T · · Systems ·

Specification of the Security Target
TCOS Residence Permit Card Version 1.1
Release 2-BAC/SLE78CLX1440P

Version: 1.1.2/20161124

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	ASE TCOS Residence Permit Card BAC 1.1.2 (IFX).docx
Stand:	24.11.2016
Version:	1.1.2
Hardware Basis:	SLE78CLX1440P
Autor:	Ernst-G. Giessmann
Geltungsbereich:	TeleSec Entwicklungsgruppe
Vertraulichkeitsstufe:	**Öffentlich**

History

Version	Date	Remark
1.1.2	2016-11-24	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 Residence Permit Card Version 1.1 Release 2-BAC/SLE78CLX1440P
TOE:	TCOS Residence Permit Card Version 1.1 Release 2-BAC/ SLE78CLX1440P
Sponsor:	T-Systems International GmbH
Editor(s):	Ernst-G. Giessmann, T-Systems International GmbH, TeleSec
CC Version:	3.1 (Revision 3)
Assurance Level:	EAL4 augmented.
General Status:	Final Document
Version Number:	1.1.2
Date:	2016-11-24
Certification ID:	BSI-DSZ-CC-0836-V2
Keywords:	Residence Permit Card, eID, eSign, ePass, MRTD, PACE, EAC

3 The TOE is a ready for Personalization contact-less chip with an initialized filesystem according to [BACPP3.1] 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 Residence Permit Card Version 1.1 Release 2-BAC” (TOE) of T-Systems for CC evaluation.

1.3 TOE Overview

5 The Target of Evaluation (TOE) addressed by the current Security Target is the electronic Residence Permit Card representing a contactless smart card programmed according to the Technical Guideline TR-03110 ([EACTR]) and being compliant to EU – Residence Permit Specification [EURPS]. For CC evaluation the following application of the corresponding product will be considered:

the Passport Application[1] (*ePassport*) containing the related user data[2] (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 Residence Permit Card will be considered as an MRTD only.

6 The corresponding product provides also the eID-Application and optionally the eSign-Application according to [EACTR]. They are not relevant for the current ST and do not infer the Security Functions of the TOE.

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

8 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. 32).

9 The MRTD is integrated into a plastic, optically readable part of the Identity Card, This is not part of the TOE.

10 If in some context the hardware base is relevant, the TOE will be identified in more detail as the "TCOS Residence Permit Card Version 1.1 Release 2-BAC/SLE78CLX1440P", otherwise the notion "TCOS Residence Permit Card Version 1.1 Release 2-BAC" will be used, indicating that this context applies to any realization regardless which hardware base is used. The SLE78CLX1440P chip is selected from the M7820 family. Note that the Chip Identifier Byte is not used in the TOE identification because it has no impact on the evaluation.

11 The TOE follows the composite evaluation aspects ([AIS36]). The Security Target of the underlying platform ([HWST]) claims conformance to Smartcard IC Platform Protection Profile ([PP0035]).

12 This composite ST is based on the ST of the underlying platform ([HWST]). The compatibility of the Life Cycle Model of the Protection Profile [RPCARDPP] and the Life Cycle Model required by [PP0035] will be shown in 1.4.1.

1.4 TOE Description

1.4.1 TOE Definition

13 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)

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

- the ePassport application[3] and
- the associated guidance documentation

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

15 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.

1.4.2 TOE security features for operational use

16 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.

1.4.3 Non-TOE hardware/software/firmware

17 In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless communication according to [ISO14443].

18 From the logical point of view, the TOE is able to recognize the terminal type (see [EACTR], sec. 3.2):

> *Basic Inspection system with Basic Access Control:* an official terminal that is always operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) (BIS-BAC[4] as defined in the Protection Profile BACPP3.1).

1.4.4 Life Cycle Phases Mapping

19 According to the PP [BACPP3.1] the TOE life cycle is described in terms of the four life cycle phases[5].(With respect to the [PP0035], the TOE life-cycle is additionally subdivided into 7 steps.)

---

3 Note that the eID- and optionally the eSign applications are part of the product but not of the TOE.
4 BIS-BAC means BAC and passive authentication with SO_D with an Basic Inspection System (BIS)
5 Note that this corresponds to the life cycle phases defined in the [RPCARDPP] as well.

Life cycle phase 1 "Development"

20 (Step1) 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.

21 (Step2) 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.

22 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.

Life cycle phase 2 "Manufacturing"

23 (Step3) 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).

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

25 (Step4) The travel document manufacturer combines the IC with hardware for the contactless interface in the inlay (embedding).

26 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 MRTD, nevertheless they are not inevitable for the secure operation of the TOE.

27 (Step5) 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.

28 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. This handing over is the delivery of the TOE in the meaning of the CC.

29 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 can not be changed.

30 For the TOE one pre-configured version (FSV01) of the file system applies. A detailed description of the sub-phases and the file system pre-configurations, including the assigned maximal available memory sizes can be found in the Administrator Guidance [TCOSADM].

31 The product is finished after initialization, after testing the OS and creation of the dedicated file system with security attributes and ready made for the import of User Data. This corresponds to the end of the life cycle phase 2 of the Protection Profile [EACPP3.1]. The TOE may also be pre-configured during manufacturing which leads to different configurations for delivering. A more detailed description of the production processes is given in the Administrator Guidance document [TCOSADM].

32 *Application Note 1*: For flexibility reasons the order of the steps (Step4) and (Step5) can be changed. Nevertheless the delivery of the TOE in the meaning of the CC can only be done after both steps are completed.

Life cycle phase 3 "Card Issuing" (also known as "Personalization of the MRTD")

33 (Step6) 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).

34 The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object. In the following this step is called "Personalization".

35 The signing of the Document security object by the Document signer [ICAO9303-1] finalizes the personalization of the travel document for the travel document holder. The personalized travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

36 *Application Note 2*: Note that from hardware point of view the life cycle phase "Card Issuing" 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"

37 (Step7) The TOE is used as MRTD's chip by the MRTD holder and the terminals in the "Operational Use" phase.

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

1.4.5 TOE Boundaries

1.4.5.1 TOE Physical Boundaries

39 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.

40 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.

41 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. There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features.

1.4.5.2 TOE Logical Boundaries

42 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.

43 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).

