T · · Systems ·

Specification of the Security Target
TCOS Passport Version 2.1
Release 2/P60D144

Version: 2.1.2/20160808

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	ASE TCOS Passport 2.1.2 (NXP).docx
Stand:	08.08.2016
Version:	2.1.2
Hardware Basis:	P60D144
Autor:	Ernst-G. Giessmann, Markus Blick
Geltungsbereich:	TeleSec Entwicklungsgruppe
Vertraulichkeitsstufe:	**Öffentlich**

History

Version	Date	Remark
2.1.2	2016-08-08	Textmarke 44 überarbeitet: 1.Satz gestrichen HW-ST/-CR angepasst Final

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 Passport Version 2.1 Release 2/P60D144
TOE:	TCOS Passport Version 2.1 Release 2/P60D144
Sponsor:	T-Systems International GmbH
Editor(s):	Ernst-G. Giessmann, Markus Blick, T-Systems International GmbH, TeleSec
CC Version:	3.1 (Revision 4)
Assurance Level:	EAL4 augmented.
General Status:	**Final Document**
Version Number:	2.1.2
Date:	2016-08-08
Certification ID:	BSI-DSZ-CC-0808-V2
Keywords:	Electronic Passport, ePass, MRTD, PACE, EAC

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

1.2 TOE Reference

4 This Security Target refers to the Product “TCOS Passport Version 2.1 Release 2” (TOE), consisting of configuration ‘01’ and ‘02’” of T-Systems International GmbH for CC evaluation.

1.3 TOE Overview

5 The Target of Evaluation (TOE) addressed by this Security Target is the electronic Passport Card representing a contactless smart card programmed according to the Logical Data Structure (LDS) and providing the Extended Access Control according to ICAO document [ICAO9303-1] and an authentication mechanism according to the technical report [EACTR]. The hardware bases on a NXP chip P60D144PVA with the TCOS operating system. The TOE is supplied with a conformant to [ISO7816] file system, with a

dedicated Passport Application[1] (*ePassport*) containing the related user data[2] (incl. biometric data) as well as the data needed for authentication (incl. MRZ).

6 According to the Technical Guideline TR-03110 the ePassport Application supports Passive Authentication, Password Authenticated Connection Establishment (PACE) with CAN and MRZ as part of the Standard and General Inspection Procedure, Terminal and Chip Authentication and also Basic Access Control (BAC), which is considered in this ST only as part of Extended Access Control (EAC) with Chip and Terminal Authentication Version 1 (cf. [EACTR, part 1 sec. 2.4.1]).

7 The ePassport Application must be accessed through the contact-less interface of the TOE according to [EACTR]. The travel document holder can control the access to his user data by conscious presenting his travel document to authorities[3] (CAN or MRZ authentication as specified in [EACTR, part 1 sec. 2.3]).

8 The cryptographic algorithms used by the TOE are defined outside the TOE in the Public Key Infrastructure. The security parameters of these algorithms must be selected by the travel document issuer according to the Organizational Security Policies [EACPassPP]. The TOE supports standardized domain elliptic curve parameters mentioned in [RFC5639] (key lengths 192, 224, 256, 320, 384 and 512 bit) and the NIST P-256 curve (key length 256 bit) mentioned in [FIPS186] including the corresponding hash functions. PACE and hence the General Inspection Procedure requires the use of AES, whereas due to compatibility reasons the Advanced Inspection Procedure with BAC may be used with TDES[4] (cf. [EACTR, part 3 sections A.2.3.1 and A.2.4.1]). This depends on the Initialization of the TOE. A more detailed description in given in the Administrator Guidance [TCOSADM].

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

10 In some context the hardware may be relevant, and if so, the TOE will be identified in more detail as "TCOS Passport Version 2.1 Release 2/P60D144", otherwise the notion "TCOS Passport Version 2.1 Release 2" will be used, indicating that this context applies to any realization regardless which hardware base is used. Note that the hardware base is identified as P60D144PVA, but it applies also to its derivates, differing in the memory layout only.

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 [EACPassPP] and the Life Cycle Model required by [PP0035] will be shown in 1.4.1.

---

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

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

3 CAN or MRZ user authentication, see [EACTR, sec. 3.3]

4 TDES is the notation for Triple DES according to [SP800-67], the Technical Guideline [EACTR] uses 3DES instead.

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)
- the ePassport application and
- the associated guidance documentation

14 The components of the TOE are therefore the hardware (IC), the operating system TCOS (OS) and the dedicated files 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 (cf. 1.4.3). The decision upon this was made by the certification body in charge. Further details are considered in the ALC documentation.

16 The TOE provides two configurations: configuration ‘01’ and configuration ‘02’. Both configurations consist of identical operating system code. The only difference is the TOE identification which can be read out during Personalization Phase by the Personalization Agent (described in the Administrator Guidance [TCOSADM] Annex D). These configurations are only needed to differentiate between two used hardware configurations of [HWCR]. There are no differences in security or functionality aspects between these configurations.

17 The TOE provides following security features:

- Password Authenticated Connection Establishment (PACE) [EACTR] protecting the access to the user data stored on the TOE,
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the terminal connected,
- Averting of inconspicuous tracing of the travel document,
- Self-protection of the TOE security functionality and the data stored inside.

18 They will be described in more details in the following section.

1.4.2 TOE security features for operational use

19 A State or Organization issues travel documents to be used by the holder for international travel. The traveler presents a travel document to the inspection system to prove his or her identity. The travel document in this context profile contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the travel document’s chip according to LDS in case of contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid travel document personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the travel document. The issuing State or Organization ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organization.

20 The travel document is viewed as unit of

(i) the physical part of the travel document in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder

(a) the biographical data on the biographical data page of the travel document surface,

(b) the printed data in the Machine Readable Zone (MRZ) and

(c) the printed portrait.

(ii) the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO9303-1] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document holder

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

(e) the digitized portraits (EF.DG2),

(f) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both1

(g) the other data according to LDS (EF.DG5 to EF.DG16) and

(h) the Document Security Object (SOD).

21 The issuing State or Organization implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.

22 The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO9303-1]. These security measures can include the binding of the travel document's chip to the travel document.

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

24 The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [ICAO9303-1], and Password Authenticated Connection Establishment [ICAOSAC]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

25 This Security Target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. The TOE uses the Chip Authentication described in [EACTR] as an alternative to the Active Authentication stated in [ICAO9303-1].

26 BAC is also supported by the TOE, but this is not considered in the scope of this Security Target due to the fact that the Basic Access Control Mechanism BAC provides only resistance against enhanced basic attack potential (i.e. AVA_VAN.3).

27 The confidentiality by Password Authenticated Connection Establishment (PACE) is a inherent security feature of the TOE. The travel document strictly conforms to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard In-

spection Procedure with PACE (PACE PP)' [PACEPassPP]. Note that this PP considers high attack potential.

28 For the PACE protocol according to [ICAOSAC], the following steps are performed:

(i) the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.

(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.

(iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys K_{MAC} and K_{ENC} from the shared secret.

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

29 After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [EACTR, part 3 appendix E], [ICAOSAC], sec 4.6.

30 The TOE implements the Extended Access Control Version 1.0 as defined in [EACTR]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol and (ii) the Terminal Authentication Protocol. The Chip Authentication Protocol (i) authenticates the travel document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication can only be performed if Chip Authentication has been successfully executed. The Terminal Authentication Protocol consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

31 The TOE implements additionally the Extended Access Control Version 2.0 as defined in [EACTR], which is not considered in the Protection Profile [EACPassPP]. The Extended Access Control Version 2.0 consists of two parts (i) the Terminal Authentication Protocol Version 2.0 and (ii) the Chip Authentication Protocol Version 2.0 in this order. The Terminal Authentication Protocol Version 2.0 provides the authentication and the access rights of the inspection system as entity authorized by the receiving State or Organization through the issuing State as the version 1 protocol does. The Chip Authentication Protocol (i) authenticates the travel document's chip to the inspection system using the established during Terminal Authentication secure messaging keys and (ii) re-establishes secure messaging after Chip Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. The protocol provides explicit authentication of the travel document's chip by verifying the authentication token and implicit authentication of the stored data to the authenticated terminal using the new session keys.

1.4.3 Non-TOE hardware/software/firmware

32 There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document; nevertheless these parts are not inevitable for the secure operation of the TOE.

1.4.4 Life Cycle Phases Mapping

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

Life cycle phase 1 “Development”

34 (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.

35 (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.

36 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 ePassport application and the guidance documentation is securely delivered to the travel document manufacturer.

Life cycle phase 2 “Manufacturing”

37 (Step3) In a first step the TOE integrated circuit is produced containing the travel document’s chip Dedicated Software and the parts of the travel document’s chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacturer to the travel document manufacturer.

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

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

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

41 (Step5) The travel document manufacturer

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

(ii) creates the ePassport application,

(iii) equips TOE's chip with pre-personalization Data.

42 The pre-personalized travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalization Agent. The travel document 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.

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

44 A detailed description of the sub-phases and the system pre-configurations, including the assigned maximal available memory sizes can be found in the Administrator Guidance [TCOSADM].

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

46 *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 "Personalization of the travel document"

47 (Step6) The personalization of the travel document includes

(i) the survey of the travel document holder's biographical data,

(ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),

(iii) the personalization (printing) of the visual readable data onto the physical part of the travel document,

(iv) the writing of the TOE User Data and TSF Data into the logical travel document (ePassport application) and

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

48 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".

49 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.

50 *Application Note 2*: Note that from hardware point of view the life cycle phase “Issuing/Personalization” is already an operational use of the composite product and no more a personalization of the hardware. The hardware’s “Personalization” (cf. [HWST]) ends with the initialization and pre-personalization of the TOE and should not be confused with the Personalization described in the Administrator Guidance [TCOSADM].

51 *Application Note 3*: The TSF data comprise (but are not limited to) the Personalization Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

Life cycle phase 4 “Operational Use”

52 (Step7) The TOE is used as a travel document's chip by the traveler and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

53 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 step7 (Operational Use) no restrictions apply.

1.4.5 TOE Boundaries

1.4.5.1 TOE Physical Boundaries

54 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.

55 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.

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

1.4.5.2 TOE Logical Boundaries

57 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.

58 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).

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

60 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

61 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

as follows:

Part 2 extended, Part 3 conformant.

62 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

63 This ST claims *strict* conformance to 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-V2-2012, version 1.3.2' [EACPassPP].

64 This ST claims *strict* conformance to 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, version 1.0, November 2011' [PACEPassPP].

2.3 Package Claims

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

66 The evaluation assurance level of the TOE is EAL4 augmented with ALC_DVS.2, ATE_\ DPT.2 and AVA_VAN.5 as defined in [CC].

2.4 Conformance Claim Rationale

67 The TOE type is a contact-less smart card which is consistent with the TOE type of the claimed PPs.

68 The following Security Problem Definition chapter and the security requirements are taken directly over from the claimed PPs.

3 Security Problem Definition

3.1 Introduction

Assets

69 The assets to be protected by the TOE include the User Data on the travel document's chip, user data transferred between the TOE and the terminal, and travel document tracing data from the claimed EAC PP [EACPassPP], chap 3.1.

70 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	Logical travel document sensitive User Data	Sensitive biometric reference data (DG3, DG4) Due to interoperability reasons the 'ICAO Doc 9303' [ICAO9303-1] requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The travel document is not in certified mode according to this ST, if this data is accessed using BAC.	Confidentiality Integrity Authenticity
2	Authenticity of the travel document's chip	The authenticity of the travel document's chip personalized by the issuing State or Organization for the travel document holder is used by the traveler to prove his possession of a genuine travel document.	Authenticity
3	User data stored on the TOE	All data (being not authentication data) stored in the context of the ePassport application as defined in [EACTR] and being allowed to be *read out* solely by an authenticated terminal (in the sense of [EACTR, part 1 sec. 3.5.2]) respectively. This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [BACPassPP].	Confidentiality[5] Integrity Authenticity
4	User data transferred between the TOE and the terminal connected (i.e. represented by a Basic Inspection System with PACE)	All (but not authentication) data being transferred in the context of the ePassport application of the travel document as defined in [ICAOSAC] between the TOE and an authenticated terminal acting as BIS-PACE (in the sense of [ICAOSAC, sec. 3.2]. User data can be received and sent.	Confidentiality Integrity Authenticity
5	Travel document tracing data	Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.	Unavailability[6]

Table 1: Primary assets

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

5 Though not each data element stored on the TOE represents a secret, the ICAO Specification [ICAOSAC] anyway requires securing their confidentiality: only terminals authenticated according to [ICAOSAC] can get access to the user data stored. They have to be operated according to P.Terminal.

