |

#### 6.1.4.2 Access Control Functions (FDP_ACF)

115 **FDP_ACF.1 Basic Security attribute based access control – Basic Access Control**

51 [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
52 [assignment: *list of authentication events*]
53 [selection: *met, surpassed*]
54 [assignment: *list of actions*]
55 [assignment: *access control SFP*]
56 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Hierarchical to: No other components.

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

FDP_ACF.1.1 The TSF shall enforce the Basic Access Control SFP[57] to objects based on the following:

1. Subjects:
   a. Personalization Agent,
   b. Basic Inspection System,
   c. Terminal;
2. Objects:
   a. data in EF.DG1 to EF.DG16 of the logical MRTD,
   b. data in EF.COM,
   c. data in EF.SOD;
3. Security attributes:
   a. Authentication status of terminals.[58].

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

1. the successfully authenticated Personalization Agent is allowed write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. a successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG5 to EF.DG16 of the logical MRTD[59].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[60].

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

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4[61].

116 *Application Note 27*: The inspection system needs special authentication and authorization for read access to DG3 and DG4 which is not defined in this protection profile (cf. [EACPassPP] for details).

57 [assignment: *access control SFP*]

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

59 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

60 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

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

### 6.1.4.3 Inter-TSF User Data Confidentiality Transfer Protection (FDP_UCT)

117 *Application Note 28*: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

118 **FDP_UCT.1 Basic data exchange confidentiality - MRTD**

| | |
|---|---|
| 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_UCT.1.1 | The TSF shall enforce the Basic Access Control SFP[62] to be able to transmit and receive[63] user data in a manner protected from unauthorized disclosure. |

119 *Application Note 29*: The SFR FDP_UCT.1 requires the use of secure messaging between the MRTD and the Basic Inspection System. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is also not applicable here.

### 6.1.4.4 Inter-TSF User Data Integrity Transfer Protection (FDP_UIT))

120 **FDP_UIT.1 Data Exchange Integrity - MRTD**

| | |
|---|---|
| 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 Basis Access Control SFP[64] to be able to transmit and receive[65] user data in a manner protected from modification, deletion, insertion and replay[66] errors. |
| FDP_UIT.1.2 | The TSF shall be able to determine on receipt of user data, |

62 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
63 [selection*: transmit, receive*]
64 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
65 [selection*: transmit, receive*]
66 [selection: *modification, deletion, insertion, replay*]

whether modification, deletion, insertion and replay[67] has occurred.

121 *Application Note 30*: The SFR FDP_UIT.1 requires the use of secure messaging between the MRTD and the Basic Inspection System. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is also not applicable here.

### 6.1.5 Class FMT Security Management

122 *Application Note 31*: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

#### 6.1.5.1 Specification of Management Functions (FMT_SMF)

123 **FMT_SMF.1 Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Initialization,
2. Pre-Personalization,
3. Personalization[68].

#### 6.1.5.2 Security Management Roles (FMT_SMR)

124 **FMT_SMR.1 Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Basic Inspection System[69].

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

67 [selection: *modification*, *deletion, insertion, replay*]
68 [assignment: *list of management functions to be provided by the TSF*]
69 [assignment: *the authorized identified roles*]

### 6.1.5.3 Limited Capabilities and Availability (FMT_LIM)

125 *Application Note 32*: 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.

126 **FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced:
Deploying Test Features after TOE Delivery do not allow,

1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[70].

127 **FMT_LIM.2 Limited availability**

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced:
Deploying Test Features after TOE Delivery do not allow,

1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[71].

128 *Application Note 33*: The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy. Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

70 [assignment: *Limited capability and availability policy*]
71 [assignment: *Limited capability and availability policy*]

### 6.1.5.4 Management of TSF data (FMT_MTD)

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMF.1 Specification of management functions<br>FMT_SMR.1 Security roles |
| FMT_MTD.1.1/ INI_ENA | The TSF shall restrict the ability to write[72] the Initialization Data and Pre-personalization Data[73] to the Manufacturer[74]. |

130 *Application Note 34*: 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.

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMF.1 Specification of management functions<br>FMT_SMR.1 Security roles |
| FMT_MTD.1.1/ INI_DIS | The TSF shall restrict the ability to disable read access for users to[75] the Initialization Data[76] to the Personalization Agent[77]. |

132 *Application Note 35:* 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 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 will to this data will be blocked. The MRTD Manufacturer will write the Pre-Personalization Data.

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

| | |
|---|---|
| Hierarchical to: | No other components. |

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

| | |
|---|---|
| Dependencies: | FMT_SMF.1 Specification of management functions<br>FMT_SMR.1 Security roles |
| FMT_MTD.1.1/<br>KEY_READ | The TSF shall restrict the ability to write[78] the Document Basic Access Keys[79] to the Personalization Agent[80]. |

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

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMF.1 Specification of management functions<br>FMT_SMR.1 Security roles |
| FMT_MTD.1.1/<br>KEY_READ | The TSF shall restrict the ability to read[81] the Document Basic Access Keys and Personalization Agent Keys [82] to none[83]. |

135 *Application Note 36:* The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

### 6.1.6 Class FPT Protection of the Security Functions

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

#### 6.1.6.1 TOE Emanation (FPT_EMS)

137 **FPT_EMS.1 TOE Emanation**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_EMS.1.1 | The TOE shall not emit *power variations, timing variations during command execution*[84] in excess of *non-useful information* [85] en- |

78 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
79 [assignment: *list of TSF data*]
80 [assignment: *the authorized identified roles*]
81 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
82 [assignment: *list of TSF data*]
83 [assignment: *the authorized identified roles*]

abling access to the *Personalization Agent Key(s)*[86] and *Basic Access Control Keys*[87].

FPT_EMS.1.2 The TSF shall ensure any unauthorized users[88] are unable to use the following interface smart card circuit contacts[89] to gain access to Personalization Agent Key(s)[90] and *Basic Access Control Keys*[91].

138 *Application Note 37*: The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well.

### 6.1.6.2 Fail Secure (FPT_FLS)

139 **FPT_FLS.1 Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
1. exposure to out-of-range operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1[92].