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

45 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

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

Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012,

Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012,

Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

47 as follows:

Part 2 extended, Part 3 conformant.

48 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012, [CC] has to be taken into account. The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations.

2.2 PP Claims

49 This ST claims *strict* conformance to 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application" Basic Access Control, Version 1.10, BSI-PP-0055 issued by Bundesamt für Sicherheit in der Informationstechnik (BSI) [BACPP3.1].

2.3 Package Claims

50 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 5.

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

2.4 Conformance Rationale

52 Since the ST is not claiming conformance to any other protection profile and the PP [BACPP3.1] is not claiming conformance to another PP, no rationale is necessary here.

3 Security Problem Definition

3.1 Introduction

Assets

53 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], sec. 3.2). 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 Integrity Authenticity
2	user data transferred between the TOE and the service provider connected[6]	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 [EACPP3.1, sec. 3.2]. User data can be received and sent.	Confidentiality Integrity 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. TOE tracing data can be provided / gathered.	Unavailability[7]

Table 1: Primary assets

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

55 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

6 For the ePassport application, the service provider is always an authority represented by a local RF-terminal

7 represents a prerequisite for anonymity of the MRTD holder

Object No.	Asset	Definition	Property to be maintained by the current security policy
5	Genuineness of the TOE	Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way. This asset covers the 'Authenticity of the MRTD's chip' in [BACPP3.1].	Availability
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 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 Authenticity

Table 2: Secondary assets

56 *Application Note 3*: Please note that MRZ are not to convey to the TOE.

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

Subjects and external entities

58 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. This entity is commensurate with 'MRTD Holder' in [BACPP3.1]. Please note that an MRTD holder can also be an attacker (s. below).
2	–	MRTD presenter	A person presenting the MRTD to a terminal[8] and claiming the identity of the MRTD holder. This subject is commensurate with 'Traveller' in [BACPP3.1]. 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. 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[9] 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). BIS-BAC is supporting/applying the Passive Authentication. BIS-BAC is equivalent to the Basic Inspection System (BIS) as defined in [BACPP3.1].
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. A Document Signer is authorized by the national CSCA issuing the

8 in the sense of [EACTR]

9 concretely, by a control officer

External Entity	Subject	Role	Definition
			Document Signer Certificate (C_{DS}), see [EACTR], chap. 1.1 and [ICAO9303-1]. This role is usually delegated to a Personalization Agent. This entity is commensurate with the respective external entity #9 in [PACEPassPP].
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. 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. 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], sec. 2.2.1.
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 Residence Permit Card (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). 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[10]

3.2 Threats

59 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.

10 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.

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

60 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 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**

61 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**

62 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**

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

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

T.Abuse-Func Abuse of Functionality

65 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

66 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

67 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**

68 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

69 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**

70 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**

71 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**

72 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].

73 *Application Note 4*: 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

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

75 The PP ([BACPP3.1]) includes the assumption **A.MRTD_Manufact**. It is covered in this ST by ALC_DVS.2. Therefore it will not be repeated here.

76 The PP ([BACPP3.1]) includes the assumption **A.MRTD_Delivery**. It is covered in this ST by ALC_DEL.1. Therefore it will not be repeated here.

77 *Application note 5:* Assumptions A.MRTD_Manufact and A.MRTD_Delivery from [BACPP3.1] address manufacturing, testing and delivery aspects. Fulfillment of such assumptions is a necessary condition for a 'pass' judgement 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 ([BACPP3.1]) by choosing the assurance components ALC_DVS.2 and ALC_DEL.1.

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

78 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**

79 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.

80 *Application Note 6*: 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 **Personalization of the MRTD's chip**

81 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.

82 *Application Note 7*: 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

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

4.1 Security Objectives for the TOE

84 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

85 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.

86 *Application Note 8*: The OT.AC_Pers implies that the data of the LDS groups written during personalization for MRTD holder can not 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

87 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

88 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

89 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.

90 *Application Note 9*: 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.

91 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

92 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

93 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.

94 *Application Note 10:* 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

95 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

96 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.

97 *Application Note 11:* 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

98 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

99 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

100 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.

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

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

OE.Personalization Personalization of the logical MRTD

102 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

103 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

104 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

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

OE.Exam_MRTD Authentication of rightful terminals

106 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

107 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

108 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

109 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

	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
A.BAC-Keys													x			

Table 4:Security Objective Rationale

110 A detailed justification required for suitability of the security objectives to coup with the security problem definition is given in the Protection Profile ([BACPP3.1]). Hence there is no need to duplicate it here.

111 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).

112 The following Security Objectives for the Hardware Platform are based on [PP0035]:

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)

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

114 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

115 This protection profile uses components defined as extensions to CC part 2. All these extended components are drawn from Definitions of chapter 5 of [BACPP3.1].

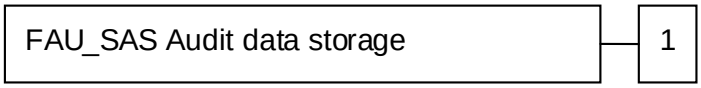
5.1 FAU_SAS Audit data storage

116 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.

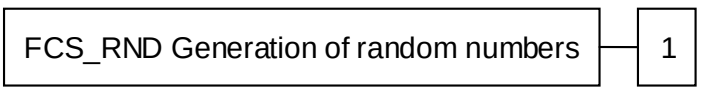
5.2 FCS_RND Generation of random numbers

117 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*].

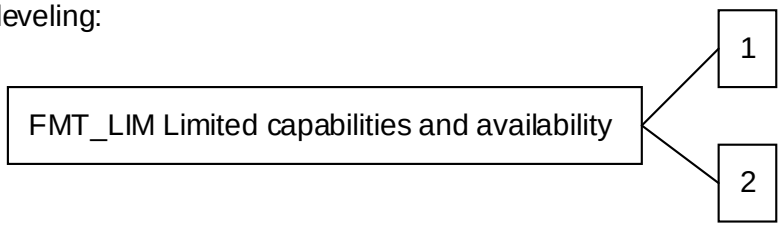
5.3 FMT_LIM Limited capabilities and availability

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

Family behaviour

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.

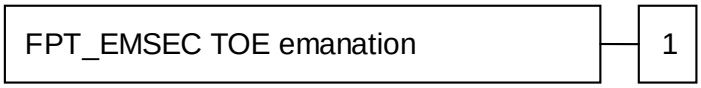
5.4 Definition of the Family FPT_EMSEC

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

Dependencies: No other components.