6 represents a prerequisite for anonymity of the travel document holder

72 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
6	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
7	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 'Authenticity of the MRTD's chip' in [BACPassPP].	Availability
8	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
9	TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Objects SO_D, containing digital signatures) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
10	Travel document communication establishment authorization data	Restricted-revealable[7] authorization information for a human user being used for verification of the authorization attempts as authorized user (PACE password). These data are stored in the TOE and are not to send to it. This asset covers the respective object #8 in [EACPassPP].	Confidentiality[7] Integrity

Table 2: Secondary assets

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

Subjects and external entities

74 This ST considers the following subjects additionally to those defined by the EAC PP [EACPassPP]:

External Entity	Subject	Role	Definition
1	1	Country Verifying Certification Authority (CVCA)	The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the travel document. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.
2	2	Document Verifier (DV)	The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the travel document in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.
3	3	Terminal	A Terminal is a technical system communicating with the TOE either through the contact interface or the contactless interface.
4	4	Extended Inspection System using AIP (EIS-AIP-BAC and	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveler and verifying its authenticity and (ii) verifying the traveler as travel document

7 The travel document holder may reveal, if necessary, verification values of the CAN and MRZ to an authorized person or device who definitely act according to respective regulations and are trustworthy.

External Entity	Subject	Role	Definition
		EIS-AIP-PACE)	holder. The Extended Inspection System (EIS) performs the Advanced Inspection Procedure and therefore (i) contains a terminal for the communication with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information, (iv) implements the Terminal Authentication and Chip Authentication Protocols (version 1) and (v) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used. EIS-AIP-BAC is a Basic Inspection System (BIS) in the sense of [BACPassPP] additionally supporting/applying Chip Authentication (incl. passive authentication and Terminal Authentication protocols in the context of AIP and is authorized[8] by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the ePassport application.
5	–	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, especially (i) to manipulate the logical travel document without authorization, (ii) to read sensitive biometric reference data (i.e. DG3, DG4), (iii) to forge a genuine travel document, or (iv) to trace a travel document. The attacker is assumed to possess an at most *high* attack potential.
6	5	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. 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 travel document Manufacturer using this role Manufacturer.
7	6	Personalization Agent	An organization acting on behalf of the travel document Issuer to personalize the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [EACTR], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object (travel document) defined in [ICAO9303-1] (in the role of DS). The Personalization Agent performs the Personalization of the TOE, which consists of the steps (iv)-(vi). Please note that the role 'Personalization Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.
8	7	Basic Inspection System with PACE (BIS-PACE)	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 travel document presenter as the travel document holder (by comparing the real biometrical data of the travel document presenter with the stored biometrical data of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication protocol.
9	–	Document Signer (DS)	An organization enforcing the policy of the CSCA and signing the Document Security Objects stored on the travel document for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [EACTR, part 1 sec. 1.1] and also [ICAO9303-1]. This role is usually delegated to a Personalization Agent.

8 by issuing terminal certificates

9 concretely, by a control officer

External Entity	Subject	Role	Definition
10	–	Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document 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.
11	8	Travel document holder	A person for whom the travel document Issuer has personalized the travel document[10]. This entity is commensurate with 'MRTD Holder' in [BACPassPP]. Please note that a travel document holder can also be an attacker (s. above).
12	–	Travel document presenter (traveller)	A person presenting the travel document to a terminal[11] and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [BACPassPP]. Please note that a travel document presenter can also be an attacker (s. below).

Table 3: Subjects and external entities[12]

3.2 Assumptions

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

A.Insp_Sys Inspection Systems for global interoperability

76 The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [1] and/or BAC [BACPassPP]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol in order to ensure access control and is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

77 *Application note 4:* Assumption A.Insp_Sys does not confine any of the security objectives of [EACPassPP] as it repeats the requirements of P.Terminal for EIS and adds only assumptions for the EAC functionality of the TOE.

10 i.e. this person is uniquely associated with a concrete electronic travel document

11 in the sense of [ICAOSAC]

12 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.

A.Auth_PKI PKI for Inspection Systems

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

79 *Application note 5:* This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [EACPassPP] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication protocol.

80 The following assumption is included from the EAC PP [EACPassPP], chap 3.4.

A.Passive_Auth PKI for Passive Authentication

81 The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication, i.e. digital signature creation and verification for the logical travel document. The issuing States or Organizations run a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations. It is assumed that the Personalization Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [ICAO9303-1].

3.3 Threats

82 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 stored in or protected by the TOE and the method of TOE's use in the operational environment.

T.Read_Sensitive_Data Read the sensitive biometric reference data

83 An attacker tries to gain the *sensitive biometric reference data* through the communication interface of the travel document's chip.

84 The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [BACPassPP]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack

(sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

85 Threat agent has high attack potential, knows the PACE Password, and is in possession of a legitimate travel document.

T.Counterfeit **Counterfeit of travel document chip's data**

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

87 Threat agent has high attack potential, and is in possession of one or more legitimate travel documents.

88 The following threats are included from the PACE PP [PACEPassPP, chap 3.2].

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

89 An attacker imitates an inspection system in order to get access to the *user data stored on or transferred between the TOE and the inspecting authority connected* via the contactless interface of the TOE. The threat agent has high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

90 *Application Note 6:* A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST. When using EIS-AIP-BAC, this threat is confined only to selected data groups (DG3, DG4) within the ePassport application.

T.Eavesdropping **Eavesdropping on the communication between the TOE and the PACE terminal**

91 An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the *user data transferred between the TOE and the terminal connected*.

92 *Application Note 7*: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST. When using EIS-AIP-BAC, this threat is confined only to selected data groups (DG3, DG4) within the ePassport application.

T.Tracing **Tracing travel document**

93 An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE. The threat agent has high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

94 *Application Note 8*: This threat completely covers and extends “T.Chip-ID” from BAC PP [BACPassPP].

95 *Application Note 9*: A product using BAC (whatever the type of the inspection system is: BIS-BAC or EIS-AIP-BAC) cannot avert this threat in the context of the security policy defined in the PP and used in this ST. Hence, this threat is considered not to be allied with using EIS-AIP-BAC.

T.Forgery Forgery of Data

96 An attacker fraudulently alters the *User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected* in order to outsmart the authenticated inspection terminal by means of changed travel document holder’s related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

97 *Application Note 10*: The threat T.Forgery from the PACE PP [PACEPassPP] is extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE.

T.Abuse-Func Abuse of Functionality

98 An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclosure the *User Data stored in the TOE*, (ii) to manipulate or to disclose the *TSF-data stored in the TOE* or (iii) to manipulate (bypass, deactivate or modify) soft-coded *security functionality of the TOE*. This threat addresses the misuse of the functions for the initialization and the personalization in the operational phase after delivery to the travel document holder.

99 *Application Note 11*: Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage Information Leakage from ePassport

100 An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

101 *Application Note 12*: 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).

T.Phys-Tamper Physical Tampering

102 An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE’s Embedded Software. An attacker

may physically modify the travel document in order to modify (i) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.

103 *Application Note 13*: The physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the travel document) 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 travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the 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.

T.Malfunction Malfunction due to Environmental Stress

104 An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

105 *Application Note 14:* 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 threat T.Phys-Tamper) assuming a detailed knowledge about the TOE's internals.

3.4 Organizational Security Policies

106 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.Sensitive_Data Privacy of sensitive biometric reference data

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

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

108 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 travel document with respect to the travel document holder. The personalization of the travel document for the holder is performed by an agent authorized by the issuing State or Organization only.

109 This PP includes also all OSPs from the PACE PP [EACPassPP, chap 3.3].

P.Pre-Operational **Pre-operational handling of the travel document**

1. The travel document issuer issues travel documents and approves terminals complying with all applicable laws and regulations.
2. The travel document issuer guarantees the correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE[13].
3. The travel document issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life phases, i.e. *before* they are in the operational phase.
4. If the travel document issuer authorizes a Personalization Agent to personalize the travel document for the travel document holder, the travel document issuer has to ensure that the Personalization Agent acts in accordance with the travel document issuer's policy.

P.Card_PKI **PKI for Chip and Passive Authentication[14] (issuing branch)**

110 *Application Note 15*: The description below states responsibilities of the involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1. The travel document issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim he runs a Country Signing Certification Authority (CSCA). The travel document issuer shall publish the CSCA Certificate (C_{CSCA}).
2. The CSCA shall securely generate, store and use the CSCA Key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document issuer by strictly secure means, see [ICAO9303-1, 5.1.1] The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and distribute them to the travel document issuer, see [ICAO9303-1, 5.1.1].
3. A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document

13 cf. Table 1 and Table 2 above

14 Passive authentication is considered to be part of the Chip Authentication protocol.

Signer Private Key secret, (iv) securely use the Document Signer Private Key for signing the Document Security Objects of the travel documents.

P.Trustworthy_PKI Trustworthiness of PKI

111 The CSCA shall ensure that it issues its certificates exclusively to the rightful organizations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel documents.

P.Manufact Manufacturing of the travel document's chip

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

P.Terminal Abilities and trustworthiness of terminals

113 The Inspection Systems with PACE (BIS-PACE, EIS-AIP-PACE) shall operate their terminals as follows:

1. The related terminals shall be used by terminal operators and by travel document holders as defined in [ICAO9303-1].
2. They shall implement the terminal parts of the PACE protocol [ICAOSAC], of the Passive Authentication [ICAO9303-1] and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [ICAO9303-1]).
5. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates), where it is necessary for a secure operation of the TOE according to the Protection Profiles [EACPassPP] and [EACPassPP].

4 Security Objectives

114 This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

4.1 Security Objectives for the TOE

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

OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

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

OT.Chip_Auth_Proof Proof of travel document's chip authenticity

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

118 *Application Note 16:* The OT.Chip_Auth_Proof implies the travel document's chip to

119 The OT.Chip_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (stored in EF.DG14) in the LDS defined in [ICAO9303-1] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

120 The following Security Objectives are taken over from the PACE PP [PACEPassPP].

OT.Data_Integrity Integrity of Data

121 The TOE must ensure integrity of the User Data and the TSF-data[15] stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized modifying).
The TOE must ensure integrity of the User Data and the TSF-data. during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE, EIS-AIP-PACE) after the PACE Authentication as well as the Terminal- and the Chip Authentication.

OT.Data_Authenticity Authenticity of Data

122 The TOE must ensure authenticity of the User Data and the TSF-data[15] stored on it by enabling verification of their authenticity at the terminal-side[16].
The TOE must ensure authenticity of the User Data and the TSF-data[15] during their exchange between the TOE and the Service Provider connected (and represented by PACE authenticated BIS-PACE, EIS-AIP-PACE) after the PACE Authentication as well as the Terminal- and the Chip Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[17].

123 *Application Note 17:* A product using BIS-BAC cannot achieve this objective either for stored or being transmitted data in the context of the security policy defined in the ST. When using EIS-AIP-BAC, this objective is confined only to selected data groups (DG3, DG4) within the travel document application.

OT.Data_Confidentiality Confidentiality of Data

124 The TOE must ensure the confidentiality of the User Data and the TSF-data[15] by granting read access only to authorized rightful terminals (BIS-PACE, EIS-AIP-BAC, EIS-GAP, ATT, SGT) according to the effective terminal authorization level (CHAT)[18] presented by the terminal connected[19].
The TOE must ensure confidentiality of the User Data and the TSF-data[15] during their exchange between the TOE and the Service Provider connected (and represented by PACE authenticated BIS-PACE, EIS-AIP-PACE) after the PACE Authentication as well as the Terminal- and the Chip Authentication.

---

15 where appropriate, see Table 2 above

16 verification of SO_D

17 Secure messaging after the chip authentication, see also [EACTR, sec. 4.4.2]

18 CHAT is not applicable to BIS (here: BIS-PACE). For BIS-PACE, table 1.2 in sec. 1.1 of [EACTR] (column PACE) shall be applied.

19 The authorization of the terminal connected (CHAT) is drawn from the terminal certificate chain used for the successful terminal authentication as defined in [EACTR], sec. 4.4 and shall be a non-strict subset of the authorization defined in the Terminal Certificate (C_T), the Document Verifier Certificate (C_{DV}) and the C_{CVCA} in the certificate chain up to the Country Verifying Certification Authority of the travel document issuer (receiving PKI branch of the travel document issuer). The effective terminal authorization can additionally be restricted by the travel document holder by a respective input at the terminal.

125 *Application Note 18*: A product using BIS-BAC cannot achieve this objective in the context of the security policy defined in this ST. When using EIS-AIP-BAC, this objective is confined to only selected data groups (DG3, DG4) by granting read access only to authorized terminal (EIS) according to the terminal authorization level (CHAT) presented by the terminal connected.