### 6.1.6.3 TSF Self Test (FPT_TST)

140 **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,*

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

| | |
|---|---|
| | *periodically during normal operation*[93] to demonstrate the correct operation of the TSF[94]. |
| FPT_TST.1.2 | The TSF shall provide authorized users with the capability to verify the integrity of TSF data[95]. |
| FPT_TST.1.3 | The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[96]. |

141 *Application Note 38*: The MRTD's chip uses state-of-the-art smart card technology, therefore it will run the some self tests at the request of an authorized user and some self tests automatically (cf. [HWST]). E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 is executed during initial start-up by the user Manufacturer in the life phase 'Manufacturing'. Other self tests automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation of a integrity check value as soon as data is accessed.

#### 6.1.6.4 TSF Physical Protection (FPT_PHP)

142 **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[97] to the TSF[98] by responding automatically such that the SFRs are always enforced. |

143 *Application Note 39*: 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' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

## 6.2 Security Assurance Requirements for the TOE

144 The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following components:

93 [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions* [assignment: *conditions under which self test should occur*]]
94 [selection: [assignment: *parts of TSF*], *the TSF*]
95 [selection: [assignment: *parts of TSF*], *TSF data*]
96 [selection: [assignment: *parts of TSF*], *TSF*]
97 [assignment: *physical tampering scenarios*]
98 [assignment: *list of TSF devices/elements*]

- ALC_DVS.2 (Sufficiency of security measures),

## 6.3 Security Requirements Rationale

### 6.3.1 Security Functional Requirements Rationale

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

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

| | OT.AC_Pers | OT.Data_Int | OT.Data_Conf | OT.Identification | OT.Prot_Inf_Leak | OT.Prot_Phys-Tamper | OT.Prot_Malfunction | OT.Prot_Abuse-Func |
|---|---|---|---|---|---|---|---|---|
| FPT_TST.1 | x | | | | x | | x | |
| FPT_PHP.3 | x | | | | x | x | | |

**Table 6: Coverage of Security Objectives for the TOE by SFR**

146 The detailed discussion of the coverage given in this table is already provided by the Protection Profile [BACPassPP]. Therefore it is not necessary to duplicate it in the ST that claims strict conformance to this PP.

### 6.3.2 Rationale for SFR's Dependencies

147 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.

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

| No. | SFR-component from the PP | Dependencies assumed | Supported/fulfilled by SFR |
|---|---|---|---|
| 1 | FAU_SAS | No dependencies | n.a. |
| 2 | FCS_CKM.1 | FCS_CKM.2 or FCS_COP.1<br>FCS_CKM.4 | FCS_COP.1/ENC and FCS_COP.1/MAC<br>FCS_CKM.4 |
| 3 | FCS_CKM.4 | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | FCS_CKM.1 |
| 4 | FCS_COP.1/SHA | FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | See justification 1 of [BACPassPP, p. 54]<br>FCS_CKM.4 |
| 5 | FCS_COP.1/ENC | FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | FCS_CKM.1<br>FCS_CKM.4 |
| 6 | FCS_COP.1/AUTH | FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | See justification 2 of [BACPassPP, p. 54]<br>See justification 2 of [BACPassPP, p. 54] |
| 7 | FCS_COP.1/MAC | FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | FCS_CKM.1<br>FCS_CKM.4 |
| 8 | FCS_RND.1 | No dependencies | n.a. |
| 9 | FIA_AFL.1 | FIA_UAU.1 | FIA_UAU.1 |
| 10 | FIA_UID.1 | No dependencies | n.a. |
| 11 | FIA_UAU.1 | FIA_UID.1 | FIA_UID.1 |

| No. | SFR-component from the PP | Dependencies assumed | Supported/fulfilled by SFR |
|---|---|---|---|
| 12 | FIA_UAU.4 | No dependencies | n.a. |
| 13 | FIA_UAU.5 | No dependencies | n.a. |
| 14 | FIA_UAU.6 | No dependencies | n.a. |
| 15 | FDP_ACC.1 | FDP_ACF.1 | FDP_ACF.1 |
| 16 | FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | FDP_ACC.1<br>See justification 3 of [BACPassPP, p. 54] |
| 17 | FDP_UCT.1 | [FTP_ITC.1 or FTP_TRP.1]<br>[FDP_IFC.1 or FDP_ACC.1] | See justification 4 of [BACPassPP, p. 55]<br>FDP_ACC.1 |
| 18 | FDP_UIT.1 | [FTP_ITC.1 or FTP_TRP.1]<br>[FDP_IFC.1 or FDP_ACC.1] | See justification 4 of [BACPassPP, p. 55]<br>FDP_ACC.1 |
| 19 | FMT_SMF.1 | No dependencies | n.a. |
| 20 | FMT_SMR.1 | FIA_UID.1 | FIA_UID.1 |
| 21 | FMT_LIM.1 | FMT_LIM.2 | FMT_LIM.2 |
| 22 | FMT_LIM.2 | FMT_LIM.1 | FMT_LIM.1 |
| 23 | FMT_MTD.1/INI_ENA | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 |
| 24 | FMT_MTD.1/INI_DIS | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 |
| 25 | FMT_MTD.1/KEY_WRITE | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 |
| 26 | FMT_MTD.1/KEY_READ | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1<br>FMT_SMR.1 |
| 27 | FPT_EMS.1 | No dependencies | n.a. |
| 28 | FPT_FLS.1 | No dependencies | n.a. |
| 29 | FPT_TST.1 | No dependencies | n.a. |
| 30 | FPT_PHP.3 | No dependencies | n.a. |

**Table 7: Dependencies between the SFRs**

149 The justification of non-satisfied dependencies is given in the Protection Profile ([BACPassPP]). Therefore it is not necessary to duplicate it in this ST.

### 6.3.3 Security Assurance Requirements Rationale

150 The current assurance package was chosen based on the pre-defined assurance package EAL4. This package permits 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 retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where develo-

pers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

151 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 sensitive material.