6 Security Requirements

119 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.

120 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.

121 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~~.

122 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*.

123 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*.

124 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.

125 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.

126 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

127 **FAU_SAS.1 Audit storage**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer[11] with the capability to store the IC Identification Data [12] in the audit records.

128 *Application Note 12*: 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)

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

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Control Key Derivation Algorithm [13] and specified cryptographic key sizes 112 bit[14] that meet the following: [ICAO9303-1], normative appendix 5 [15].

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

131 *Application Note 13*: 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.

132 **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*[16] that meets the following: *none*[17].

133 *Application Note 14*: 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)

134 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.

135 **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

15 [assignment: *list of standards*]
16 [assignment*: cryptographic key destruction method*]
17 [assignment*: list of standards*]

FCS_COP.1.1/ SHA	The TSF shall perform hashing [18] in accordance with a specified cryptographic algorithm SHA-1 [19] and cryptographic key sizes none [20] that meet the following: FIPS 180-2 [FIPS180] [21].

136 **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 de-cryption [22] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode [23] and cryptographic key sizes 112 bit [24] that meet the following: FIPS 46-3 [FIPS46] and [ICAO9303-1, Normative Appendix 5, A5.3][25].

137 **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 de-cryption [26] in accordance with a specified cryptographic algorithm AES [27] and cryptographic key sizes 128 bit [28] that meet the following: FIPS 197 [FIPS197][29].

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

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

Hierarchical to: No other components.

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

FCS_COP.1.1/MAC: The TSF shall perform secure messaging – message authentication code [30] in accordance with a specified cryptographic algorithm Retail MAC [31] and cryptographic key sizes 112 bit [32] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [33].

6.1.2.3 Random Number Generation (FCS_RND)

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

140 **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 PTG.2 generator according to* [AIS31][34].

FCS_RND.1.2: The TSF shall provide a mechanism to generate random numbers that meet the requirements for SOF-high according to [AIS31] 35.

141 Application Note 15: This requirement is specified in [AIS31] in more details. The TOE implements a physical random number generator of the pre-defined class PRG.2 that provides the following security capabilities (PTG.2.1 to PTG.2.5) with a defined quality metric (PTG.2.6 and PTG.2.7):

(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

---

29 [assignment: *list of standards*]
30 [assignment: *list of cryptographic operations*]
31 [assignment: *cryptographic algorithm*]
32 [assignment: *cryptographic key sizes*]
33 [assignment: *list of standards*]
34 [assignment: *a defined quality metric*]
35 [assignment: *a defined quality metric*]

(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source*[36].

(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered *continuously*[37]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

The TSF provide *octets of bits*[38] that meet:

(PTG.2.6) Test procedure A[39] does not distinguish the internal random numbers from output sequences of an ideal RNG.

(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.

142 *Application Note 16*: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocols as required by FIA_UAU.4.

6.1.3 Class FIA Identification and Authentication

143 *Application Note 17:* 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)

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

36 [selection: *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy*]

37 [selection: *externally, at regular intervals, continuously, applied upon specified internal events*]

38 [selection: *bits, octets of bits, numbers* [assignment: *format of the numbers*]]

39 [assignment: *additional standard test suites*]

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"[40] 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.

145 *Application Note 18:* 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 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.

146 *Application Note 19:* 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 then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

6.1.3.2 User Authentication (FIA_UAU)

147 **FIA_UAU.1 Timing of authentication**

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow 1. to read the Initialization Data in Phase 2 "Manufacturing"

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

2. to read the random identifier in Phase 3 "Personalization of the MRTD",
3. to read the random identifier in Phase 4 "Operational Use"[41]

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.

148 *Application Note 20:* The Basic Inspection System and the Personalization Agent authenticate themselves.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on *Symmetric Authentication Mechanism based on AES-128* [42][43].

150 *Application Note 21:* 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.

151 *Application Note 22:* 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.

152 **FIA_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components.

41 [assignment: *list of TSF-mediated actions*]
42 [selection: *Triple-DES, AES or other approved algorithms*]
43 [assignment: *identified authentication mechanism(s)*]

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

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

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*[46].
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[47].

153 *Application Note 23:* In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [EACPP3.1] is 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. [EACPP3.1] FIA_UAU.5.2).

154 *Application Note 24:* 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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

44 [selection: Triple-DES, AES]

45 [assignment: *list of multiple authentication mechanisms*]

46 [selection: *the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key,* [assignment *other*]]

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

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[48].

156 *Application Note 25:* 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.

157 *Application Note 26:* Note that in case the TOE fulfills [EACPP3.1] 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)

158 **FIA_AFL.1 Authentication failure handling**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when 1 unsuccessful authentication attempts occur related to *BAC authentication protocol within a single power-on-session*[49].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met or surpassed*[50], the TSF shall *wait before accepting any other command at least the time which is necessary for re-initialization after power-on*[51].

159 *Application Note 27:* 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 RF field. On the other side this is suffi-

48 [assignment: *list of conditions under which re-authentication is required*]
49 [assignment: *list of authentication events*]
50 [selection: *met, surpassed*]
51 [assignment: *list of actions*]

cient too: If the initialization lasts at least 0.1 seconds then with an expected entropy of 2^{56} bit the estimated time for a brute force attack will more than 200 millions years.

6.1.4 Class FDP User Data Protection

6.1.4.1 Access Control Policy (FDP_ACC)

160 **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 [52] on terminals gaining write, read, modification access to data in EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD [53].

6.1.4.2 Access Control Functions (FDP_ACF)

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

Hierarchical to: No other components.

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

FDP_ACF.1.1 The TSF shall enforce the Basic Access Control SFP[54] 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.[55].

52 [assignment: *access control SFP*]
53 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
54 [assignment: *access control SFP*]

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[56].

FDP_ACF.1.3
1. The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[57].

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[58].

162 *Application Note 28*: The inspection system needs special authentication and authorization forread access to DG3 and DG4 not defined in this protection profile (cf. [EACPP3.1] for details).

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

163 *Application Note 29*: 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.

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

Hierarchical to: No other components.