OT.Tracing Tracing travel document

126 The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without knowledge of the correct values of shared password (PACE password) in advance.

127 *Application Note 19:* A product using BAC (whatever the type of the inspection system is: EIS-AIP-BAC) cannot achieve this objective in the context of the security policy defined in the ST. Hence, this objective is considered not to be allied with using EIS-AIP-BAC.

OT.Prot_Abuse-Func Protection against Abuse of Functionality

128 The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

OT.Prot_Inf_Leak Protection against Information Leakage

129 The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document

- 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

130 *Application Note 20:* 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

131 The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF-data and the travel document's Embedded Software 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 functionality.

OT.Prot_Malfunction Protection against Malfunctions

132 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 functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

133 The following TOE security objectives address the aspects of identified threats to be countered involving the TOE's environment.

OT.Identification Identification of the TOE

134 The TOE must provide means to store Initialization[20] and Pre-Personalization Data in its non-volatile memory. The Initialization Data must provide a unique identification of the IC during the manufacturing and the card issuing life phases of the travel document. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).

OT.AC_Pers Access Control for Personalization of logical MRTD

135 The TOE must ensure that the logical travel document 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 travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalization of the document.

136 *Application Note 21:* The OT.AC_Pers implies that the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalization.

4.2 Security Objectives for the Operational Environment

I. Travel Document issuer as the general responsible

137 The travel document issuer as the general responsible for the global security policy related will implement the following security objectives of the TOE environment:

OE.Legislative_Compliance

138 The travel document issuer must issue travel documents and approve using the terminals complying with all applicable laws and regulations.

20 amongst other, IC Identification data

II. Travel Document Issuer and CSCA: travel document's PKI (issuing) branch

139 The travel document issuer and the related CSCA will implement the following security objectives for the TOE environment:

OE.Auth_Key_Travel_Document Travel document Authentication Key

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

OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

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

OE.Passive_Auth_Sign Authentication of travel document by signature

142 The travel document issuer has to establish the necessary public key infrastructure as follows: The CSCA acting on behalf and according to the policy of the travel document issuer must (i) generate a cryptographic secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (C_{CSCA}). Hereby authenticity and integrity of these certificates are being maintained.

The Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographic secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in Document Security Object relates to all security information objects according to [EACTR]. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO9303-1]. The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel documents.

OE.Personalization Personalization of travel document

143 The travel document issuer must ensure that the Personalization Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enroll the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Identification Card (optical personalization) and store them in the travel document (electronic personalization) for the travel document holder as defined in [EACTR], (iv) write the document details data, (v) write the initial TSF data, and (vi) sign the Document Security Objects defined in [ICAO9303-1] (in the role of a DS).

III. Travel document issuer and CVCA: Terminal's PKI (receiving) branch

144 The travel document issuer and the related domestic CVCA as well as the foreign CVCAs under agreement (with the travel document issuer Card Issuer)[21] will implement the following security objectives of the TOE environment:

OE.Exam_Travel_Document Examination of the physical part of the travel document

145 An inspection system of the receiving State or Organization must examine the travel document presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of PACE [ICAOSAC] and/or the Basic Access Control [ICAO9303-1]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol to verify the Authenticity of the presented travel document's chip.

OE.Prot_Logical_Travel_Document Protection of data from the logical travel document

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

OE.Ext_Insp_Systems Authorization of Extended Inspection Systems

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

IV. Terminal operator: Terminal's receiving branch

OE.Terminal Terminal operating

148 The terminal operators must operate their terminals as follows:

1. The related terminals (basic inspection systems cf. above) are used by terminal operators and by travel document holders as defined in [ICAO9303-1].
2. The related terminals implement the terminal parts of the PACE protocol [ICAOSAC], of the Passive Authentication [ICAOSAC] (by verification of the signature of the Document Security Object) and use them in this order[22]. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

---

21 The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the current PP in order to reflect an appropriate relationship between the parties involved.

22 This order is commensurate with [ICAOSAC].

3. The related terminals need not to use any own credentials.
4. The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [ICAO9303-1]).
5. The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates), where it is necessary for a secure operation of the TOE according to the current ST.

149 *Application Note 22:* OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from BAC PP [BACPassPP].

V. Travel document holder obligations

OE.Travel_Document_Holder Travel document holder obligations

150 The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

4.3 Security Objective Rationale

151 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.Sens_Data_Cnof	OT.Chip_Auth_Proof	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Identification	OT.AC_Pers	OE.Legislative_Compliance	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Passive_Auth_Sign	OE.Personalization	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_System	OE.Terminal	OE.Travel_Document_Holder
T.Read_Sensitive_Data	x														x					x		
T.Counterfeit		x												x				x				
T.Skimming			x	x	x																	x
T.Eavesdropping					x																	
T.Tracing						x																x
T.Abuse-Func							x															
T.Information_Leakage								x														
T.Phys-Tamper									x													
T.Malfunction										X												
T.Forgery			x	x			x		x			x				x	x	x			x	
P.Sensitive_Data	x														x					x		
P.Personalization											x	x					x					

	OT.Sens_Data_Cnof	OT.Chip_Auth_Proof	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Identification	OT.AC_Pers	OE.Legislative_Compliance	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Passive_Auth_Sign	OE.Personalization	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_System	OE.Terminal	OE.Travel_Document_Holder
P.Manufact											x											
P.Pre-Operational											x	x	x				x					
P.Terminal																		x			x	
P.Card_PKI																x						
P.Trustworthy_PKI																x						
A.Insp_Sys	n.a.																	x	x			
A.Auth_PKI															x					x		
A.Passive_Auth																x		x				

Table 4:Security Objective Rationale

152 A detailed justification required for suitability of the security objectives to coup with the security problem definition is given in the Protection Profiles [EACPassPP] and [PACEPassPP]. Hence it will not be repeated here.

153 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).

154 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)

155 They all will be shown being relevant and not contradicting the Security Objectives of the TOE. They will be mapped to corresponding objectives of the TOE.

156 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

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

5.1 FIA_API Authentication Proof of Identity

158 The family “Authentication Proof of Identity (FIA_API)” is specified as follows.

Family behavior

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

Component leveling:

FIA_API Authentication Proof of Identity	1

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.2 FAU_SAS Audit data storage

159 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 Audit data storage	1

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

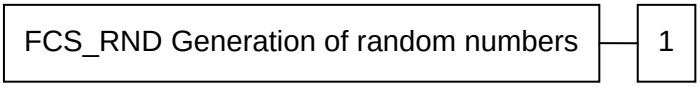
5.3 FCS_RND Generation of random numbers

160 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*].

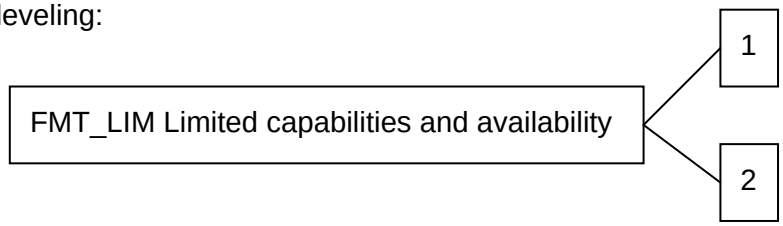
5.4 FMT_LIM Limited capabilities and availability

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

Family behavior

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component leveling:



FMT_LIM.1 Limited capabilities require that the TSF is built to provide only the capabilities (perform action, gather information) which are necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s lifecycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.2 Limited availability.

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.1 Limited capabilities.

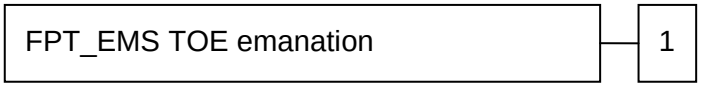
5.5 FPT_EMS TOE Emanation

162 The family “TOE Emanation (FPT_EMS)” is specified as follows. Note that this family is identical to the family FPT_EMSEC defined in other PPs.

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMS.1 TOE emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

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

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

Dependencies: No other components.

6 Security Requirements

163 This part of the ST 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.

164 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.

165 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~~.

166 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*.

167 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*.

168 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.

169 The definition of the subjects "Manufacturer", "Personalization Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in the Glossary or in the following table. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and "re-authenticate" are originally taken from [CC]. The operation "load" is synonymous to "import" used in [CC].

6.1 Security Functional Requirements for the TOE

6.1.1 Overview

170 The following table provides the definition of security attributes:

Security attribute	Values	Meaning
Terminal authentication status	None (any terminal)	Default role (i.e. without authorization after start-up)
	CVCA	Roles defined in the certificate used for authentication (cf. [EACTR]); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA.
	DV (domestic)	Roles defined in the certificate used for authentication (cf. [EACTR]); Terminal is authenticated as domestic Document Verifier after successful CA and TA.
	DV (foreign)	Roles defined in the certificate used for authentication (cf. [EACTR]); Terminal is authenticated as foreign Document Verifier after successful CA and TA.
	IS	Roles defined in the certificate used for authentication (cf. [EACTR]); Terminal is authenticated as Extended Inspection System after successful CA and TA.
Terminal Authorization	none	No read access to DG3 and DG4
	DG4 (Iris)	Read access to DG4 (cf. [EACTR]).
	DG3 (Fingerprint)	Read access to DG3 (cf. [EACTR]).
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4 (cf. [EACTR]).

Table 5: Security Attributes

171 The following table provides an overview of the keys and certificates used. Further keys and certificates are listed in Table 7 of [EACPassPP]:

Name	Data
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Receiving PKI branch	
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [EACTR, Glossary]). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It con-

Name	Data
(C_{IS})	tains (i) the Inspection System Public Key (PK_{IS}) as authentication reference data, (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Issuing PKI branch	
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the issuing Country or Organization signs the Document Signer Public Key Certificate (C_{DS}) with the Country Signing Certification Authority Private Key (SK_{CSCA}) and the signature will be verified by the receiving State or Organization (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key (PK_{CSCA}). 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.
Document Signer Key Pairs and Certificates	The Document Signer Certificate C_{DS} is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK_{DS}) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object (SO_D) of the logical travel document with the Document Signer Private Key (SK_{DS}) and the signature will be verified by an Extended Inspection System of the receiving State or Organization with the Document Signer Public Key (PK_{DS}).
Chip Authentication Private Key (SK_{PICC})	The Chip Authentication Key Pair (SK_{PICC}, PK_{PICC}) is used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman (ECDH, ECKA key agreement algorithm) according to [ECCTR, sec. A.2]. SK_{PICC} is used by the TOE to authenticate itself as authentic travel document.
Chip Authentication Public Key (PK_{PICC})	PK_{PICC} is stored in EF.DG14 on the TOE's logical travel document and used by the terminal for Chip Authentication. Its authenticity is verified by terminal in the context of the Passive Authentication (verification of SO_D). It is part of the user data provided by the TOE for the IT environment.
Session keys	
PACE Session Keys (PACE-K_{MAC}, PACE-K_{Enc})	Secure messaging keys for message authentication (CMAC or Retail-MAC) and for message encryption (CBC-mode) agreed between the TOE and a terminal (PCT) as result of the PACE Protocol, see [EACTR, part 1 sec. 3.3, part 3 E.2].
Chip Authentication Session Keys (CA-K_{MAC}, CA-K_{Enc})	Secure messaging keys for message authentication (CMAC or Retail-MAC) and for message encryption (CBC-mode) agreed between the TOE and terminal (EIS-AIP-BAC, EIS-GAP, ATT, SGT) as result of the Chip Authentication protocol; see [EACTR, part 1 sec. 3.4 and part 3 sections. A.2.3 and. E.2].
Ephemeral keys	
PACE authentication ephemeral key pair (ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE)	PACE authentication ephemeral key pair (ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE)

Table 6: Keys and Certificates

172 In order to give an overview of the security functional requirements mentioned in 1.4.2 in the context of the security services offered by the TOE the following table defines security functional groups and allocates the functional requirements described in the following sections to them.