152 The set of *assurance* requirements being part of EAL4 fulfils all dependencies a priori.

153 The augmentation of EAL4 chosen has no dependencies to other security requirements.

### 6.3.4 Security Requirements – Internal Consistency

154 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 an internally consistent whole.

155 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 Rationale for SFR's Dependencies for the security functional requirements shows that the basis for 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.

All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behavior of these 'shared' items.

The assurance package EAL4 is a pre-defined set of 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 internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

156 Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met, a possibility having been shown not to arise in sections 6.3.2 Rationale for SFR's Dependencies 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, there are no inconsistencies between the goals of these two groups of security requirements.

# 7 TOE Summary Specification

157 This section presents an overview of the security functionalities implemented by the TOE and the assurance measures applied to ensure their correct implementation.

158 According to the SFRs the TOE provides the following functionalities

- Access control to the User Data stored in the TOE
- Secure data exchange between the MRTD and the Service Provider connected
- Identification and authentication of users and components
- Audit
- Management of and access to TSF and TSF-data
- Reliability of the TOE Security Functionality

159 They represent the functional description of the feature overview in section 1.3.1. The TOE Summary Specification will be given in more detail in the following sections. Further technical information how the security functions actually implement the TOE security functional requirements, which TOE modules realize which functions is contained in the Security architecture Description (ADV_ARC), the Functional Specification (ADV_FSP) and the TOE Design Specification (ADV_TDS).

## 7.1 Access Control to the User Data Stored in the TOE

160 The access to User Data is restricted according to the SFRs FDP_ACC.1 and FDP_ACF.1. Basic Inspection Terminal is assigned dedicated access rights after successful authentication protocol (cf. section 7.3) supported by FIA_UAU.1.

## 7.2 Secure Data Exchange

161 The secure data exchange is supported by fulfilling FCS_COP.1/ENC giving confidentiality by data encryption/decryption and FCS_COP.1/MAC providing integrity. The quality and the authenticity of the key used base on the Personalization data. The achieved level of trust is maintained as long as the secure channel is not broken.

## 7.3 Identification and Authentication of Users and Components

162 The identification and authentication protocol is based on the knowledge of the MRZ. The Basic Access Control is described in the [ICAO9303-1], where the corresponding steps are considered and recognized as appropriate. Identification and authentication is provided for terminals (FIA_UID.1, FIA_UAU.1). Additionally the TOE supports the identification and authentication of the Personalization Agent based the Mutual Authentication Commands (FCS_COP.1/AUTH, FIA_UAU.5).

163 The TOE authenticates and re-authenticates the user, required in FIA_UAU.4, FIA_\ UAU.5 and FIA_UAU.6. It concerns the protocol data, prevents re-use and how the security state, e.g. a specified role (FMT_SMR.1) of an identified and authenticated user is achieved and maintained. The exchanged data is, based on Basic Access Control, protected against disclosure (FDP_UCT.1) and integrity violations (FDP_UIT.1).

164 To prevent brute-force attacks after a failure the authentication with Basis Access Control Keys is blocked at least for a time that is required for initialization (FIA_AFL.1). Because the MRZ carry enough entropy this is sufficient for the operational use of the TOE.

165 The security and the reliability of the identification and authentication is supported by the correct key agreement (FCS_CKM.1, FCS_COP.1/SHA) and the quality of random numbers (FCS_RND.1) used by the MRTD and the terminal. As the authentication state is left, the session keys cannot be used anymore (FCS_CKM.4).

## 7.4 Audit

166 The Manufacturer shall control the TOE production and must also file audit records (FAU_SAS.1). This is supported by FMT_MTD.1/INI_ENA (writing initialization and pre-personalization data) and is disabled for the Operational Phase (FMT_MTD.1/INI_DIS) by the Personalization Agent.

## 7.5 Management of and Access to TSF and TSF-data

167 The management and the access to the TOE security functions and the TSF data is controlled by the entire functionality class FMT. During Initialization, Personalization and in the Operational Phase of the Life Cycle Phases the Operation System of the TOE provides the management functions for identified roles (FMT_SMF.1, FMT_SMR.1) and maintain all the access rules over the life cycle of the TOE and even before the production of the TOE is finished during Initialization and Pre-personalization (FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). The test features necessary during initialization are no more available after TOE delivery (FMT_LIM.1, FMT_LIM.2).

168 After delivery the TOE is personalized (FMT_MTD.1, FMT_MTD.1/KEY_WRITE), the Basic Access Control Keys can only be used but never accessed else (FMT_MTD.1/ KEY_READ).

## 7.6 Reliability of the TOE Security Functionality

169 The operating system of the TOE protects the security functionality of the TOE as soon as it installed during Initialization Phase. The TOE will not emit physical or logical data information on security User Data outside the secure channels controlled by the operating system (FPT_EMS.1).

170 The TOE will resist physical manipulation and probing (FPT_PHP.3) and enter a secure state in case a failure occur (FPT_FLS.1). This functionality is supported also by the hardware, which was approved in a separate evaluation process.

171 The TOE will permanently run tests to maintain the correct operation of the TOE security functions and the achieved security level (FPT_TST.1).

172 This functionality is supported by the entire class FMT.

## 7.7 TOE SFR Statements

173 For the sake of completeness the TOE Summary Specification of the previous sections is re-ordered once again. All the TOE SFR statements are listed and it is described how

they are fulfilled by the TOE. If applicable appropriate requirements are handled together to avoid needless text duplication.

174 FAU_SAS.1: The IC Identification Data can be read by the successfully authenticated Manufacturer, which allows the Manufacturer to store this data in audit records. After Personalization the read access to IC Identification Data is disabled.

175 FCS_CKM.1: The cryptographic key generation used in the BAC protocol is defined in [ICAO9303-1]. The algorithm uses high quality random numbers generated by the TSF (FCS_RND.1).

176 FCS_CKM.4: Each session key is used only by the authenticated user and is destroyed if the authentication fails or is restarted again. Additionally in case of loss of power the keys are also erased, because they are not stored permanently.

177 FCS_COP.1/SHA: The hash function is used for key derivation. The recently discovered collision attacks are not relevant for this application.