55 [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*]
56 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
57 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
58 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

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

FDP_UCT.1.1	The TSF shall enforce the Basic Access Control SFP[59] to be able to transmit and receive[60] user data in a manner protected from unauthorized disclosure.

165 *Application Note 30*: 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))

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

FDP_UIT.1.1	The TSF shall enforce the Basis Access Control SFP[61] to be able to transmit and receive[62] user data in a manner protected from modification, deletion, insertion and replay[63] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[64] has occurred.

167 *Application Note 31*: 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.

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

6.1.5 Class FMT Security Management

168 *Application Note 32*: 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)

169 **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[65].

6.1.5.2 Security Management Roles (FMT_SMR)

170 **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[66].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.5.3 Limited Capabilities and Availability (FMT_LIM)

171 *Application Note 33*: 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.

65 [assignment: *list of management functions to be provided by the TSF*]
66 [assignment: *the authorized identified roles*]

172 **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[67].

173 **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 attacksgathered which may enable other attacks[68].

174 *Application Note 34*: 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.

67 [assignment: *Limited capability and availability policy*]
68 [assignment: *Limited capability and availability policy*]

6.1.5.4 Management of TSF data (FMT_MTD)

175 **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 FMT_SMR.1 Security roles
FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write[69] the Initialization Data and Pre-personalization Data[70] to the Manufacturer[71].

176 *Application Note 35*: 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.

177 **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 FMT_SMR.1 Security roles
FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to disable read access for users to[72] the Initialization Data[73] to the Personalization Agent[74].

178 *Application Note 36:* 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.

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

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to write[75] the Document Basic Access Keys[76] to the Personalization Agent[77].

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read[78] the Document Basic Access Keys[79] to none[80].

181 *Application Note 37:* 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

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

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

6.1.6.1 TOE Emanation (FPT_EMSEC)

183 **FPT_EMSEC.1 TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1 The TOE shall not emit *power variations, timing variations during command execution*[81] in excess of *non-useful information* [82] enabling access to the *Personalization Agent Authentication Key*[83] and *Basic Access Control Keys*[84].

FPT_EMSEC.1.2 The TSF shall ensure any unauthorized users[85] are unable to use the following interface smart card circuit contacts[86] to gain access to Personalization Agent Authentication Key[87] and *Basic Access Control Keys*[88].

184 *Application Note 38*: 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)

185 **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,

81 [assignment: *types of emissions*]
82 [assignment: *specified limits*]
83 [assignment: *list of types of TSF data*]
84 [assignment: *list of types of TSF data*]
85 [assignment: *type of users*]
86 [assignment: *type of connection*]
87 [assignment: *list of types of TSF data*]
88 [assignment: *list of types of TSF data*]

2. failure detected by TSF according to FPT_TST.1[89].

6.1.6.3 TSF Self Test (FPT_TST)

186 **FPT_TST.1 TSF testing**

Hierarchical to:	No other components.
Dependencies:	No dependencies
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation*[90] to demonstrate the correct operation of the TSF[91].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data[92].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[93].

187 *Application Note 39*: 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)

188 **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[94] to the TSF[95] by responding automatically such that the SFRs are always enforced.

89 [assignment: *list of types of failures in the TSF*]
90 [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*]]
91 [selection: [assignment: *parts of TSF*], *the TSF*]
92 [selection: [assignment: *parts of TSF*], *TSF data*]
93 [selection: [assignment: *parts of TSF*], *TSF*]

189 *Application Note 40*: 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

190 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:

- ALC_DVS.2 (Sufficiency of security measures),

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					
FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_RND.1	x	x	x					
FIA_UID.1			x	x				
FIA_AFL.1			x	x				
FIA_UAU.1			x	x				

94 [assignment: *physical tampering scenarios*]
95 [assignment: *list of TSF devices/elements*]

	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
FIA_UAU.4	x	x	x					
FIA_UAU.5	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_EMSEC.1	x				x			
FPT_FLS.1					x		x	
FPT_TST.1	x				x		x	
FPT_PHP.3	x				x	x		

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

192 The detailed discussion of the coverage given in this table is already provided by the Protection Profile [BACPP3.1]. 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

193 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 analysed, and non-dissolved dependencies are appropriately explained.

194 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	FCS_COP.1/ENC and FCS_COP.1/MAC

No.	SFR-component from the PP	Dependencies assumed	Supported/fulfilled by SFR
		FCS_CKM.4	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 FCS_CKM.4	See justification 1 of [BACPP3.1, p. 54] FCS_CKM.4
5	FCS_COP.1/ENC	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
6	FCS_COP.1/AUTH	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	See justification 2 of [BACPP3.1, p. 54] See justification 2 of [BACPP3.1, p. 54]
7	FCS_COP.1/MAC	FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 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
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 FMT_MSA.3	FDP_ACC.1 See justification 3 of [BACPP3.1, p. 54]
17	FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_IFC.1 or FDP_ACC.1]	See justification 4 of [BACPP3.1, p. 55] FDP_ACC.1
18	FDP_UIT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_IFC.1 or FDP_ACC.1]	See justification 4 of [BACPP3.1, p. 55] 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 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
24	FMT_MTD.1/INI_DIS	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
25	FMT_MTD.1/KEY_WRITE	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1

No.	SFR-component from the PP	Dependencies assumed	Supported/fulfilled by SFR
26	FMT_MTD.1/KEY_READ	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
27	FPT_EMSEC.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

195 The justification of non-satisfied dependencies is given in the Protection Profile ([BACPP3.1]). Therefore it is not necessary to duplicate it in this ST.

6.3.3 Security Assurance Requirements Rationale

196 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 developers 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.

197 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.

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

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

6.3.4 Security Requirements – Internal Consistency

200 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.

201 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.

202 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

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

204 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
- Accuracy of the TOE security functionality / Self-protection

205 They represent the functional description of the feature overview in section 1.4.2. 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

206 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

207 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 accieved level of trust is maintained as long as the secure channel is not broken.

7.3 Identification and Authentication of Users and Components

208 The identification and authentication protocol is based on the knowledge of the MRZ. The Basic Access Control is decribed 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).

209 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).

210 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.

211 The security and the reliability of the identification and authentification 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 can not be used anymore (FCS_CKM.4).

7.4 Audit

212 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 diabled for the Operational Phase (FMT_MTD.1/INI_DIS) by the Personalization Agent.