Security Functional Groups	Security Functional Requirements concerned
Access control to the User Data stored in the TOE	– {FDP_ACC.1/TRM, FDP_ACF.1/TRM} Supported by: – FIA_UAU: authentication and mechanisms used
Secure data exchange between the travel document and the terminal connected	– FTP_ITC.1/PACE: trusted channel for BIS-PACE, EIS-AIP-PACE Supported by: – FCS_COP.1/CA_ENC: encryption/decryption with AES or TDES – FCS_COP.1/CA_MAC: MAC generation/verification – FDP_UCT.1/TRM: Basic data exchange confidentiality – FDP_UIT.1/TRM: Data exchange integrity – FIA_API.1: Chip Identification/Authentication – FIA_UAU.1/PACE: Terminal Authentication (BIS-PACE, EIS-AIP-PACE)

Security Functional Groups	Security Functional Requirements concerned
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (BIS-PACE,EIS-AIP-PACE) – FIA_UAU.1/PACE: Terminal Authentication (EIS-AIP-BAC) – FIA_API.1: Chip Identification/Authentication for AIP (version 1) – FIA_UAU.4/PACE: single-use of authentication data – FIA_UAU.5/PACE: multiple authentication mechanisms – FIA_UAU.6/EAC: Re-authentication of Terminal – FIA_AFL.1/PACE: reaction to unsuccessful authentication attempts for establishing PACE communication using non-blocking authentication and authorization data Supported by: – FCS_CKM.1/DH_PACE: PACE authentication (PACE Terminal) – FCS_COP.1/SIG_VER: Terminal Authentication (EIS-AIP-BAC, EIS-AIP-PACE) – FCS_CKM.1/CA: key generation for Chip Authentication – FCS_CKM.4: session keys destruction (authentication expiration) – FCS_RND.1: random numbers generation – FMT_SMR.1/PACE: security roles definition.
Audit	– FAU_SAS.1: Audit storage Supported by: – FMT_MTD.1/INI_ENA: Writing Initialization and Pre-personalization – FMT_MTD.1/INI_DIS: Disabling access to Initialization and Pre-personalization Data in the operational phase
Management of and access to TSF and TSF-data	– The entire class FMT Supported by: – the entire class FIA: user identification/authentication – FCS_CKM.1.1/CA_PICC for CA key generation
Accuracy of the TOE security functionality / Self-protection	– The entire class FPT – FCS_CKM.4: Cryptographic key destruction – session keys – FDP_RIP.1: enforced memory/storage cleaning Supported by: – the entire class FMT.

Table 7: Security functional groups vs. SFRs

6.1.2 Class FCS Cryptographic Support

173 FCS_CKM.1/DH_PACE Cryptographic key generation – Diffie-Hellman Keys for PACE

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: not fulfilled
Justification: A DH key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/ The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant*

DH_PACE — *to* [ECCTR][23] and specified cryptographic key sizes *112, 128, 192 256*[24] that meet the following: [EACTR, part 3 Appendix A.3.2 and A.3.4.1][25].

174 *Application Note 23:* The TOE generates a shared secret value with the terminal during the PACE Protocol, cf. [EACTR, part 1 sec. 3.2 and part 3 annex A.3]. The shared secret is used to derive the session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [ICAOSAC]. Note that a specified key size defines also the hash function used for key derivation.

175 *Application Note 24:* The TOE supports the following standardized elliptic curve domain parameters (cf. [EACTR, part 3 Table 4]):

ID	Name	Size	Reference
9	brainpoolP192r1	192	[RFC5639, 3.2]
11	brainpoolP224r1	224	[RFC5639, 3.3]
12	NIST P-256 (secp256r1)	256	[FIPS186, D.1.2.3]
13	brainpoolP256r1	256	[RFC5639, 3.4]
14	brainpoolP320r1	320	[RFC5639, 3.5]
16	brainpoolP384r1	384	[RFC5639, 3.6]
17	brainpoolP512r1	512	[RFC5639, 3.7]

176 **FCS_CKM.1/CA Cryptographic key generation – Diffie-Hellman Keys for Chip Authentication**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: fulfilled by FCS_CKM.1/CA_ENC and FCS_CKM.1/CA_MAC
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH*[26] and specified cryptographic key sizes *112, 128, 192 and 256*[27] that meet the following: *based on an ECDH protocol compliant to* [ECCTR][28].

177 *Application Note 25:* The TOE generates a shared secret value with the terminal during the CA Protocol, see [EACTR, part 1 sec. 3.4 and part 3 annex A.4], which uses stan-

23 [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [ECCTR]]
24 [assignment: *cryptographic key sizes*]
25 [assignment: *list of standards*]
26 [assignment: *cryptographic key generation algorithm*]
27 [assignment: *cryptographic key sizes*]
28 [assignment: *list of standards*]/[selection: based on the Diffie-Hellman key derivation protocol compliant to [PKCS#3] and [EACTR], based on an ECDH protocol compliant to [ECCTR]

dardized domain parameters listed in Application Note 24 on p. 41 (cf. [EACTR, part 3 Table 4]). The shared secret is used to derive the session keys for message encryption and message authentication (CA-K_{MAC}, CA-K_{Enc}) according to the [EACTR, part 3 annex E.2 and A.2]. Note that a specified key size defines also the hash function used for key derivation.

178 **FCS_CKM.1/CA_PICC Cryptographic key generation – Chip Authentication Key Pair**

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: fulfilled by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/ CA_PICC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDSA key generation compliant to* [ECCTR][29] and specified cryptographic key sizes *192, 224, 256, 320, 384 and 512 bit length group order*[30] that meet the following: [EACTR][31].

179 *Application Note 26:* This SFR for Chip Authentication Key Pair Generation operation is added to allow a Chip Authentication Key Pair generation by the TOE.

180 *Application Note 27:* The Chip Authentication Key Pair Generation operation is only available during Personalization Phase (Phase 3) (cf. FMT_MTD.1/CAPK) and not in Phase 4 “Operational Use”.

181 *Application Note 28:* The TOE supports the standardized elliptic curve domain parameters listed in Application Note 24 on p. 41.

182 **FCS_CKM.4 Cryptographic key destruction**

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE, FCS_CKM.1/CA
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 zeros, random numbers or the new key*[32] that meets the following: *none*[33].

29 [assignment: *cryptographic key generation algorithm*]/[selection: Diffie-Hellman-Protocol compliant to [PKCS#3], ECDH compliant to [ECCTR]]

30 [assignment: *cryptographic key sizes*]

31 [assignment: *list of standards*]

32 [assignment: *cryptographic key destruction method*]

183 *Application Note 29:* This SFR applies to the Session Keys, i.e. the TOE shall destroy the PACE Session Keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip Authentication Protocol. The TOE destroys the CA Session Keys after detection of an error in a received command by verification of the MAC. The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.
This SFR applies also to the Chip Authentication Key SK_{PICC}, if generated by the Personalization Agent, and the Signature Key SCD. The TOE will overwrite the assigned to the key memory data with the new key.

184 The following iterations are caused by different cryptographic algorithms to be implemented by the TOE.

185 FCS_COP.1/SIG_VER Cryptographic operation – Signature verification

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]: not fulfilled, but justified:

The root key PK_{CVCA} used for verifying C_{DV} is stored in the TOE during its personalization (in the card issuing life phase). The import of the certificates (C_T, C_{DV}) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3 below).

FCS_CKM.4 Cryptographic key destruction: not fulfilled, but justified:

Cryptographic keys used for the purpose of the current SFR (PK_{PCD}, PK_{DV}, PK_{CVCA}) are public keys; they do not represent any secret and, hence, needn't to be destroyed.

FCS_COP.1.1/ SIG_VER: The TSF shall perform digital signature verification[34] in accordance with a specified cryptographic algorithm *ECDSA with plain signature format* [35] and cryptographic key sizes *224, 256, 320, 384 and 512 bit length group order* [36] that meet the following: [EACTR][37].

186 *Application Note 30:* The TOE implements ECDSA with plain signature format for the Terminal Authentication Protocol (cf. [EACTR], see part 1 sec. 3.5, part 2 sec. 3.4 and part 3 annex A.6 for details). The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal generated a digital signature for the TOE challenge, see [EACTR]. The respective static public keys are im-

33 [assignment: *list of standards*]
34 [assignment: *list of cryptographic operations*]
35 [assignment: *cryptographic algorithm*]
36 [assignment: *cryptographic key sizes*]
37 [assignment: *list of standards*]

ported within the certificates (C_T, C_{DV}) during the TA and are extracted by the TOE using PK_{CVCA} as the root key stored in the TOE during its personalization (see P.Terminal_PKI).

187 *Application Note 31:* An ECDSA signature should use a hash function with a corresponding security level. The TOE supports SHA-224, SHA-256, SHA-384 and SHA-512 with the standardized elliptic curve domain parameters listed in Application Note 24 on p. 41.

188 FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption/ Decryption

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE, FCS_CKM.1/CA FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/ CA_ENC	The TSF shall perform secure messaging – encryption and decryption[38] in accordance with a specified cryptographic algorithm *AES and TDES*[39] *in CBC mode*[40] and cryptographic key sizes *112 (TDES option 2), 128, 192 and 256 bit (AES)*[41] that meet the following: *compliant to* [ICAOSAC][42].

189 *Application Note 32*: This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{ENC}) or the Chip Authentication Protocol according to the FCS_CKM.1/CA (CA-K_{ENC}). Note that in accordance with [EACTR, part 3 sections E.2 and A.2] the TDES[39] with option 2 (112-bit 3DES) could be used in CBC mode for secure messaging. It is also a valid option in the Protection Profile PP-0056-V2 [EACPassPP]. Due to the fact that the Retail-MAC is not re¬commended any more by the BSI, this algorithm is applicable only to using EIS-AIP-BAC for legacy reasons of compliance. For all other terminal types being in the scope of the ST this algorithm is not applicable.

190 FCS_COP.1/CA_MAC Cryptographic operation – MAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]]; fulfilled by

38 [assignment: *list of cryptographic operations*]
39 TDES is the notation for Triple DES according to [SP800-67], the Technical Guideline [EACTR] uses 3DES instead.
40 [assignment: *cryptographic algorithm*]
41 [assignment: *cryptographic key sizes*]/[selection: 112, 128, 192, 256]
42 [assignment: *list of standards*]

FCS_CKM.1/DH_PACE, FCS_CKM.1/CA
FCS_CKM.4 Cryptographic key destruction:]; fulfilled by FCS_CKM.4.

FCS_COP.1.1/ CA_MAC	The TSF shall perform secure messaging – message authentication code[43] in accordance with a specified cryptographic algorithm *CMAC, Retail-MAC*[44] and cryptographic key sizes *112, 128, 192 or 256 bit*[45] that meet the following: *compliant to* [ICAOSAC][46].

191 *Application Note 33*: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}) or the Chip Authentication Protocol according to the FCS_CKM.1/CA (CA-K_{MAC}). Note that in accordance with [EACTR, part 3 sections E.2 and A.2.4.1] the TDES (3DES) shall be used in Retail mode for secure messaging. Due to the fact that the Retail-MAC is not recommended any more by the BSI, this algorithm is applicable only to using EIS-AIP-BAC for legacy reasons of compliance. For all other terminal types being in the scope of the ST this algorithm is not applicable.

192 FCS_RND.1 Quality metric for random numbers

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet *the quality requirements for a DRG.4 generator according to* [AIS31][47].

193 *Application Note 34*: This requirement is specified in [AIS31] in more detail. The TOE implements a *hybrid deterministic*[48] random number generator of the pre-defined class DRG.4 that provides the following security capabilities:

(DRG.4.1) The internal state of the RNG shall *use PTRNG of class PTG.2 as random source*[49].

(DRG.4.2) The RNG provides forward secrecy.

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

(DRG.4.4) The RNG provides enhanced forward secrecy *on condition "session closed or aborted"* [50].

---

43 [assignment: *list of cryptographic operations*]
44 [assignment: *cryptographic algorithm*]
45 [assignment: *cryptographic key sizes*]/[selection: 112, 128, 192, 256] bit
46 [assignment: *list of standards*]
47 [assignment: *a defined quality metric*]
48 [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]
49 [selection: *use PTRNG of class PTG.2 as random source, have* [assignment: *work factor*], *require* [assignment: *guess work*]]

(DRG.4.5) The internal state of the RNG is seeded by *a PTRNG of class PTG.2*[51].

(DRG.4.6) The RNG generates output for which $k > 2^{34}$ strings[52] of bit length 128 are mutually different with probability $1-\varepsilon$, with $\varepsilon < 2^{-16}$ [53].

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[54], *the NIST and the dieharder*[55] *tests*[56].

194 *Application Note 35*: This SFR requires the TOE to generate random numbers (random nonces) used for the authentication protocols PACE and TA as required by FIA_UAU.4.

195 *Application Note 36*: Chip Authentication, the (static and ephemeral) key generation and the challenge nonce generation during Personalization use directly the output of the PTG.2 provided by the hardware. For the security capabilities of this random number generator please refer to the hardware ST ([HWST]).