178 FCS_COP.1/ENC: The TDES algorithm provides a medium level of security, which is sufficient for the Basic Access Control Protocol. Sensitive biometric data are not accessible for this authentication level (FDP_ACF.1). Nevertheless no exploitable weakness of the TDES algorithm is known except the effective key length of 112 bits.

179 FCS_COP.1/AUTH: The symmetric authentication of the Personalization Agent is based on the AES algorithm. It provides a high level of security based on 128 bit keys.

180 FCS_COP.1/MAC: The Retail-MAC algorithm is a standardized secure message authentication algorithm. It is sufficient for the Basic Access Control Protocol. Sensitive biometric data are not accessible for this authentication level (FDP_ACF.1).

181 FCS_RND.1: The randomness of values for challenges or ephemeral or permanent keys bases on the underlying hardware TSF. Its Random Number Generator claims the functionality class PTG.2 according to [AIS31]. This includes also the fulfillment of the online test requirements. A cryptographic post-processing guarantees that statistical tests cannot practically distinguish between generated values and an ideal random number generator.

182 FIA_AFL.1: The Basic Access Control Keys carry entropy of about 56 bits, if the Document Number is selected randomly. To prevent brute force attacks at the user data it is sufficient to block the execution of any command for a time of at least 0.1 seconds. Even with the entropy of the Document Number (9 alpha-numeric digits) only a brute force attack will last some thousand years.

183 FIA_UID.1, FIA_UAU.4: The access rules allow establishing a communication channel before the user is authenticated. After successful authentication based on the knowledge of the Basic Access Control Keys (Terminal) or a symmetric authentication key (Personalization Agent) a security status is maintained. Based on that status the access rules apply that allow or disallow the execution of commands and the access to security data controlled by the Operating System of the TOE.

184 FIA_UAU.5: The authentication of the Manufacturer, a Personalization Agent and a Terminal is controlled by the Access Rules laid down in the Operating System in a very early stage of the life cycle. Even if the file system is not available, the Initialization Data can only be written by a successfully authenticated user (in a Manufacturer's role). The authentication attempts as Personalization Agent can be based on Symmetric Authentication Mechanism with the Personalization Agent Key and the Terminal Authentication Protocol with Personalization Agent Keys. The high entropy of the Symmetric Keys used herein guarantees the reliability of these authentications.

185 FIA_UAU.6: The TOE guarantees based on the inherent MAC verification in the secure messaging mechanism that the re-authentication of the user or component (Personalization Agent, Terminal) is possible for every command after successful authentication.

186 FDP_ACC.1: The Terminal Access Control SFP access rules are fixed in the Operating System of the TOE; it cannot be changed nor bypassed.

187 FDP_ACF.1: The access control rules of FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE.

188 FDP_UCT.1, FDP_UIT.1: The TOE operating system controls the secure channel established after the Basic Access Control protocol. The security level is maintained until a command outside the channel is received. After the secure channel is broken, the encryption and authentication keys cannot be used anymore.

189 FMT_SMF.1, FMT_SMR.1: Maintaining the different roles and TSFs of the TOE using dedicated access rules cannot be changed or disabled in the Operating System. The assignment of a specific role is supported by a successful authentication and the following-up Secure Messaging. The embedded software (i.e. the operating system) enforces the application of the access rules before any function is allowed to proceed.

190 FMT_LIM.1, FMT_LIM.2: Limitations of capabilities or availability are enforced by the Operating System of the TOE controlling the integrity of the stored access rules and the used functions. After Initialization all data testing-specific commands and actions are disabled. It is not possible to override these controls and restore them for use.

191 FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS: Initialization Data is used for audit log of a pre-personalized TOE. It is stored in the TOE, but the access to this information is disabled as soon as the TOE is personalized.

192 FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ: The Basic Access Control Keys are objects under access control that is fixed in the file system. The can be written during Personalization only and can never be changed or read in the operational phase.

193 FPT_EMS.1: The Operating System of the TOE monitors the regular execution of commands, and if variations occur with test failures or integrity mismatch the communication is closed. The strict care of uniformity and non-overloading single components is implemented in the Operating System and will be described detailed in ADV and AVA documentation. This implies the leakage of information about the Personalization Agent Authentication Key and the Chip Authentication Key.

194 FPT_FLS.1: The Operating System of the TOE guarantees that the TOE preserves a secure state if a test failure or integrity check mismatch occur

195 FPT_TST.1: The self tests of the underlying hardware and additional test maintained by the TOE provide the means for demonstrating that the TSF operation is correct and that the data is not manipulated.

196 FPT_PHP.3: The Operating System of the TOE monitors the regular execution of commands, and if variations occur with test failures or integrity mismatch the communication will be closed immediately.

## 7.8 Statement of Compatibility

197 This is the statement of compatibility between this Composite Security Target and the Security Target Chip of the underlying hardware [HWST].

### 7.8.1 Relevance of Hardware TSFs

198 In the following lists the relevance of the hardware security services (SS) and functions (SF) for the composite security target is considered.

**Relevant:**

- SS.RNG: Random Number Generator
- SS.HW_AES: Triple-AES Co-processor
- SS.HW_DES: Triple-DES Co-processor
- SS.CRC: Cyclic Redundancy Check
- SF.OPC: Control of Operating Conditions
- SF.PHY: Protection against Physical Manipulation
- SF.LOG: Logical Protection
- SF.MEM_ACC: Memory Access Control
- SF.SFR_ACC: Special Function Register Access Control

**Not relevant:**

- SS.RECONFIG: Customer Reconfiguration
- SF.COMP: Protection of Mode Control
- SF.FFW: Firmware Firewall
- SF.FIRMWARE: Firmware Support

### 7.8.2 Security Requirements

199 The relevant Security Requirements of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

**Security Functional Requirements related to the Composite ST:**

- FAU_SAS.1 matches FAU_SAS.1 of [HWST]
- FCS_CKM.1 not relevant
- FCS_CKM.4 no conflicts
- FCS_COP.1/SHA not relevant
- FCS_COP.1/ENC matches FCS_COP.1[HW_DES] of [HWST]
- FCS_COP.1/AUTH matches FCS_COP.1[HW_AES] of [HWST]
- FCS_COP.1/MAC matches FCS_COP.1[HW_DES] of [HWST]
- FCS_RND.1 matches FCS_RNG.1 of [HWST]
- FIA_AFL.1 no conflicts