7.5 Management of and Access to TSF and TSF-data

213 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 Prepersonalization (FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). The during initialization necessary test features are no more availabe after TOE delivery (FMT_LIM.1, FMT_LIM.2).

214 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

215 The operating system of the TOE protects the security functionality of the TOE as soon as it 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_EMSEC.1).

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

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

218 This functionality is supported by the entire class FMT.

7.7 TOE SFR Statements

219 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 unneccessary text duplication.

220 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.

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

222 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.

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

224 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 algortihm is known except the effective keylength of 112 bits.

225 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.

226 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).

227 FCS_RND.1 The randomness of values for challenges or ephemeral or permanent keys is guaranteed by the underlying hardware TSF. To achieve the SOF “high” the generated data must have sufficient entropy. This is fulfilled automatically if the random number generator is certified as P2 according [AIS31].

228 FIA_AFL.1 The Basic Access Control Keys carry an 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..

229 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 controlled by the Operating System of the TOE.

230 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.

231 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.

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

233 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.

234 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 seccure channel is broken, the encryption and authentication keys can not be used anymore.

235 FMT_SMF.1, FMT_SMR.1: Maintaining the different roles and TSFs of the TOE using dedicated access rules can not 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.

236 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.

237 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 acces to this information is disabled as soon as the TOE is personalized.

238 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.

239 FMT_MTD.3 The Operating System of the TOE accepts only valid certificates; this includes the existence of a valid certificate chain up to the trust anchor (CVCA key) of the TOE.

240 FPT_EMSEC.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.

241 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

242 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.

243 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

244 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

245 The TOE is equipped with following Security Features to meet the security functional requirements:

Relevant:

- SF_DPM Device Phase Management
- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks
- SF_PLA Protection against Logical Attacks
- SF_CS Cryptographic Support

  Cryptographic support includes 3DES, AES, RSA (not relevant), EC (not relevant), SHA-2 (SHA-256 and SHA512 – both not relevant), TRNG (relevant) and PRNG (not relevant).

Not relevant:

7.8.2 Compatibility: TOE Security Environment

Assumptions

246 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 ([PP0035]):

247 A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization) is relevant until the Personalization of the hardware (TOE Initialization)

The assumption A.Process-Sec-IC covers the secure handling of the SC from the delivery by the hardware manufacturer to the developer until the completion of the TOE. This assumption is regarded as being relevant, but not significant, because the content of this assumption is examined during the examination of the assurance families ALC_DEL and ALC_DVS. This assumption is no more required for Composite TOE and is therefore not included into this Composite ST.

248 A.Plat-Appl (Usage of Hardware Platform) is relevant during TOE development

The assumption A.Plat-Appl assumes that the Smartcard Embedded Software securely uses the hardware, taking into account the hardware user guidance and the hardware evaluation. This assumption is regarded as being relevant, but not significant, because the content of this assumption is examined during the examination of the assurance family ADV_COMP. That corresponds to the achievement of the security objectives e.g. OT.EMSEC-Design, OT.Tamper-ID and OT.Tamper-Resistance in the TOE end usage. This assumption is not required for Composite TOE and is therefore not included into this Composite-ST.

249 A.Resp-Appl (Treatment of User Data)

This assumption is covered by the hardware's objective for the environment OE.Resp-Appl which is related to TOE's Life Cycle Phase 1 "Development". It is supported by the Security Objectives OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality and TOE's Environment Objective OE.Chip_Auth_Key.

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

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

  Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). This assumption is covered by the Hardware's objective OE.Resp-Appl for the environment and applies to Life Cycle Phase 1 "Development".

Threats

250 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 Smardcard IC PP [PP0035]
- T.Abuse-Func matches the corresponding threat of the of the Smardcard IC PP [PP0035]
- T.Information_Leakage matches T.Leak-Inherent and T.Leak-Forced of the Smardcard IC PP [PP0035]
- T.Phys-Tamper matches T.Phys-Probing and T.Phys-Manipulation of the Smardcard IC PP [PP0035]
- T.Malfunction matches corresponding threat of the Smardcard IC PP [PP0035]

Threats of the hardware ST ([PP0035]):

- 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.Mem-Access (Memory Access Violation)

Parts of the Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code) or privilege levels. Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software. This threat is related to TOE's Life Cycle Phase 1 "Development". It is covered by the threat T.Abuse_Func of the TOE.

Organizational Security Policies

251 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-Functions (Additional Specific Security Functionality) no conflict
  The TOE' hardware provides the following specific security functionality to the Smartcard Embedded Software: Advanced Encryption Standard, Triple Data Encryption Standard (not relevant), Rivest-Shamir-Adleman Cryptography (not relevant), Elliptic Curve Cryptography (not relevant), Secure Hash Algorithm SHA-2.
- P.Process-TOE ([PP0035]) is covered by P.Manufact of the Composite ST

Security Objectives

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

Security Objectives for the Composite ST of the TOE:

- OT.Data_Int covers O.Add_Functions (AES, DES) of the [HWST]
- OT.Data_Conf covers O.Add_Functions (AES, DES) of the [HWST]
- OT.AC_Res no conflict
- OT.Identification matches O.Identification from [PP0035]
- OT.Prot_Abuse-Func covers O.Abuse-Func from [PP0035]
- OT.Prot_Inf_Leak covers O.Leak-Inherent and O.Leak-Forced from [PP0035]
- OT.Prot_Phys-Tamper covers O.Phys-Probing and O.Phys-Manipulation from [PP0035]
- OT.Prot_Malfunction matches O.Malfunction from [PP0035]

Security Objectives for the hardware ([PP0035] 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.Add-Functions (Additional Specific Security Functionality)
- The hardware TOE must provide the following specific security functionality to the Smartcard Embedded Software: Advanced Encryption Standard (AES) and Triple Data Encryption Standard (TDES), which is mapped to OT.Data_Int, and OT.Data_Conf. The security functionality of Rivest-Shamir-Adleman algorithm, Elliptic Curve Cryptography and Secure Hash Algorithm is not used and therefore not relevant.
- O.MEM_ACCESS is mapped to T.MEM_ACCESS

  This objective for the hardware supports the correct operation of the TOE providing control on restricted data or privilege levels.