196 This ST also includes all SFRs of the PACE-Pass PP [PACEPassPP]. For the functional class FCS, there are the following additional components: FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC. They are already covered by FCS_COP.1/CA_ENC, FCS_\ COP.1/CA_MAC, as the Diffie-Hellmann key agreement and symmetric key derivation is the same for Chip Authentication and PACE.

6.1.3 Class FIA Identification and Authentication

197 *Application Note 37:* The following Table provides an overview of the authentication mechanisms used.

Name	SFR for the TOE
Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE
PACE protocol	FIA_UAU.1/PACE, FIA_UAU.5, FIA_UAU.6/PACE, FIA_AFL.1/PACE
Chip Authentication Protocol version 1 (for AIP)	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol version 1 (for AIP)	FIA_UAU.5/PACE
Passive Authentication using SO_D	FIA_UAU.5/PACE

Table 8: Overview of authentication SFRs

198 *Application Note 38*: The Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. This property is used for implementation of the version 2 protocols which are outside the scope of the Protection Profile [EACPassPP].

---

50 [selection: *on demand, on condition* [assignment: *condition*], *after* [assignment: *time*]]

51 [selection: *internal entropy source*, *PTRNG of class PTG.2*, *PTRNG of class PTG.3*, [other selection]]

52 [assignment: *number of strings*]

53 [assignment: *probability*]

54 [assignment: *additional test suites*]

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

56 [assignment: *additional test suites*]

199 **FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authentication/authorization data**

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1/ PACE	The TSF shall detect when *2*[57] unsuccessful authentication attempts occurs related to authentication attempts using PACE password as shared password[58].
FIA_AFL.1.2/ PACE	When the defined number of unsuccessful authentication attempts has been met[59], the TSF shall *require the restart of the PACE protocol and increases the reaction time to the next authentication attempt*[60].

200 *Application Note 39*: The assignment operation reflects the fact that according the implementation the authentication procedure consumes a defined minimal amount of time. Because MRZ possesses enough entropy for this reaction time (cf. Administrator Guidance [TCOSADM]), this is sufficient even to prevent a brute force attack with attack potential beyond high (to recover a random 9 digit number would require already about 30 years). Since the CAN with lower entropy does not represent a secret, because it may be revealed already to external entities (cf. footnote 7 on p. 16) it might be not necessary to consider a brute force attack against the CAN. The waiting time after power-up is sufficient to prevent the skimming of the TOE even for a random 6 digit CAN value if the Attacker does not know the CAN.

201 *Application Note 40*: The TOE detects any unsuccessful authentication attempt. After a administrator configurable number of authentication failures with the CAN has been met, the TSF adds an extra time before it allows for the next PACE run with the CAN (cf. [TCOSADM]).

202 *Application Note 41*: Note that there is no explicit requirement for BAC authentication failure handling (EIS-AIP-BAC). Nevertheless since the travel document is evaluated as a BAC TOE, a corresponding failure handling applies. Since it is not required by the Protection Profile [EACPassPP] it is not included here as a SFR.

203 **FIA_API.1 Authentication Proof of Identity**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide the Chip Authentication Protocol v.1 according to [EACTR, part 1 sec. 3.4][61] to prove the identity of the TOE[62].

57 [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
58 [assignment: *list of authentication events*]
59 [selection: *met, surpassed*]
60 [assignment: *list of actions*]
61 [assignment: authentication mechanism]

204 *Application Note 42:* This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [EACTR]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (ECDH) and two session keys for secure messaging in ENC_MAC mode according to [ICAOSAC], normative appendix 5, A5.1. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14). If the Chip Authentication was successfully performed, Secure Messaging is restarted using the derived session keys (CA-K_{MAC}, CA-K_{ENC}).

205 **FIA_UID.1/PACE Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/PACE The TSF shall allow

1. to establishing the communication channel,
2. carrying out the PACE Protocol according to [ICAOSAC],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to carry out the Chip Authentication Protocol v.1 according to [EACTR],
5. to carrying out the Terminal Authentication Protocol v.1 according to [EACTR],
6. *none*[63]

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

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

206 *Application Note 43:* The user identified after a successfully performed PACE protocol is a PACE terminal (PCT). This SFR FIA_UID.1.1/PACE drawn from the Protection Profile [EACPassPP] covers the definition in PACE PP [EACPassPP] and extends it by EAC aspect 4, and GAP aspect 5. As mentioned in [EACPassPP] this extension does not conflict with the strict conformance to PACE PP.

207 **FIA_UAU.1/PACE Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE.

FIA_UAU.1.1/PACE The TSF shall allow

1. to establishing a communication channel,
2. carrying out the PACE Protocol according to [ICAOSAC],
3. to read the Initialization Data if it is not disabled by TSF accord-

62 [assignment: *authorized user or role*]
63 [assignment: *list of TSF-mediated actions*]

ing to FMT_MTD.1/INI_DIS,
4. to identify themselves by selection of the authentication key,
5. to carry out the Chip Authentication Protocol Version 1 according to [EACTR, part 1 sec. 3.4],
6. to carry out the Terminal Authentication Protocol Version 1 according to [EACTR, part 1 sec. 3.5],
7. *to carry out the Terminal Authentication Protocol Version 2 according to* [EACTR, part 2 sec. 3.4],
8. *none*[64]

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

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

208 *Application Note 44:* The user authenticated after a successfully performed PACE protocol is a terminal. If PACE was successfully performed, Secure Messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}).

209 *Application Note 45:* The user authenticated after a successfully performed TA protocol is a Service Provider represented by Extended Inspection System (EIS-GAP or EIS-AIP-BAC).

210 FIA_UAU.4/PACE 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/ PACE: The TSF shall prevent reuse of authentication data related to
1. PACE Protocol according to [ICAOSAC],
2. Authentication Mechanism based on *TDES, AES*[65],
3. Terminal Authentication Protocol v.1 according to [EACTR][66].

211 FIA_UAU.5/PACE Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/ PACE: The TSF shall provide
1. PACE Protocol according to [ICAOSAC],
2. Passive Authentication according to [ICAO9303-1],
3. Secure messaging in MAC_ENC mode according to

64 [assignment: *list of TSF-mediated actions*]
65 [assignment: *TDES, AES or other approved algorithms*]
66 [assignment: *identified authentication mechanism(s)*]

[ICAOSAC],
4. Symmetric Authentication Mechanism based on *AES, TDES*,
5. Terminal Authentication Protocol v.1 according to [EACTR][67],

to support user authentication.

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

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalization Agent by *the Authentication Mechanism with Personalization Agent Key*[68].
3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v.1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol Version 1 only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism v1.
5. *The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol Version 2, only if (i) the terminal presents its static public key*[69] *being successfully verifiable up to CVCA and (ii) the terminal uses the PICC identifier*[70] *calculated during and the secure messaging established by the current PACE authentication*[71].

212 *Application Note 46:* Please note that Chip Authentication Protocol does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the TOE's identity.

213 *Application Note 47:* The commands GET CHALLENGE and MSE:SET will be accepted even if they sent outside the SM channel. But in this case the channel will be closed and therefore all other commands with mandatory access control will not be accepted anymore.

214 **FIA_UAU.6/PACE Re-authenticating – Re-authenticating of Terminal by the TOE**

Hierarchical to: No other components.

67 [assignment: *list of multiple authentication mechanisms*]
68 [selection: *the Authentication Mechanism with Personalization Agent Key(s)*]
69 PK_{PCD}
70 ID_{PICC} = H(ephem-PK_{PICC}-PACE)
71 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

Dependencies: No dependencies.

FIA_UAU.6.1/ PACE: The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE Protocol shall be verified as being sent by the PACE terminal[72].

215 **FIA_UAU.6/EAC Re-authenticating – Re-authenticating of Terminal by the TOE**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/EAC: The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System[73].

216 *Application Note 48:* The PACE and the Chip Authentication Protocols as specified in [EACTR] start secure messaging used for all commands exchanged after successful PACE authentication and CA. The TOE checks each command by secure messaging in encrypt-then-authenticate mode, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

6.1.4 Class FDP User Data Protection

217 **FDP_ACC.1/TRM Subset access control – Terminal Access**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control: fulfilled by FDF_ACF.1/TRM

FDP_ACC.1.1/ TRM: The TSF shall enforce the Access Control SFP[74] on terminals gaining access to the User Data and data stored in the EF.SOD of the logical travel document[75].

218 **FDP_ACF.1/TRM Security attribute based access control – Terminal Access**

72 [assignment: *list of conditions under which re-authentication is required*]
73 [assignment: *list of conditions under which re-authentication is required*]
74 [assignment: *access control SFP*]
75 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM
FMT_MSA.3 Static attributes initialization: not fulfilled, but **justified:** The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalization and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

FDP_ACF.1.1/TRM The TSF shall enforce the Access Control SFP[76] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. BIS-PACE,
   c. Extended Inspection System;
2. Objects:
   a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document,
   b. data in EF.DG3 of the logical travel document,
   c. data in EF.DG4 of the logical travel document,
   d. all TOE intrinsic secret cryptographic keys stored in the travel document[77];
3. Security attributes:
   a. PACE Authentication,
   b. Terminal Authorization v.1,
   c. Authorization of the Terminal[78].

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A BIS-PACE is allowed to read data objects from FDP_\ACF.1.1/TRM according to [ICAOSAC] after a successful PACE authentication as required by FIA_UAU.1/PACE[79].

FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[80].

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

1. Any terminal being not authenticated as a PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel

76 [assignment: *access control SFP*]
77 e.g., Chip Authentication and ephemeral keys
78 [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*]
79 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
80 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

document.

3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.
5. Nobody is allowed to read the data objects 2d) of FDP_\ ACF.1.1/TRM.
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4[81].

219 *Application Note 49*: The SFR FDP_ACF.1.1/TRM covers the definition in PACE PP [PACEPassPP] and extends it by additional subjects and objects. The SFRs FDP_\ ACF.1.2/TRM and FDP_ACF.1.3/TRM cover the definition in PACE PP [PACEPassPP]. The SFR FDP_ACF.1.4/TRM covers the definition in PACE PP [PACEPassPP] and extends it by 3) to 6). As claimed in [EACPassPP] these extensions do not conflict with the strict conformance to PACE PP.

220 *Application Note 50*: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [EACTR]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

221 *Application note 51*: Please note that the Document Security Object (SO_D) stored in EF.SOD (see [ICAO9303-1], sec. A.10.4) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [ICAOSAC].

222 *Application Note 52*: FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication to the Inspection System. The Password Authenticated Connection Establishment and the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

223 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource*

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

from[82] the following objects:

1. session keys (immediately after closing related communication session),
2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret *K*)[83],
3. *none*[84].

224 *Application Note 53*: The functional family FDP_RIP possesses such a general character, so that is applicable not only to user data (as assumed by the class FDP), but also to TSF data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction. This is done by zeroization or explicit overwriting as assigned in FCS_CKM.4.

225 FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UCT.1.1/ TRM	The TSF shall enforce the Access Control SFP[85] to be able to transmit and receive[86] user data in a manner protected from unauthorized disclosure.

226 FDP_UIT.1/TRM Data exchange integrity

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UIT.1.1/ TRM	The TSF shall enforce the Access Control SFP[87] to be able to transmit and receive[88] user data in a manner protected from modification, deletion, insertion and replay[89] errors.
FDP_UIT.1.2/	The TSF shall be able to determine on receipt of user data, whether

82 [selection: *allocation of the resource to, de-allocation of the resource from*]
83 according to [EACTR], sec. 4.2.1, #3.b
84 [assignment: *list of objects*]
85 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
86 [selection: *transmit, receive*]
87 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
88 [selection: *transmit, receive*]
89 [selection: *modification, deletion, insertion, replay*]

TRM	modification, deletion, insertion and replay[90] has occurred.

6.1.5 Class FMT Security Management

227 *Application Note 54*: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

228 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, 4. Configuration[91].

229 *Application Note 55*: Note that Configuration in Life Cycle Phase 3 “Personalization” is restricted to writing of the TOE User Data and TSF Data during Personalization. The functionality of the TSF can not be changed.

230 FMT_SMR.1/PACE Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE, FIA_UID.1/PACE.
FMT_SMR.1.1/ PACE	The TSF shall maintain the roles 1. Manufacturer, 2. Personalization Agent, 3. Terminal, 4. PACE authenticated BIS-PACE, 5. Country Verifying Certification Authority, 6. Document Verifier, 7. Domestic Extended Inspection System, 8. Foreign Extended Inspection System[92].
FMT_SMR.1.2/ PACE	The TSF shall be able to associate users with roles.

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

231 *Application Note 56*: The SFR FMT_SMR.1.1/PACE in the current PP covers the definition in PACE PP [PACEPassPP] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

232 **FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2.