- FIA_UID.1 no conflicts
- FIA_UAU.1 no conflicts
- FIA_UAU.4 no conflicts
- FIA_UAU.5 no conflicts
- FIA_UAU.6 no conflicts
- FDP_ACC.1 not relevant
- FDP_ACF.1 not relevant
- FDP_UCT.1 no conflicts
- FDP_UIT.1 no conflicts
- FMT_SMF.1 no conflicts
- FMT_SMR.1 not relevant
- FMT_LIM.1 matches FMT_LIM.1 of [HWST]
- FMT_LIM.2 matches FMT_LIM.2 of [HWST]
- FMT_MTD.1/INI_ENA not relevant
- FMT_MTD.1/INI_DIS not relevant
- FMT_MTD.1/KEY_WRITE not relevant
- FMT_MTD.1/KEY_READ not relevant
- FPT_EMS.1 is supported by the Security Feature SF.OPC of the hardware ([HWST]) and the AVA_VAN.5 evaluation
- FPT_FLS.1 matches FPT_FLS.1 of [HWST]
- FPT_TST.1 no conflicts
- FPT_PHP.3 matches FPT_PHP.3 of [HWST]

**Security Functional Requirements of the hardware**

- FAU_SAS.1 covered by FAU SAS.1 of the Composite ST
- FCS_COP.1[HW_AES] covered by FCS_COP.1/AUTH of the Composite ST
- FCS_COP.1[HW_DES] covered by FCS_COP.1/ENC and FCS_COP.1/MACFCS_RNG.1[HW] matches FCS_RND.1 of the Composite ST
- FDP_ACC.1 [MEM] and [SFR] (Subset access control) is not relevant for the TOE, but for the implementation of the OS, therefore it is covered by ADV_IMP.1 (Implementation representation of the TSF)
- FDP_ACF.1 [MEM] and [SFR] (Security attribute based access control) is not relevant for the TOE, but for the implementation of the OS, therefore it is covered by ADV_IMP.1 (Implementation representation of the TSF
- FDP_ITT.1[HW] is covered by FPT_EMS.1 of the Composite ST
- FDP_IFC.1 is covered by FPT_EMS.1 of the Composite ST
- FMT_SMF.1 is covered by FMT_SMF.1 of the Composite ST
- FMT_LIM.1 is covered by FMT_LIM.1 of Composite ST
- FMT_LIM.2 is covered by FMT_LIM.2 of Composite ST
- FMT_MSA.1 [MEM] and [SFR] no conflicts
- FMT_MSA.3 [MEM] and [SFR] no conflicts

- FPT_FLS.1 matches FPT_FLS.1 of the Composite ST
- FPT_ITT.1[HW] is covered by FPT_EMS.1 of the Composite ST
- FPT_PHP.3 is covered by FPT_FLS.1 and FPT_PHP.3 of the Composite ST
- FDP_SDI.2[HW] concerns the hardware operation, does not conflict with SFRs of the TOE
- FRU_FLT.2 concerns the hardware operation, does not conflict with SFRs of the TOE

**Security Assurance Requirements**

200 The level of assurance of the TOE is EAL 4 augmented with ALC_DVS.2.

201 The chosen level of assurance of the hardware is EAL 6 augmented with ALC_FLR.1 and ASE_TSS.2. This includes ALC_DVS.2, ATE_DPT.3 and AVA_VAN.5.

202 This shows that the Assurance Requirements of the TOE matches the Assurance Requirements of the hardware.

203 The Security Objectives of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

### 7.8.3 Security Objectives for the Composite ST of the TOE:

- OT.Data_Int covers O.HW_DES3 of the [HWST]
- OT.Data_Conf covers O.HW_DES3 of the [HWST]
- OT.AC_Res no conflict
- OT.Identification matches O.Identification from [ICPP]
- OT.Prot_Abuse-Func covers O.Abuse-Func from [ICPP]
- OT.Prot_Inf_Leak covers O.Leak-Inherent and O.Leak-Forced from [ICPP]
- OT.Prot_Phys-Tamper covers O.Phys-Probing and O.Phys-Manipulation from [ICPP]
- OT.Prot_Malfunction matches O.Malfunction from [ICPP]

**Security Objectives for the hardware ([ICPP] and [HWST]):**

- O.Leak-Inherent (Protection against Inherent Information Leakage) is covered by OT.Prot_Inf_Leak
- O.Phys-Probing (Protection against Physical Probing) is mapped to OT.Prot_Phys-Tamper
- O.Malfunction (Protection against Malfunctions) is covered by the corresponding objective OT.Prot_Malfunction
- O.Phys-Manipulation (Protection against Physical Manipulation) is mapped to OT.Prot_Phys-Tamper
- O.Leak-Forced (Protection against Forced Information Leakage) is covered by OT.Prot_Inf_Leak

- O.Abuse-Func (Protection against Abuse of Functionality) is covered by the corresponding objective OT.Prot_Abuse-Func
- O.Identification (Hardware Identification) covered by OT.Identification, which is relevant for the pre-operational phases
- O.RND (Random Numbers) is covered by Security Objectives OT.Data_Int, and OT.Data_Conf.

  The objectives of the TOE address the integrity and confidentiality of transmitted data, based on the protocols of Terminal and Chip Authentication, depending on a high cryptographic quality of random number generation.
- O.INTEGRITY_CHK Integrity control of transferred data

  The hardware provides a security service for stored data integrity checks and an operation control feature for data transfer, both used by the TOE. As it concerns the hardware reliability it is mapped to OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.
- O.HW_DES3 (Triple DES Functionality) is mapped to OT.Data_Int, and OT.Data_Conf.