Security Requirements

253 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 Requirements of the Composite ST of the TOE:

- 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/DES of [HWST]
- FCS_COP.1/AUTH matches FCS_COP.1/AES of [HWST]
- FCS_COP.1/MAC no conflicts
- 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
- FMT_MTD.3 not relevant
- FPT_EMSEC.1 is supported by the Security Feature SF_PS 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 Requirements of the hardware

- FAU_SAS.1 covered by FAU SAS.1 of the Composite ST
- FCS_COP.1/AES covered by FCS_COP.1/AUTH of the Composite ST
- FCS_COP.1/DES covered by FCS_COP.1/ENC and FCS_COP.1/MAC FCS_COP.1/RSA, FCS_COP.1/ECDSA, FCS_COP.1/ECDH, FCS_COP.1/SHA are not relevant since they are not used
- FCS_RNG.1 (Quality metric for random numbers) matches FCS_RND.1 of the Composite ST
- FDP_ACC.1 (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 (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 (Basic internal transfer protection) is covered by FPT_EMSEC.1 of the Composite ST
- FDP_IFC.1 (Subset information flow control) is covered by FPT_EMSEC.1 of the Composite ST
- FMT_SMF.1 (Specification of Management Functions) is covered by FMT_SMF.1 of the Composite ST
- FMT_LIM.1 (Limited capabilities) is covered by FMT_LIM.1 of Composite ST
- FMT_LIM.2 (Limited availability) is covered by FMT_LIM.2 of Composite ST
- FMT_MSA.1 (Management of security attributes) no conflicts

- FMT_MSA.3 (Static attribute initialization) no conflicts
- FPT_FLS.1 (Failure with preservation of secure state) matches FPT_FLS.1 of the Composite ST
- FPT_ITT.1 (Basic internal TSF data transfer protection) is covered by FPT_EMSEC.1 of the Composite ST
- FPT_PHP.3 (Resistance to physical attack) is covered by FPT_FLS.1 and FPT_PHP.3 of the Composite ST
- FDP_SDI.1, FDP_SDI.2, FRU_FLT.2, FPT_TST.2 concern the hardware operation, no conflicts to SFRs of the TOE

Assurance Requirements

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

255 The chosen level of assurance of the hardware is EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5

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

7.8.3 Conclusion

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

7.9 Assurance Measures

258 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 MRTD
ADV_FSP.4	Functional Specification TCOS MRTD
ADV_IMP.1	Implementation of the TSF TCOS MRTD
ADV_TDS.3	Modular Design of TCOS MRTD

Guidance documents

AGD_OPE.1	User Guidance TCOS MRTD
AGD_PRE.1	Administrator Guidance TCOS MRTD

Life-cycle support

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

Tests

ATE_COV.2, ATE_DPT.2	Test Documentation for TCOS MRTD

ATE_FUN.1	Test Documentation of the Functional Testing
Vulnerability assessment	
AVA_VAN.5	Independent Vulnerability Analysis TCOS MRTD

259 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.

260 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.

261 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.

262 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.

263 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.

264 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

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

Glossary

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the MRTD's chip to produce Terminal Certificates with the correct certificate effective date, see also [EACTR], sec. 2.2.5].
Advanced Electronic Signature	according to the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on "a Community framework for electronic signatures" a digital signature qualifies as an electronic signature, if it is: - uniquely linked to the signatory; - capable of identifying the signatory; - created using means that the signatory can maintain under his sole control, and - linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Agreement	This term is used in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
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 MRTD's chip to store the Initialization Data and Pre-personalization Data.
Authentication terminal (ATT)	A technical system being operated and used either by a governmental organization (Official Domestic Document Verifier) or by any other, also commercial organization and (i) verifying the MRTD presenter as the MRTD holder (using the secret eID-PIN[96]), (ii) updating a subset of data of the eID application and (iii) activating the eSign application. See also [EACTR], chap. 3.2 and C.4.
Authenticity	Ability to confirm that the MRTD itself and the data elements stored in were issued by the MRTD issuer
Basic Access Control	Security mechanism defined in [BACPP3.1] 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) based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
Basic Inspection System (BIS)	A technical system being used by an authority[97] and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying correspondence between the stored and printed MRZ. BIS implements the terminal's part of the Basic Access Control protocol and authenticates itself to the MRTD using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (MRTD document details data and biographical data) stored on the MRTD (ePassport application only). See also [EACTR], chap. G.1 and H; also [ICAO9303-1].
Biographical data (biodata)	The personalized details of the MRTD holder appearing as text in the visual and machine readable zones of and electronically stored in the MRTD. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Identification Card), semi-static (e.g. printed on a label on the Identification Card) or dynamic (randomly chosen by the electronic MRTD and displayed by it using e.g. ePaper, OLED or similar technologies), see [EACTR], sec. 3.3
Card Security Object (SO_C)	A RFC 3369 CMS Signed Data Structure signed by the Document Signer (DS). It is stored in the MRTD (EF.CardSecurity, see [EACTR], Table A.1 and sec. A.1.2) and carries the hash

96 the secret eID-PUK can be used for unblocking the eID-PIN and resetting the retry counter related

97 concretely, by a control officer

Term	Definition
	values of different Data Groups as defined in [EACTR], Appendix A. It shall also carry the Document Signer Certificate (C_{DS}) [EACTR], A.1.2.
Certificate chain	Hierarchical sequence of Terminal Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Certification Service Provider (CSP)	An organization issuing certificates or providing other services related to electronic signatures. There can be CSP, who cannot issue qualified certicates (usually named 'common') or Qualified CSP, who issues qualified certificates. A CSP is the Certification Service Provider in the sense of [SSCDPP].
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means [ICAO9303-1].
Country Signing CertA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority and stored in the rightful terminals.
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. The CSCA also issues the self-signed Country Signing CertA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see [ICAO9303-1], 5.1.1. The Country Signing CertA 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], sec. 2.2.1
Country Verifying Certification Authority (CVCA)	An organization enforcing the privacy policy of the MRTD issuer with respect to protection of user data stored in the MRTD (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the rightful terminals (EIS, ATT, SGT) and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [EACTR], chap. 2.2.1. The CSCA 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], sec. 2.2.1
CV Certificate	Card Verifiable Certificate according to [EACTR], appendix C.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Details Data	Data printed on and electronically stored in the MRTD representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
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 ePassport application of the MRTD. It may carry the Document Signer Certificate (C_{DS}); see [ICAO9303-1]
Document Signer (DS)	An organization enforcing the policy of the CSCA and signing the MRTD Security Object stored on the MRTD for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [EACTR], chap. 1.1 and [ICAO9303-1]. This role is usually delegated to the Personalization Agent.
Document Verifier (DV)	An organization (certification authority) enforcing the policies of the CVCA and of a service provider (governmental or commercial organization) and managing the terminals belonging together (e.g. terminals operated by a State's border police) by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a CertA, authorized by at least the national CVCA to issue certificates for national terminals, see [EACTR], chap. 2.2.2. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the MRTD issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the MRTD issuer und a foreign CVCA ensuring enforcing the MRTD issuer's privacy policy[98]).