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 manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed[93].

233 **FMT_LIM.2 Limited availability**

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.1.

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 manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks, and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed[94].

234 **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: fulfilled by FMT_SMF.1

93 [assignment: *Limited capability and availability policy*]
94 [assignment: *Limited capability and availability policy*]

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write[95] the Initialization Data and Pre-personalization Data[96] to the Manufacturer[97].

235 **FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialization and Pre-personalization Data**

Hierarchical to: No other components.

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

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to read out[98] the Initialization Data and the Pre-personalization Data[99] to the Personalization Agent[100].

236 *Application Note 57:* The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialization Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, the read and use access shall be blocked in the 'operational use' by the Personalization Agent, when he switches the TOE from the life phase 'issuing' to the life phase 'operational use'.

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/ CVCA_INI	The TSF shall restrict the ability to write[101] the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date 4. *none*[102]

95 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
96 [assignment: *list of TSF data*]
97 [assignment: *the authorized identified roles*]
98 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
99 [assignment: *list of TSF data*]
100 [assignment: *the authorized identified roles*]
101 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

to *the Personalization Agent*[103].

238 *Application Note 58:* The initial Country Verifying Certification Authority Public Key is written by the Personalization Agent in the issuing phase (cf. [EACTR, part 3 sec. 2.4]). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The metadata of the initial Country Verifying Certification Authority Certificate and the initial Current Date are needed for verification of the certificates and the calculation of the Terminal Authorization Level. Please note that only a *subset* of the metadata must be stored in the TOE, see [EACTR, sec. A.6.2.3]; storing of further certificate's content is optional. In fact it is not the initial CVCA Certificate, which is necessary for verification, but the public key included therein, and the self-signature gives no additional security. Therefore the TOE will expect the initial CVCA Certificate to be written by the Personalization Agent without the self-signature (cf. [TCOSADM]).

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1
FMT_MTD.1.1/ CVCA_UPD	The TSF shall restrict the ability to update[104] the 1. Country Verifying Certification Authority Public Key, 2. Country Verifying Certification Authority Certificate[105] to Country Verifying Certification Authority[106].

240 *Application Note 59:* The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key and the related metadata by means of the CVCA link certificates (cf. [EACTR, part 3 sec. 2.1]). The TOE updates its internal trust-point, if a valid CVCA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [EACTR, part 3 sec. 2.3 and 2.4]).

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

102 [assignment: *list of TSF data*]
103 [assignment: *the authorized identified roles*]
104 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
105 [assignment: *list of TSF data*]
106 [assignment: *the authorized identified roles*]

FMT_MTD.1.1/ DATE	The TSF shall restrict the ability to modify[107] the Current Date[108] to 1. Country Verifying Certification Authority, 2. Document Verifier, 3. Domestic Extended Inspection System[109].

242 *Application Note 60*: The authorized role is identified by the certificate issued to an entity (cf. [EACTR, part 3 sec. 2.2 and C.3]) and is authorized by validation of the certificate chain up to CVCA (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. [EACTR, part 3 sec. A.6.2.3, B.11.1, C.1.3, C.1.5, D.2] for details).

243 FMT_MTD.1/PA Agent — Management of TSF data – Personalization

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/PA	The TSF shall restrict the ability to write[110] the Document Security Object (SO_D)[111] to the Personalization Agent[112].

244 *Application Note 61*: By writing SO_D into the TOE, the Personalization Agent confirms (on behalf of DS) the correctness and genuineness of all the personalization data related. The latter consist of user data and TSF data, as well.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1
FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to *load or create*[113] the Chip Authentication Private Key **(SK_{PICC})**[114] to *Personalization Agent*[115].

107 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
108 [assignment: *list of TSF data*]
109 [assignment: *the authorized identified roles*]
110 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
111 [assignment: *list of TSF data*]
112 [assignment: *the authorized identified roles*]
113 [selection: *create, load*]/[selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
114 [assignment: *list of TSF data*]

246 *Application Note 62:* The component FMT_MTD.1/CAPK is refined by (i) selecting other operations and (ii) defining a selection for the operations “create” and “load”. The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. This is the default operation. The verb “create” means here that the Chip Authentication Private Key is generated by the TOE itself during Personalization. This operation is no more available after Personalization.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1. FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read[116] the 1. PACE passwords, 2. Chip Authentication Private Key **(SK_{PICC}),** 3. Personalization Agent Keys[117] to none[118].

248 FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data: fulfilled by FMT_MTD.1/ CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE
FMT_MTD.3.1	The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control **SFP**[119].

Refinement: The certificate chain is valid if and only if

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

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

---

115 [assignment: *the authorized identified roles*]
116 [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
117 [assignment: *list of TSF data*]
118 [assignment: *the authorized identified roles*]
119 [assignment: *list of TSF data*]

(3) the digital signature of the Certificate of the Country Verifying Certification Authority has been verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

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

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

249 *Application Note 63:* The Terminal Authentication is used for Extended Inspection Systems as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization Level derived from the C_{CVCA}, C_{DV} and C_T is used as TSF data for access control required by FDP_ACF.1/TRM.

6.1.6 Class FTP Trusted Path/Channels

250 FTP_ITC.1/PACE Inter-TSF trusted channel after PACE

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for <u>any data exchange between the TOE and the Terminal</u>[120].

251 *Application note 64*: The trusted IT product is the Terminal. In FTP_ITC.1.3/PACE, the word "initiate" is changed to 'enforce", as the TOE is a passive device that can not initiate the communication. All the communications are initiated by the Terminal, and the TOE enforces the trusted channel.

252 *Application note 65*: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}): this secure messaging enforces preventing tracing while establishing Chip Authentication; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC.
The PACE secure messaging session is immediately superseded by a CA secure mes-

120 [assignment: *list of functions for which a trusted channel is required*]

saging session after successful Chip Authentication as required by FTP_ITC.1/CA.
The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

6.1.7 Class FAU Security Audit

253 FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[121] with the capability to store the Initialization and Pre-Personalization Data[122] in the audit records.

254 *Application Note 66*: The Manufacturer role is the default user identity assumed by the TOE in the life phase 'manufacturing'. The IC manufacturer and the travel document 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 travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.1.8 Class FPT Protection of the Security Functions

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

256 FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit *power variations, timing variations during command execution*[123] in excess of *non-useful information*[124] enabling access to

121 [assignment: *authorized users*]
122 [assignment: *list of audit information*]
123 [assignment: *types of emissions*]

1. Chip Authentication Session Keys
2. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem-SK_{PICC}-PACE,
4. *none*[125]
5. Personalization Agent Key(s),
6. Chip Authentication Private Key, and
7. *none*[126]

FPT_EMS.1.2 The TSF shall ensure any users[127] are unable to use the following interface smart card circuit contacts[128] to gain access to

1. Chip Authentication Session Keys
2. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem-SK_{PICC}-PACE,
4. *none*[129]
5. Personalization Agent Key(s)
6. the Chip Authentication Private Key (SK_{PICC}), and
7. *none*[130].

257 *Application Note 67*: The SFR FPT_EMS.1.1 covers the definition given in the Protection Profile [PACEPassPP] and extends it by EAC aspects 1., 4. and 6. The SFR FPT_\ EMS.1.2 covers the definition in PACE PP [PACEPassPP] and extends it by EAC aspects 1., 4. and 6. As claimed in [EACPassPP] these extensions do not conflict with the strict conformance to PACE PP.

258 *Application Note 68*: 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 travel document's chip provides a smart card contactless interface but there may exist sensitive contacts on the surface. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions. SFR FPT_EMS.1.1 covers the analogous definition in PACE PP [PACEPassPP].

259 **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:

124 [assignment: *specified limits*]
125 [assignment: *list of types of (further) TSF data*]
126 [assignment: *list of types of (further) user data*]
127 [assignment: *type of users*]
128 [assignment: *type of connection*]
129 [assignment: *list of types of (further) TSF data*]
130 [assignment: *list of types of (further) user data*]

1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1
3. *none*[131].

260 **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*[132] to demonstrate the correct operation of the TSF[133].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data[134].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[135].

261 *Application Note 69*: The travel document'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 an integrity check value as soon as data is accessed.

262 **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[136] to the TSF[137] by responding automatically such that the SFRs are always enforced.

263 *Application Note 70*: 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.

131 [assignment: *list of types of failures in the TSF*]
132 [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*]]
133 [selection: [assignment: *parts of TSF*], *the TSF*]
134 [selection: [assignment: *parts of TSF*], *TSF data*]
135 [selection: [assignment: *parts of TSF*], *TSF*]
136 [assignment: *physical tampering scenarios*]
137 [assignment: *list of TSF devices/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

264 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),
- ATE_DPT.2 (Testing: security enforcing modules) and
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

6.3 Security Requirements Rationale

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FCS_CKM.1/DH_PACE				X	X	X						
FCS_CKM.1/CA	X	X	X	X	X	X						
FCS_CKM.1/CA_PICC		X										
FCS_CKM.4	X		X	X	X	X						
FCS_COP.1/SIG_VER	X		X									
FCS_RND.1	X		X	X	X	X						
FCS_COP.1/CA_ENC	X	X	X	X		X						
FCS_COP.1/CA_MAC	X	X	X	X	X							
FIA_AFL.1/PACE										X		
FIA_API.1		X										
FIA_UID.1/PACE	X		X	X	X	X						
FIA_UAU.1/PACE	X		X	X	X	X						
FIA_UAU.4/PACE	X		X	X	X	X						
FIA_UAU.5/PACE	X		X	X	X	X						
FIA_UAU.6/PACE				X	X	X						
FIA_UAU.6/EAC	X		X	X	X	X						
FDP_ACC.1/TRM	X		X	X		X						
FDP_ACF.1/TRM	X		X	X		X						
FDP_RIP.1				X	X	X						
FDP_UCT.1/TRM	X			X		X						
FDP_UIT.1/TRM				X		X						

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FTP_ITC.1/PACE				X	X	X				X		
FAU_SAS.1			X				X					
FMT_SMF.1			X	X	X	X	X					
FMT_SMR.1/PACE			X	X	X	X	X					
FMT_LIM.1								X				
FMT_LIM.2								X				
FMT_MTD.1/INI_ENA			X				X					
FMT_MTD.1/INI_DIS			X				X					
FMT_MTD.1/CVCA_INI	X											
FMT_MTD.1/CVCA_UPD	X											
FMT_MTD.1/DATE	X											
FMT_MTD.1/PA			X	X	X	X						
FMT_MTD.1/CAPK	X	X		X								
FMT_MTD.1/KEY_READ	X	X	X	X	X	X						
FMT_MTD.3	X											
FPT_EMS.1			X						X			
FPT_FLS.1									X			X
FPT_TST.1									X			X
FPT_PHP.3				X					X		X	

Table 9: Coverage of Security Objectives for the TOE by SFR

265 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in the PP ([EACPassPP]) and is therefore not repeated here.

6.3.1 Rationale for SFR's Dependencies

266 The dependency analysis for the security functional requirements given in Table 7 of the Protection Profile [EACPassPP] shows that the mutual support and internal consistency between all defined functional requirements except FCS_CKM.1/CA_PICC is satisfied or justified. The dependencies for the remaining SFR FCS_CKM.1/CA_PICC are fulfilled by FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC and FCS_CKM.4. This completes the dependency analysis being expected by CC part 2 and by extended components definition (chapter 5).

6.3.2 Security Assurance Requirements Rationale

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

268 The selection of the component ALC_DVS.2 provides a higher assurance of the security of the travel document's development and manufacturing especially for the secure handling of the travel document's material.

269 The selection of the component ATE_DPT.2 provides a higher assurance than the predefined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

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

271 The component ALC_DVS.2 has no dependencies.

272 The component ATE_DPT.2 has the following dependencies: ADV_ARC.1, ADV_TDS.3 and ADV_FUN.1. All of these are met or exceeded in the EAL4 assurance package.

273 The component AVA_VAN.5 has the following dependencies: ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1 and ATE_DPT.1. All of these are met or exceeded in the EAL4 assurance package.

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

6.3.3 Security Requirements – Internal Consistency

275 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.

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

The dependency analysis in section 6.3.1 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 6.3.2 Security Assurance Requirements Rationale shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

277 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 6.3.1 Rationale for SFR's Dependencies and 6.3.2 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.2 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

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

279 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 travel document and the Terminal
- Identification and authentication of users and components
- Audit
- Management of and access to TSF and TSF-data
- Reliability of the TOE security functionality

280 They are already mentioned in section 6.1.1 and 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

281 The access to User Data is restricted according to the SFRs FDP_ACC.1/TRM and FDP_ACF.1/TRM. Different types of Terminals (PACE, EIS) are assigned dedicated access rights after successful authentication protocol (cf. section 7.3) supported by FIA_\ UAU.1/PACE and Terminal Authentication (FIA_UAU.4/PACE). The reached security level of authentication is maintained by FIA_UAU.5/PACE, FIA_UAU.6/PACE and FIA_\ UAU.6/EAC.