  The TDES (DES3) Functionality is used to ensure the integrity and the confidentiality of personal data during transmission.
- O.HW_AES (AES Functionality) The AES Functionality is used to ensure the correct authentication of the Personalization Agent and is not relevant in the Operational Use Phase.
- O.CUST_RECONFIG: Customer Option Reconfiguration (not relevant)

  This functionality is not used in TOE's OS.
- O.EEPROM_INTEGRITY: Integrity support of data stored in EEPROM

  The hardware shall provide a mechanism to support the integrity of the data stored in the EEPROM. This objective is mapped due to the used in hardware security features to OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.
- O.FM_FW (MIFARE Firewall) not relevant
- O.MEM_ACCESS is mapped to OT.Prot_Abuse-Func

  This objective for the hardware supports the correct operation of the TOE providing memory area access control.
- O.SFR_ACCESS is mapped to OT.Prot_Abuse-Func

  The objectives O.MEM_ACCESS and O.SFR_ACCESS support the correct operation of the TOE providing memory area access and Special Function Registers access control. Therefore these objectives are mapped to OT.Prot_Abuse-Func.

### 7.8.4 Compatibility: TOE Security Environment

**Assumptions**

204 The following list shows that assumptions neither of the TOE nor of the hardware have any conflicts between each other. They are either not relevant for this Security Target or are covered by appropriate Security Objectives.

**Assumptions of the Composite ST:**

A.MRTD_Manufact is related to manufacturing phases (4 to 6) after Initialization and is not conflicting to earlier phases.

A.MRTD_Delivery is related to manufacturing phases (4 to 6) after Initialization and is not conflicting to earlier phases.

A.MRTD_Pers_Agent is an assumption for the operating environment, and is therefore not conflicting to earlier life cycle phases.

A.Insp_Sys is an assumption for the operating environment, and is therefore not conflicting to earlier life cycle phases.

A.BAC-Keys is an assumption for the operating environment, and is therefore not conflicting to earlier life cycle phases.

**Assumptions of the Hardware PP ([ICPP]):**

A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization) is not relevant, because the Personalization of the hardware is finished after Initialization Phase.

A.Plat-Appl (Usage of Hardware Platform) not relevant

A.Resp-Appl (Treatment of User Data ) This assumption is covered by the hardware's objective for the environment OE.Resp-Appl, which addresses the Security User Data objects of the TOE. This assumption is covered by OT.Data_Int, OT.Data_Conf and OT.Prot_Inf_Leak of the TOE and OE.Personalization of TOE's environment

**Assumptions of the specific hardware platform ([HWST]):**

- A.Check-Init (Check of Initialization Data by the Security IC Embedded Software)

  The Check of Initialization Data of the hardware is related to the Life Cycle Phase 2 "Manufacturing of the TOE" and should not be confused with the check of Initialization Data during Personalization. The Assumption A.Check-Init is no more relevant after TOE Initialization, because Hardware Initialization Data is overridden by TOEs Initialization and Pre-Personalization Data.

- A.Key-Function (Usage of Key-dependent Functions)

  This assumption requires that key-dependent functions are implemented in the OS such that they are not susceptible to leakage attacks. It is covered by the Hardware's objective OE.Resp-Appl for the environment and applies to Life Cycle Phase 1 "Development".

### Threats

205 The Threats of the TOE and the hardware can be mapped or are not relevant. They show no conflict between each other.

### Threats of the Composite ST:

- T.Chip_ID no conflict
- T.Skimming no conflict
- T.Eavesdropping no conflict
- T.Forgery covers T.RND of the Smartcard IC PP [ICPP]
- T.Abuse-Func matches the corresponding threat of the of the Smartcard IC PP [ICPP]
- T.Information_Leakage matches T.Leak-Inherent and T.Leak-Forced of the Smartcard IC PP [ICPP]
- T.Phys-Tamper matches T.Phys-Probing and T.Phys-Manipulation of the Smartcard IC PP [ICPP]
- T.Malfunction matches corresponding threat of the Smartcard IC PP [ICPP]

### Threats of the hardware ST ([ICPP]):

- T.Leak-Inherent matches T.Information_Leakage of the Composite ST
- T.Phys-Probing matches T.Phys-Tamper of the Composite ST
- T.Malfunction matches corresponding threat of the Composite ST
- T.Phys-Manipulation matches T.Phys-Tamper of the Composite ST
- T.Leak-Forced matches T.Information_Leakage of the Composite ST
- T.Abuse-Func matches corresponding threat of the Composite ST
- T.RND is related to T.Information_Leakage and T.Forgery of the Composite ST. An attacker predicting the output of the random number generator due its deficiency can disclose confidential User Data or data exchanged between the TOE and an Inspection System.

### Threats of the hardware ST ([HWST]):

T.Unauthorized_Access Unauthorised Memory or Hardware Access

An attacker may try to read, modify or execute code or data stored in restricted memory areas. And or or an attacker may try to access or operate hardware resources that are restriced by executing code that accidentally or deliberately accesses this restricted hardware resources. This threat is related to the partitioning of memory areas in Firmware Mode, System Mode and the segmentation of memory areas in User Mode. This threat is covered by the objectives O.FW_HW, O.MEM_ACCESS, O.SFR_ACCESS of the

Hardware ([HWST]] and may be considered as part of the threat T.Abuse-Func Protection Profile.

### 7.8.5 Organizational Security Policies

206 The Organizational Security Policies of the TOE and the hardware have no conflicts between each other. They are shown in the following list.

**Organizational Security Policies of the Composite ST of the TOE:**

- P.Manufact covers P.Process-TOE of the hardware ST
- P.Personalization no conflict
- P.Personal_data no conflict

**Organizational Security Policies of the Hardware ST:**

- P.Add-Components (Additional Specific Security Components) no conflict

  The TOE's hardware provides AES/TDES encryption/decryption, Area based Memory Access Control, Memory separation for different software parts and Special Function Register Access Control as security functionalities to the Security IC Embedded Software. They are used in security functionalities of the TOE and are considered in the implementation of the OS. The AES support is used for authentication purposes only.
- P.Process-TOE ([ICPP]) is covered by P.Manufact of the Composite ST

### 7.8.6 Conclusion

207 No contradictions between the Security Targets of the TOE and the underlying hardware can be found.

## 7.9 Assurance Measures

208 The documentation is produced compliant to the Common Criteria Version 3.1. The following documents provide the necessary information to fulfill the assurance requirements listed in section 6.2.