98 Existing of such an agreement may be technically reflected by means of issuing a C_{CVCA-F} for the Public Key of the foreign CVCA signed by the domestic CVCA.

Term	Definition
Eavesdropper	A threat agent reading the communication between the MRTD and the Service Provider to gain the data on the MRTD.
eID application	A part of the TOE containing the non-executable, related user data and the data needed for authentication; this application is intended to be used for accessing official and commercial services, which require access to the user data stored in the context of this application. See [EACTR], sec. 3.1.2
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]
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [EACTR], sec. 3.1.1.
eSign application	A part of the TOE containing the non-executable data needed for generating advanced or qualified electronic signatures on behalf of the MRTD holder as well as for authentication; this application is intended to be used in the context of official and commercial services, where an advanced or qualified digital signature of the MRTD holder is required. The eSign application is optional: it means that it can optionally be activated[99] on the MRTD by a Certification Service (or on his behalf) using the ATT with an appropriate authorization level. See [EACTR], sec. 3.1.3.
Extended Access Control	Security mechanism identified in [ICAO9303-1] 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.
Extended Inspection System (EIS)	See *Inspection system*
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or 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 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 Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
MRTD (electronic)	The contactless smart card integrated into the plastic, optical readable cover and providing the following applications: ePassport, eID and eSign (optionally)
MRTD holder	The rightful/legitimated holder of the electronic ID Card for whom the issuing authority personalized the ID Card.
MRTD issuer (issuing authority)	Organization authorized to issue an electronic Identity Card to the MRTD holder
MRTD presenter	A person presenting the MRTD to a terminal and claiming the identity of the MRTD holder.
Identity Card (physical and electronic)	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Identity Card is used in order to verify that identity claimed by the Identity Card presenter is commensurate with the identity of the Identity Card holder stored on/in the card.
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; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO9303-1]

99 'activated' means (i) generate and store in the *eSign* application one or more signature key pairs and (ii) optionally store there the related certificates

Term	**Definition**
Initialization Data	Any data defined by the MRTD manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as IC_Card material (IC identification data).
Inspection	The act of an authority examining an MRTD presented to it by an MRTD presenter and verifying its authenticity as the MRTD holder. See also [ICAO9303-1].
Inspection system (EIS)	A technical system being used by an authority[100] 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). The specification [EACTR], sec. 3.2 (and C.4) knows only one type of the inspection system, namely according to the result of the terminal authentication in the context of the Extended Access Control. It means that the Inspection System in the context of [EACTR], (and of the PP RPCARDPP) is commensurate with the Extended Inspection System (EIS) as defined in [EACPP3.1][101].
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements stored upon have not been altered from that created by the MRTD issuer.
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.
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 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] The MRZ-Password is a secret key that is derived from the machine readable zone and may be used for both PACE and BAC.
Machine-verifiable biometrics 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]
Malicious equipment	A technical device does not possessing a valid, certified key pair for its authentication; validity of its certificate is not verifiable up to the respective root CertA (CVCA for a terminal and CSCA for an MRTD).
Manufacturer	The generic term for the IC Manufacturer producing the 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.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [EACTR], sec. C.1.3. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date, - Certificate Extensions (optional).
PACE Terminal (PCT)	A technical system verifying correspondence between the stored password and the related value presented to the terminal. PCT implements the terminal's part of the PACE protocol and authenticates itself to the MRTD

100 concretely, by a control officer

101 please note that an Extended Inspection System also covers the General Inspection Systems (GIS) in the sense of [EACPP3.1]

Term	Definition
	using a shared password (CAN, eID-PIN, eID-PUK or MRZ). The PCT is not allowed reading User Data (see sec. 4.2.2 in [EACTR]). See [EACTR], chap. 3.3, 4.2, table 1.2 and G.2.
Passive authentication	Security mechanism implementing (i) verification of the digital signature of the Card (Document) Security Object and (ii) comparing the hash values of the read data fields with the hash values contained in the Card (Document) Security Object. See [EACTR], sec. 1.1.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [EACTR], sec. 4.2. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personal Identification Number (PIN)	A short secret password being only known to the MRTD holder. PIN is a blocking password, see [EACTR], sec. 3.3
Personalization	The process by which the individual-related data (biographic and biometric data, signature key pair(s) for the eSign application) of the MRTD holder are stored in and unambiguously, inseparably associated with the MRTD.
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[102], (ii) enrolling the biometric reference data of the MRTD holder[103], (iii) writing a subset of these data on the physical Identification Card (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 Security Object defined in [ICAO9303-1] (in the role of DS).
PIN Unblock Key (PUK)	A long secret password being only known to the MRTD holder. The PUK is a non-blocking password, see [EACTR], sec. 3.3
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalized MRTD and/or to secure shipment within or between the life cycle phases *manufacturing* and *card issuing*.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Authentication Key Pair of the chip.
Receiving State	The Country to which the MRTD holder 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.
Remote terminal	A remote device directly communicating with the TOE and using the technical infrastructure between them (Internet, a local RF-terminal) merely as a message carrier. Only after Chip Authentication when a secure end-to-end connection between the TOE and remote terminal is established, the TOE grants access to the data of the eID application, see [EACTR], sec. 3.4.1
Restricted Identification	Restricted Identification aims providing a temporary MRTD identifier being specific for a terminal sector (pseudo-anonymization) and supporting revocation features (sec. 2.3, 4.1.2, 4.5 of [EACTR]. The security status of MRTD is not affected by Restricted Identification.
Rightful equipment (rightful terminal or rightful MRTD)	A technical device possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either EIS or ATT or SGT. A terminal as well as an MRTD can represent the rightful equipment, whereby the root CertA for a terminal is CVCA and for an MRTD – CSCA.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO9303-1]
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Service Provider	An official or commercial organization providing services which can be used by the MRTD holder. Service Provider uses the rightful terminals managed by a DV.
Signature terminal (SGT)	A technical system being used for generation of digital signatures. See [EACTR], chap. 3.2 and C.4. It is equivalent – as a general term – to SCA and HID as defined in [SSCDPP].
Skimming	Imitation of a rightful terminal to read the MRTD or parts of it via the contactless communi-