7.2 Secure data exchange

282 The secure data exchange in a trusted channel is required by FTP_ITC.1/PACE. It is supported by fulfilling FCS_COP.1/CA_ENC for authenticated terminal giving confidentiality by data encryption/decryption and by fulfilling FCS_COP.1/CA_MAC providing integrity. The quality and the authenticity of the key used based on the successful execution of the PACE protocol, Terminal Authentication and the Chip Authentication governed by FIA_API.1. FDP_UCT.1/TRM provides the means to protect the confidentiality and FDP_UIT.1/TRM to determine whether modification, deletion, insertion and replay have occurred. FIA_UAU.1/PACE implies secure data exchange after user authentication.

7.3 Identification and authentication of users and components

283 The identification and authentication protocol is described in the [EACTR], where the reliability and the security of the corresponding steps is considered and recognized as

appropriate. Identification and authentication is provided for users (FIA_UID.1/PACE, FIA_UAU.1/PACE) and external entities like terminals of different types (FIA_UID.1/ PACE, FIA_UAU.1/PACE). During the terminal authentication protocol a certificate is used, this is supported by FCS_COP.1/SIG_VER.

284 The TOE itself must also be authenticated, which is supported by FIA_API.1. The travel document application can be authenticated by Passive Authentication. The Requirements laid down in FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/PACE and FIA_UAU.6/EAC concerns the protocol data, prevents re-use and how the security state, e.g. a specified role (FMT_SMR.1/PACE) of an identified and authenticated user or device is achieved and maintained.

285 To prevent skimming attacks on non-blocking PACE passwords, i. e. the CAN (if exists) and MRZ, the TOE blocks the authentication procedure after detecting any failed authentication attempt. Because the MRZ carry enough entropy this is even sufficient for a brute force attack, which is not necessary for the CAN, because the latter is restricted revealable. Note that the TOE does not react immediately after detecting a failure but only before the *next* authentication attempt (FIA_AFL.1/PACE).

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

7.4 Audit

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

7.5 Management of and access to TSF and TSF-data

288 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/ PACE) and maintain all the access rules over the life cycle of the TOE and even before the production of the TOE is finished during Initialization and Pre-personalization (FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). The test features necessary during initialization are no more available after TOE delivery (FMT_LIM.1, FMT_LIM.2).

289 After delivery the TOE is personalized (FMT_MTD.1/PA), the initial CVCA data is stored (FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE) together with the Chip Authentication Private Key (FMT_MTD.1/CAPK), which can only be used internally but never accessed else (FMT_MTD.1/KEY_READ). The Chip Authentication Private Key can be loaded on the TOE during Personalization (FMT_MTD.1/CAPK) or generated (FCS_CKM.1/CA_PICC), following the same requirements as for ECDH ephemeral key agreement.

290 PACE passwords represent non-blocking authentication data, which is used to establish a secure channel. No additional access rights are granted after successfully executed PACE protocol. To avert the inconspicuous skimming of the TOE, the initial PACE proto-

col must be restarted if any failure has been detected (FIA_AFL.1/PACE). Additionally the reaction time is increased after the second authentication failure.

7.6 Reliability of the TOE security functionality

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

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

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

294 The TOE operating system controls the assignment of memory to the User Data in the file system and ensures that no information is available upon de-allocation of a resource. The access rules to the assigned memory remain the same even if the data is no more operational (FDP_RIP.1).

295 This functionality is supported by the entire class FMT.

7.7 TOE SFR Statements

296 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 appropriate then requirements are handled together to avoid needless text duplication.

297 FCS_CKM.1/DH_PACE: The EC Diffie-Hellman Session Key Derivation Algorithm uses a Challenge-Response-Protocol for the derivation of the session keys. The correctness of the keys is verified implicitly by the correct realization of the secure messaging exchange.

298 FCS_CKM.1/CA: The EC Diffie-Hellman Session Key Derivation Algorithm uses a Challenge-Response-Protocol for the derivation of the session keys. The correctness of the keys is verified implicitly by the correct realization of the secure messaging exchange.

299 FCS_CKM.1/CA_PICC: The Chip Authentication Key Pair is usually loaded during Personalization. Beside this it can also be created by the TOE in this life cycle phase, but this is no more possible after the Personalization is finished.

300 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.

301 FCS_COP.1/SIG_VER uses the initial public key Country Verifying Certification Authority and the public keys in certificates provided by the terminals as TSF data for the Terminal Authentication Protocol and the Access Control. Their validity verified according to FMT_MDT.3 and their security attributes are managed by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. There is no need to import user data or manage their security attributes.

302 FCS_COP.1/CA_ENC: The AES algorithm is a generally recognized as secure encryption algorithm. No exploitable weakness is known, and the security level is higher than 100 bit, which is accepted as appropriate in the future. The Triple DES (TDES) is not classified as secure as the AES due to the smaller key length. Taking in account the fact that this algorithm is used only in the case of backward compatibility for EIS-AIP-BAC terminals and that the security level is higher than 100 bit the TDES can be used until the EIS-AIP-BAC terminals are phased out.

303 FCS_COP.1/CA_MAC: The CMAC algorithm is a generally recognized as secure message authentication algorithm. This mode of operation fixes security deficiencies of the legacy CBC-MAC. The Retail-MAC is used for secure messaging and is restricted to data from DG3 and DG4 for EIS-AIP-BAC terminals only. Due to the low data exchange the Retail MAC remains secure for this application.

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

305 FIA_AFL.1/PACE: implement well-known user authentication data handling. If any authentication failure for the non-blocking authentication data (CAN, MRZ) has been detected during the PACE protocol, the TSF blocks the protocol and require a restart of the PACE. Because the MRZ carries enough entropy the minimal reaction time is sufficient to prevent a brute force attack with attack potential beyond high. Even for the case the CAN is used, this reaction time would be sufficient to prevent the tracing of the card, since a brute force attack requires some days of permanent access to the TOE. Nevertheless the TOE increases the reaction time after the second authentication failure.

306 FIA_API.1: The chip authentication implementation based on the description of the protocol in [EACTR] provides a proof of the authenticity of the chip, which is proven to prevent the Challenge Semantics attack. The private Chip Authentication is either leaded or created during personalization phase and can only be used after terminal authentication and never read out.

307 FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE: The access rules allow establishing a communication channel before the user is authenticated. After successful authentication of the Terminal based on PACE or Terminal Authentication Protocol a security status is maintained. Based on that status the access rules apply that allow or disallow the execution of commands and the access to security data controlled by the Operating System of the TOE. The PACE protocol is proven to be secure.

308 FIA_UAU.5/PACE: 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.
After run of the Chip Authentication Protocol and the Terminal Authentication the TOE accepts only commands with a correct message authentication code sent by means of Secure Messaging with key agreed with the terminal by means of the Chip Authentication Mechanism. The security proof of the protocol defined in [EACTR] guarantees the correctness and the reliability of the authentications.

309 FIA_UAU.6/PACE, FIA_UAU.6/EAC: 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. Since the secure messaging uses a sequence counter also replay attacks and insertion are detected.

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

311 FDP_ACF.1/TRM: 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.

312 FDP_RIP.1: The TOE operating system controls the assignment of memory to the User Data in the file system and ensures that no information is available upon de-allocation of a resource. The access rules to the assigned memory remain the same even if the data is no more operational (FDP_RIP.1).

313 FDP_UCT.1/TRM, FDP_UIT.1/TRM: The TOE operating system controls the secure channel established according to Access Control SFP (FDP_ACF.1.1/TRM). The security level is maintained until a command outside the channel is received. After the secure channel is broken, the encryption and authentication keys cannot be used anymore.

314 FTP_ITC.1/PACE: The TOE provides a secured communication channel based on the approved algorithms of Secure Messaging if the PACE protocol with the selected authentication data.

315 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.

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

317 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.

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

319 FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE: The initial Personalization data from the Issuing Branch, initial CVCA key, initial CVCA certificate and the initial Current Date, is written by the authenticated Personalization Agent. The update of the CVCA key and CVCA certificate is allowed only if the terminal authenticates itself as a valid CVCA based on FMT_MTD.3. This access rule cannot be disabled. The data of the Current Date can be overwritten by a terminal that authenticates itself as CVCA or DV. This is based on the validation of a certificate containing the holder authorization/access rights. This access rule cannot be disabled too.

320 FMT_MTD.1/PA, FMT_MTD.1/CAPK: Only the User authenticated as Personalization Agent is able to update the Personalization Data and to create/load the private chip authentication key. These objects are under access control that is fixed in the file system and can never be changed in the operational phase.

321 FMT_MTD.1/KEY_READ: The private chip authentication key is object under access control that is fixed in the file system and can never be changed in the operational phase.

322 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.

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

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

325 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

326 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.

327 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

328 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

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

330 **Relevant:**

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

331 **Not relevant:**

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

7.8.2 Security Requirements

332 **Security Functional Requirements**

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

334 **Security Requirements of the TOE related to the Composite ST:**

335 The following Security Requirements of the TOE are specific for the ePassport Application and have no conflicts with the underlying hardware.

- FCS_CKM.1/DH_PACE not relevant
- FCS_CKM.1/CA not relevant

- FCS_CKM.1/CA_PICC not relevant
- FCS_CKM.4 no conflicts
- FCS_COP.1/SIG_VER not relevant
- FIA_API.1 no conflicts
- FIA_UID.1/PACE no conflicts
- FIA_UAU.1/PACE no conflicts
- FIA_UAU.4/PACE no conflicts
- FIA_UAU.5/PACE no conflicts
- FIA_UAU.6/PACE no conflicts
- FIA_UAU.6/EAC no conflicts
- FDP_ACC.1/TRM not relevant
- FDP_ACF.1/TRM not relevant
- FDP_RIP.1 no conflicts
- FDP_UCT.1 no conflicts
- FDP_UIT.1 no conflicts
- FTP_ITC.1/PACE not relevant
- FIA_AFL.1 no conflicts
- FMT_SMF.1 no conflicts
- FMT_SMR.1/PACE not relevant
- FMT_MTD.1/INI_ENA not relevant
- FMT_MTD.1/INI_DIS not relevant
- FMT_MTD.1/CVCA_INI not relevant
- FMT_MTD.1/CVCA_UPD not relevant
- FMT_MTD.1/DATE not relevant
- FMT_MTD.1/PA not relevant
- FMT_MTD.1/CAPK not relevant
- FMT_MTD.1/KEY_READ not relevant
- FMT_MTD.3 not relevant
- FPT_TST.1 no conflicts

336 Note that some of these requirements, e.g., FCS_CKM.1/DH_PACE rely also on requirements of the hardware as FCS_RNG.1 [HW]. Nevertheless it is considered as not relevant, because the latter is already covered by FCS_RND.1 of the TOE.

337 The remaining Security Requirements of the TOE can be mapped to Security Requirements of the hardware. They show no conflict between each other.