Development
- ADV_ARC.1 Security Architecture Description TCOS Passport 2.1
- ADV_FSP.4 Functional Specification TCOS Passport 2.1
- ADV_IMP.1 Implementation of the TSF TCOS Passport 2.1
- ADV_TDS.3 Modular Design of TCOS Passport 2.1

Guidance documents
- AGD_OPE.1 User Guidance TCOS Passport 2.1
- AGD_PRE.1 Administrator Guidance TCOS Passport 2.1

Life-cycle support
- ALC_CMC.4, ALC_CMS.4 Documentation for Configuration Management
- ALC_DEL.1 Documentation for Delivery and Operation TCOS Passport 2.1
- ALC_LCD.1 Life Cycle Model Documentation TCOS Passport 2.1
- ALC_TAT.1, ALC_DVS.2 Development Tools and Development Security for TCOS Passport 2.1

Tests
- ATE_COV.2, ATE_DPT.1 Test Documentation for TCOS Passport 2.1
- ATE_FUN.1 Test Documentation of the Functional Testing TCOS Passport 2.1

Vulnerability assessment
- AVA_VAN.3 Focused Vulnerability Analysis TCOS Passport 2.1

209 The developer team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, user documentation, administrator documentation, and security flaws. The security of the configuration management is described in detail in a separate document.

210 The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developer's master copy and the user's version. The Administrator and the User are provided with necessary documentation for initialization and start-up of the TOE.

211 The implementation is based on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements.

212 The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life-cycle model of the TOE. The development tools are well-defined and use semi-formal methods, i.e. a security model.

213 The development department is equipped with organizational and personnel means that are necessary to develop the TOE. The testing and the vulnerability analysis require technical and theoretical know-how available at T-Systems International GmbH.

214 As the evaluation is identified as a composite evaluation based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.

# Appendix Glossary and Acronyms

215 This is the unchanged chapter from [BACPassPP], more detailed information can be found there, too.

## Glossary

| *Term* | Definition |
|---|---|
| *Active Authentication* | Security mechanism defined in [ICAO9303-1] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization. |
| *Application note* | Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE. |
| *Audit records* | Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data. |
| *Authenticity* | Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization |
| *Basic Access Control (BAC)* | Security mechanism defined in [ICAO9303-1] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there). |
| *Basic Inspection System (BIS)* | An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD. |
| *Biographical data (bio-data)* | The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO9303-1] |
| *Biometric reference data* | Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data. |
| *Counterfeit* | An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO9303-1] |
| *Country Signing CA Certificate ($C_{CSCA}$)* | Self-signed certificate of the Country Signing CA Public Key ($K_{PuCSCA}$) issued by CSCA stored in the inspection system. |
| *Document Basic Access Keys* | Pair of symmetric (two-key) 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 [ICAO9303-1]. 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. |
| *Document Security Object ($SO_D$)* | 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 ($C_{DS}$). [ICAO9303-1] |
| *Eavesdropper* | A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip. |
| *Enrolment* | The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO9303-1] |
| *Extended Access Control* | Security mechanism identified in [6] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data. |
| *Extended Inspection System (EIS)* | A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism. |
| *Forgery* | Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO9303-1] |
| *Global Interoperability* | The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability |

| *Term* | **Definition** |
|---|---|
| | is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO9303-1] |
| *IC Dedicated Support Software* | That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases. |
| *IC Dedicated Test Software* | That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter. |
| *IC Identification Data* | The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. |
| *Impostor* | A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO9303-1] |
| *Improperly documented person* | A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa |
| *Initialization* | Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.2, TOE life cycle, Phase 2, Step 3). |
| *Initialization Data* | Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data). |
| *Inspection* | The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO9303-1] |
| *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. |
| *Integrated circuit (IC)* | Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit. |
| *Integrity* | Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization |
| *Issuing Organization* | Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO9303-1] |
| *Issuing State* | The Country issuing the MRTD. [ICAO9303-1] |
| *Logical Data Structure (LDS)* | The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO9303-1]. The capacity expansion technology used is the MRTD's chip. |
| *Logical MRTD* | Data of the MRTD holder stored according to the Logical Data Structure [ICAO9303-1] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16) (6) EF.COM and EF.SOD |
| *Logical travel document* | Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional). |
| *Machine readable travel document (MRTD)* | 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. [ICAO9303-1] |
| *Machine readable visa (MRV)* | A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [ICAO9303-1] |
| *Machine readable zone (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. [ICAO9303-1] |
| *Machine-verifiable bio-metrics feature* | A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO9303-1] |
| *MRTD application* | Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes (i) the file structure implementing the LDS [ICAO9303-1], (ii) the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to |

| *Term* | **Definition** |
|---|---|
| | EF.DG14, EF.DG 16, EF.COM and EF.SOD) and (iii) the TSF Data including the definition the authentication data but except the authentication data itself. |
| *MRTD Basic Access Control* | Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS. |
| *MRTD holder* | The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD. |
| *MRTD's Chip* | A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [7], p. 14. |
| *MRTD's chip Embedded Software* | Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle. |
| *Optional biometric reference data* | Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data. |
| *Passive authentication* | (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. |
| *Personalization* | The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. sec. 1.2, TOE life cycle, Phase 3, Step 6). |
| *Personalization Agent* | The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder. |
| *Personalization Agent Authentication Information* | TSF data used for authentication proof and verification of the Personalization Agent. |
| *Personalization Agent Key* | Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6. |
| *Physical travel document* | Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data. |
| *Pre-Personalisation* | Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the MRTD Application (cf. sec. 1.2, TOE life cycle, Phase 2, Step 5) |
| *Pre-personalization Data* | Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair. |
| *Pre-personalized MRTD's chip* | MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip. |
| *Primary Inspection System (PIS)* | An inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism. |
| *Random identifier* | Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability. |
| *Receiving State* | The Country to which the Traveler is applying for entry. [ICAO9303-1] |
| *Reference data* | Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt. |
| *Secondary image* | A repeated image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO9303-1] |
| *Secure messaging in encrypted mode* | Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 |
| *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. |
| *Travel document* | A passport or other official document of identity issued by a State or Organization, which may |

| *Term* | Definition |
|---|---|
| | be used by the rightful holder for international travel. [ICAO9303-1] |
| *Traveler* | Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder. |
| *TSF data* | Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]). |
| *Unpersonalized MRTD* | The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer. |
| *User data* | Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]). |
| *Verification* | The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO9303-1] |
| *Verification data* | Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity. |