102 relevant for the ePassport, the eID and the eSign applications

103 relevant for the ePassport application

Term	Definition
	cation channel of the TOE without knowledge of the printed MRZ CAN, eID-PIN or eID-PUK data.
Terminal	A technical system communicating with the TOE through the contactless interface. The role 'Terminal' is the default role for any terminal being recognized by the TOE as neither PCT nor EIS nor ATT nor SGT ('Terminal' is used by the MRTD presenter).
Terminal Authorization Level	Intersection of the Certificate Holder Authorizations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the MRTD gathered by inconspicuous (for the MRTD holder) recognizing the MRTD
Travel document	A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel [ICAO9303-1].
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC]).
Unpersonalized MRTD	MRTD material prepared to produce a personalized MRTD containing an initialized and pre-personalized MRTD's chip.
User Data	All data (being not authentication data) stored in the context of the applications of the MRTD as defined in [EACTR] and 1. being allowed to be *read out or written* solely by an authenticated terminal (in the sense of [EACTR], sec. 3.2) respectively 2. being allowed to be *used* solely by an authenticated terminal (in the sense of [EACTR, sec. 3.2]) (the private Restricted Identification key; since the Restricted Identification according to [EACTR, sec. 4.5] represents just a functionality of the MRTD, the key material needed for this functionality and stored in the TOE is considered here as 'user data') respectively 3. being allowed to be *used* solely by the authenticated MRTD holder (the private signature key within the eSign application); from this point of view, the private signature key of the MRTD holder is also considered as 'user data'. CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC]).
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
ATT	Authentication Terminal as defined in [EACTR], sec. 3.2
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority (the PP author decided not to use the usual abbreviation 'CA' in order to avoid a collision with 'Chip Authentication')
DTBS	Data to be signed, please refer to [SSCDPP]
EAC	Extended Access Control
EIS	Extended Inspection System (equivalent to the Inspection Systems as defined in [EACTR], sec. 3.2)
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PCT	PACE-authenticated terminal
PICC	Proximity Integrated Circuit Chip
PIN	Personal Identification Number
PP	Protection Profile
PUK	PIN Unblock Key
RAD	Reference Authentication Data, please refer to [SSCDPP]
RF	Radio Frequency
SAR	Security assurance requirements
SCA	Signature creation application, please refer to [SSCDPP]. It is equivalent to SGT in the current context.
SCD	Signature Creation Data, please refer to [SSCDPP]; the term 'private signature key within the eSign application' is synonym.
SGT	Signature Terminal as defined in [EACTR], sec. 3.2
SVD	Signature Verification Data, please refer to [SSCDPP]
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE security functions
TSP	TOE Security Policy (defined by the current document)
VAD	Verification Authentication Data, please refer to [SSCDPP]

Appendix Results of Cryptographic Assessment

266 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.		PTG.2 Random number generator	[AIS31]	n.a.	[ECARDTR]	-

Table 8: Cryptographic algorithms used by TCOS Residence Permit Card

267 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.

268 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), AIS 31, Version 1 vom 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS36]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 2 vom 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[ALGO]
Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn, 06.01.2010, Veröffentlicht am 04.02.2010 im Bundesanzeiger Nr. 19, S. 426

[BACPP3.1]
CC Protection Profile Machine Readable Travel Document with “ICAO Application” Basic Access Control, Version 1.10, BSI-PP-0055, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-03-25

[CC]
Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and General Model; Version 3.1, Sept. 2012, CCMB-2012-09-001,
Part 2: Security Functional Requirements; Version 3.1, Sept. 2012, CCMB-2012-09-002,
Part 3: Security Assurance Requirements; Version 3.1, Sept. 2012, CCMB-2012-09-003

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Sept. 2012, CCMB-2012-09-004

[EACPP2.3]
CC Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control, Version 1.2, BSI-PP-0026, 2006-09-07

[EACPP3.1]
CC Protection Profile Machine Readable Travel Document with “ICAO Application” Extended Access Control, Version 1.3.2, BSI-PP-0056-V2-2012, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-12

[EACTR]
Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03

[EACTR2.03]
Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010-03-24

[ECARDTR]
Technische Richtlinie TR-03116-2 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2 – Hoheitliche Ausweisdokumente, Stand 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016-03

[ECCTR]
Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-06-28

[EURPS]
EU – Residence permit Specification, Annex II.a to Commission Decision C(2008), version 1.0, 20.08.2008

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

[FIPS180]
Federal Information Processing Standards Publication FIPS PUB 180-2, Specifications for the Secure Hash Standard (SHS), February 2004

[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-0829-V2-2015-MA-01 Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015-08-03

[HWST] Security Target of the underlying hardware platform
Security Target M7820 A11, Version 2.0, Infineon Technologies AG, Chipcard and Security, Evaluation Documentation, 2016-03-11

[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

[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

[RPCARDPP]
CC Protection Profile: Electronic Residence Permit Card (RP_Card PP), Version 1.00, BSI-PP-0069, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010-08-13

[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(s) cards – Proximity cards, 2000

[ISO15946]
ISO 15946, Information technology – Security techniques – Cryptographic techniques based on elliptic curves, 2002

[PP0035]
Smartcard IC Platform Protection Profile, Version 1.0, 15.06.2007, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0035-2007

[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

[SSCDPP]
Protection Profiles for Secure Signature Creation Device – Part 2: Device with Key Generation, EN 14169-1:2009, ver. 1.03, CEN/TC 224, Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0059-2009-MA-02, 2016-06-30

[TCOSADM]
TCOS Residence Permit Card Version 1.1 Release 2, Administrator's Guidance Version 1.3, T-Systems International GmbH, 2016-11