## Acronyms

| Acronym | Term |
|---|---|
| *BIS* | Basic Inspection System |
| *CC* | Common Criteria |
| *EF* | Elementary File |
| *GIS* | General Inspection System |
| *ICCSN* | Integrated Circuit Card Serial Number. |
| *MF* | Master File |
| *n.a.* | not applicable |
| *OSP* | Organizational security policy |
| *PP* | Protection Profile |
| *PT* | Personalization Terminal |
| *SAR* | Security assurance requirements |
| *SFR* | Security functional requirement |
| *TOE* | Target of Evaluation |
| *TLA* | three letter acronym |
| *TSF* | TOE security functions |

# Appendix Results of Cryptographic Assessment

216 The following cryptographic algorithms are used by the TOE to enforce its security policy:

| # | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Standard of Application | Comments |
|---|---|---|---|---|---|---|
| 1. | Authenticity | Symmetric Authentication of the Personalisation Agent, AES | [FIPS197] | \|k\|=128 | [EACTR] | FCS_COP.1/AUTH |
| 2. | Key Agreement | BAC Key Derviation SHA-1 | [FIPS 180] | - | [EACTR] | FCS_COP.1/SHA |
| 3. | | Document Basic Access Key Derivation Algorithm | [ICAO9303-1] normative appendix 5 | - | [EACTR] | FCS_CKM.1 |
| 4. | Confidentiality | Secure Messaging, TDES in CBC mode | [FIPS46] | \|k\|=112 | [EACTR] | FCS_COP.1/ENC |
| 5. | Integrity | Secure Messaging, TDES in Retail-MAC mode | [FIPS46] | \|k\|=112 | [EACTR] | FCS_COP.1/ MAC |
| 6. | Cryptographic Primitive | Hash for key derivation SHA-1 | [FIPS 180] | n.a. | [EACTR] | FCS_COP.1/SHA |
| 7. | Cryptographic Primitive | PTG.2 Random number generator | [AIS31] | n.a. | [ECARDTR] | FCS_RND.1 |
| 8. | Cryptographic Primitive | Hybrid deterministic RNG DRG.4 | [AIS31] | n.a. | [ECARDTR] | FCS_RND.1 |

**Table 8: Cryptographic algorithms used by TCOS Passport**

217 All cryptographic algorithms listed in table 8 are implemented by the TOE because of the standards building the TOE application (e.g. [EACTR]). For that reason an explicit validity period is not given.

218 The strength of the cryptographic algorithms was not rated in the course of this evaluation. According to Technical Guideline [EACTR], the algorithms are suitable for securing integrity, authenticity and confidentiality of the stored data for machine readable travel documents (MRTDs).

# References

[AIS31]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), A proposal for Functionality classes for random number generators Version 2.0 vom 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS36]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 5 vom 15.03.2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[BACPassPP]
CC Protection Profile Machine Readable Travel Document with “ICAO Application” Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0055-2009, 2009-03

[CC]
Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and General Model; Version 3.1, April 2017, CCMB-2017-04-001,
Part 2: Security Functional Requirements; Version 3.1, April 2017, CCMB-2017-04-002,
Part 3: Security Assurance Requirements; Version 3.1, April 2017, CCMB-2017-04-003

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, April 2017, CCMB-2017-04-004

[EACPassPP]
CC Protection Profile: Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, Version 1.3.2, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0056-V2-2012, 2012-12-05

[EACTR][99]
Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents,
Part 1 - eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015,
Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), BSI, Version 2.21, 2016-12,
Part 3 - Common Specifications, BSI, Version 2.21, 2016-12

[ECARDTR]
Technische Richtlinie TR-03116-2, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, Stand 2017, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017-01-23

[FIPS46]
Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), July 1977, Reaffirmed October 1999, Withdrawn May 2005

99 The Protection Profiles refer to the Version 1.11 of this Technical Guideline. The references given in the PPs are adapted to this version.

[FIPS180]
Federal Information Processing Standards Publication FIPS PUB 180-4, Specifications for the Secure Hash Standard (SHS), 2012-03

[FIPS197]
Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, 2001-11-26

[HWCR]
Certification Report of the underlying hardware platform, BSI-DSZ-CC-1059-2018 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018-05

[HWST]
Security Target of the underlying hardware platform, NXP Secure Smart Card Controller P6022y VB, Security Target Lite, BSI-DSZ-CC-1059, 2018-04

[ICAO9303-1]
ICAO Doc 9303-1, Specifications for electronically enabled passports with biometric identification capabilities. In Machine Readable Travel Documents – Part 1: Machine Readable Passport, volume 2, ICAO, 6th edition, 2006 (including also the corresponding supplements)

[PACEPassPP]
CC Protection Profile: Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0068-V2-2011, 2011-11

[ISO7816]
ISO 7816-4:2013, Identification cards – Integrated circuit cards with contacts, Part 4: Organization, security and commands for interchange, ISO, 2013-04

[ISO14443]
ISO 14443, Identification cards – Contactless integrated circuit cards – Proximity cards, Parts 1-4 and Amendments, 2008-2014

[ICPP]
Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0084-2014, 2014-01

[SP800-38B]
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

[TCOSADM]
Guidance Document – Common Part, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC/PSA protocol, 2019

[TCOSCONF]
- Administrator's Guidance – Residence Permit, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC/PSA protocol, 2019

- Operator's Guidance – Residence Permit, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC/PSA protocol, 2019
- Administrator's Guidance – Passport, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC/PSA protocol, 2019
- Operator's Guidance – Passport, Guidance Documentation of TCOS ID Version 2.0 Release 1 with BAC, PACE/SAC and EAC/PSA protocol, 2019