- FCS_COP.1/CA_ENC matches FCS_COP.1[HW_AES]and FCS_COP.1[HW_DES]of [HWST]
- FCS_COP.1/CA_MAC matches FCS_COP.1[HW_AES]and FCS_COP.1[HW_DES]of [HWST]
- FCS_RND.1 matches FCS_RNG.1[HW] of [HWST]
- FAU_SAS.1 matches FAU_SAS.1[HW] of [HWST]
- FMT_LIM.1 matches FMT_LIM.1 of [HWST] in the pre-usage phase
- FMT_LIM.2 matches FMT_LIM.2 of [HWST] in the pre-usage phase
- FPT_EMS.1 is supported by the Security Feature SF.OPC of the hardware ([HWST]) and the AVA_VAN.5 evaluation

- FPT_FLS.1 matches FPT_FLS.1 of [HWST]
- FPT_PHP.3 matches FPT_PHP.3 of [HWST]

338 Security Requirements of the hardware

- FAU_SAS.1[HW] : covered by FAU SAS.1 of the Composite ST
- FCS_COP.1[HW_AES]: covered by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC of the Composite ST
- FCS_COP.1[HW_DES]: covered by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC of the Composite ST
- FCS_RNG.1[HW]: matches FCS_RND.1 of the Composite ST
- FDP_ACC.1 [MEM] and [SFR] (Subset access control): are not relevant for the TOE, but for the implementation of the OS, therefore it is covered by ADV_IMP.1 (Implementation representation of the TSF)
- FDP_ACF.1 [MEM] and [SFR] (Security attribute based access control): are not relevant for the TOE, but for the implementation of the OS, therefore it is covered by ADV_IMP.1 (Implementation representation of the TSF
- FDP_ITT.1[HW] (Basic internal transfer protection): is covered by FPT_EMS.1 of the Composite ST
- FDP_IFC.1 (Subset information flow control): is covered by FPT_EMS.1 of the Composite ST
- FMT_SMF.1[HW] (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 [MEM] and [SFR] (Management of security attributes): no conflicts
- FMT_MSA.3 [MEM] and [SFR] (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[HW] (Basic internal TSF data transfer protection): is covered by FPT_EMS.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.2[HW] (Stored data integrity monitoring and action): concerns the hardware operation, does not conflict with SFRs of the TOE
- FRU_FLT.2 (Limited fault tolerance): concerns the hardware operation, does not conflict with SFRs of the TOE

339 Security Assurance Requirements

340 The level of assurance of the TOE is EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

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

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

7.8.3 Security Objectives

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

344 **Security Objectives of the TOE related to the Composite ST:**

- OT.Data_Integrity: covers O.HW_AES and O.HW_DES3 of the [HWST]
- OT.Data_Authenticity: covers O.HW_AES and O.HW_DES3 of the [HWST]
- OT.Data_Confidentiality: covers O.HW_AES and O.HW_DES3 of the [HWST]
- OT.Tracing: no conflict
- OT.Sens_Data_Confidentiality: no conflict
- OT.Chip_Auth_Proof: no conflict
- 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.AC_Pers: no conflict
- OT.Prot_Malfunction: matches O.Malfunction from [PP0035]
- OT.Identification: matches O.Identification from [PP0035]

345 **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_Integrity, and OT.Data_Confidentiality.

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

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

- O.HW_DES3 (Triple DES Functionality) is mapped to OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality.
  The Triple DES (TDES) Functionality is used to ensure the integrity and the confidentiality of personal data during transmission
- O.HW_AES (AES Functionality) is mapped to OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality.
  The AES Functionality is used to ensure the integrity and the confidentiality of personal data during transmission
- O.CUST_RECONFIG (Post delivery configuration): not relevant
  This functionality is not used in TOE's OS.
- O.EEPROM_INTEGRITY: Integrity support of data stored in EEPROM
  The hardware shall provide a mechanism to support the integrity of the data stored in the EEPROM. This objective is mapped due to the used in hardware security features to OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.
- O.FM_FW: Firmware Mode Firewall (not relevant)
  This functionality is not used in TOE's OS.
- O.MEM_ACCESS: is mapped to OT.Prot_Abuse-Func
  This objective for the hardware supports the correct operation of the TOE providing memory area access control.
- O.SFR_ACCESS: is mapped to OT.Prot_Abuse-Func
  The objectives O.MEM_ACCESS and O.SFR_ACCESS support the correct operation of the TOE providing memory area access and Special Function Registers access control. Therefore these objectives are mapped to OT.Prot_Abuse-Func.

7.8.4 Compatibility: TOE Security Environment

346 Assumptions

347 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.

348 Assumptions for the TOE related to the Composite ST:

- A.Insp_Sys (Inspection Systems for global interoperability) no conflicts, as it is related to the protocol level and its correct execution of the Terminal's side.
- A.Auth_PKI (PKI for Inspection Systems) no conflict, as it is related to trustworthy installation of the PKI of Inspection Systems.
- A.Passive_Auth (PKI for Passive Authentication) no conflict, as this assumption is related only to public data of the TOE.

349 Assumptions of the Hardware PP ([PP0035]):

- A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization) is not relevant, because the Personalization of the hardware is finished after Initialization Phase.
- A.Plat-Appl (Usage of Hardware Platform) not relevant
- A.Resp-Appl (Treatment of User Data) relevant

  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.

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

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

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

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

351 Threats

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

353 Threats for the TOE related to the Composite ST:

- T.Read_Sensitive_Data no conflict
- T.Skimming no conflict
- T.Eavesdropping no conflict
- T.Tracing no conflict
- T.Forgery covers T.RND of the Smartcard IC PP [PP0035]
- T.Counterfeit no conflict
- T.Abuse-Func matches the corresponding threat of the of the Smartcard IC PP [PP0035]
- T.Information_Leakage matches T.Leak-Inherent and T.Leak-Forced of the Smartcard IC PP [PP0035]
- T.Phys-Tamper matches T.Phys-Probing and T.Phys-Manipulation of the Smartcard IC PP [PP0035]

- T.Malfunction matches corresponding threat of the Smartcard IC PP [PP0035]

354 **Threats of the hardware ST related to 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 covered by T.Information_Leakage and T.Forgery of the Composite ST.

  This threat (Deficiency of Random Numbers) is covered by T.Information_Leakage and T.Forgery because the Random Number Generator is used by the TOE for key generation and User Data protection. In case the key data is disclosed the confidentiality and integrity protection fails (for the actual session or Chip Authentication).

355 **Threats of the hardware ST ([HWST]):**

- T.Unauthorized_Access (Unauthorised Memory or Hardware Access)

  This threat is related to the partitioning of memory areas in Boot Mode, Firmware Mode, System Mode and segmentation of memory areas in User Mode. This threat is covered by the objectives O.FW_HW, O.SFR_ACCESS, and O.MEM_ACCESS of the hardware ([HWST]] and may be considered as part of the threat T.Abuse-Func of the Protection Profile [EACPassPP].

7.8.5 Organizational Security Policies

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

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

- P.Sensitive_Data no conflict
- P.Personalization no conflict as it is not related to the hardware personalization
- P.Pre-Operational covers P.Process-TOE of the hardware ST ([PP0035])
- P.Card_PKI no conflict
- P.Trustworthy_PKI no conflict
- P.Manufact covers P.Process-TOE of the hardware ST ([PP0035])
- P.Terminal no conflict

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

- P.Add-Components (Additional Specific Security Components) no conflict
  The TOE's hardware provides AES and TDES encryption/decryption and Area based Memory Access Control, Memory separation for different software parts and Special Function Register Access Control as security functionalities to the Security IC Embedded Software.
  They are used in security functionalities of the TOE and are considered in the implementation of the OS.
- P.Process-TOE ([PP0035]) is covered by P.Pre-Operational and P.Manufact of the Composite ST

7.8.6 Conclusion

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

7.9 Assurance Measures

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

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

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

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

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

Vulnerability assessment
- AVA_VAN.5 Independent Vulnerability Analysis TCOS Passport 2.1

361 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.

362 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.

363 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.

364 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.

365 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.

366 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

367 Glossary and list of acronyms is taken over from the Protection Profile [EACPassPP].

Glossary

Term	**Definition**
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [EACTR].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [ICAOSAC], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SOD and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
Agreement	This term is used in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [ICAO9303-1] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organization.
Application note	optional informative part 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 travel document's chip to store the Initialization Data and Pre-personalization Data part 1 [CC]).
Authenticity	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organization
Basic Access Control (BAC)	Security mechanism defined in [ICAO9303-1] by which means the travel document's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System with PACE protocol (BIS-PACE)	A technical system being used by an inspecting authority and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorized by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.
Biographic data (biodata)	The personalized details of the travel document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document. [ICAO9303-1]
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.
Certificate chain	a sequence defining a hierarchy certificates The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
Counterfeit	an unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO9303-1]
Country Signing CA Certificate (C_{CSCA})	certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system

Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO9303-1], 5.5.1. 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 Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EACTR].
Country Verifying Certification Authority (CVCA)	An organization enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (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 terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [EACTR]. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO9303-1]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EACTR].
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.
CV Certificate	Card Verifiable Certificate according to [EACTR].
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 Basic Access Key Derivation Algorithm	The [ICAO9303-1] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
PACE passwords	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAOSAC].
Document Details Data	Data printed on and electronically stored in the travel document 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). It carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (C_{DS}) [ICAO9303-1].
Document Signer (DS)	An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}); see [EACTR] and [ICAO9303-1]. This role is usually delegated to a Personalization Agent.
Document Verifier (DV)	An organization enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organization / inspection authority) and managing 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 Certification Authority, authorized by at least the national CVCA to issue certificates for national terminals, see [EACTR]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the TOE cannot recognize a DV as a subject; hence, it merely represents an organizational entity. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document 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 travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy).
Eavesdropper	A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.
Enrolment	the process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity [ICAO9303-1]
Travel document (elec-	The contact based or contactless smart card integrated into the plastic or paper, optical

tronic)	readable cover and providing the following application: ePassport.
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].
Extended Access Control	Security mechanism identified in [ICAO9303-1] by which means the travel document'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)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO9303-1]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all travel documents. [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 Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC 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.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO9303-1]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa, (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]
Initialization	Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document's material (IC identification data).
Inspection	The act of a State examining a travel document presented to it by a traveler (the travel document holder) and verifying its authenticity. [ICAO9303-1]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveler and verifying its authenticity and (ii) verifying the traveler as travel document holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organization.
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO9303-1]
Issuing State	The Country issuing the travel document. [ICAO9303-1]
Logical Data Structure	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO9303-1]. The capacity expansion technology used is the travel docu-

(LDS)	ment's chip.
Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [ICAO9303-1] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) 1. personal data of the travel document holder 2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 3. the digitized portraits (EF.DG2), 4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5. the other data according to LDS (EF.DG5 to EF.DG16). 6. EF.COM and EF.SOD
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 travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO9303-1] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
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]
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. 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 travel document Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [EACTR]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorization Template, - Certificate Effective Date, - Certificate Expiration Date.
ePassport application	Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes • the file structure implementing the LDS [ICAO9303-1], • the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and • the TSF Data including the definition the authentication data but except the authentication data itself. Optional biometric reference data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data. Passive (i) verification of the digital signature of the Document Security Object authentication and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [ICAOSAC]. 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 p). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
PACE Password	A password needed for PACE authentication, e.g. CAN or MRZ.
Personalization	The process by which the Personalization Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. TOE life-cycle).
Personalization Agent	An organization acting on behalf of the travel document Issuer to personalize the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [EACTR], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object 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 travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalization Data	A set of data incl. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Document Security Object). Personalization data are gathered and then written into the non-volatile memory of the TOE by the Personalization Agent in the life-cycle phase card issuing.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Cryptographic authentication key used (i) by the Personalization Agent to prove his identity and to get access to the logical travel document and (ii) by the travel document's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/EAC.
Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the travel document Application (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalized travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
Pre-personalized travel document's chip	travel document's chip equipped with a unique identifier
Receiving State	The Country to which the traveler is applying for entry. [ICAO9303-1]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO9303-1]
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
Service Provider	An official organization (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between a travel document and a terminal as required by [ICAOSAC], namely (i) PACE or BAC and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In the PP the role 'Terminal' corresponds to any terminal being authenticated by the TOE. Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
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 travel document gathered by inconspicuous (for the travel document holder) recognizing the travel document.
Travel document	Official document issued by a state or organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read, see [ICAO9303-1] (there “Machine readable travel document”).
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organization personalized the travel document.
Travel document’s Chip	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 [ISO14443] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO9303-1], sec III.
Travel document’s Chip Embedded Software	Software embedded in a travel document’s chip and not being developed by the IC Designer. The travel document’s chip Embedded Software is designed in Phase 1 and embedded into the travel document’s chip in Phase 2 of the TOE life-cycle.
Traveler	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC]).
Un-personalized travel document	The travel document that contains the travel document chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User data	All data (being not authentication data) (i) stored in the context of the ePassport application of the travel document as defined in [EACTR] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. 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	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee’s template. [ICAO9303-1]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
BAC	Basic Access Control
BIS	*Basic Inspection System*
BIS-PACE	*Basic Inspection System with PACE*
CA	*Chip Authentication*
CAN	*Card Access Number*
CC	*Common Criteria*
EAC	*Extended Access Control*
EF	*Elementary File*
ICCSN	*Integrated Circuit Card Serial Number.*
MF	*Master File*
MRZ	*Machine readable zone*
n.a.	*Not applicable*
OSP	*Organizational security policy*
PACE	*Password Authenticated Connection Establishment*
PCD	*Proximity Coupling Device*
PICC	*Proximity Integrated Circuit Chip*
PP	*Protection Profile*
PT	*Personalization Terminal*
RF	*Radio Frequency*
SAR	*Security assurance requirements*
SFR	*Security functional requirement*
SIP	*Standard Inspection Procedure*
TA	*Terminal Authentication*
TDES	*Triple DES according to* [SP800-67]*, note that other documents use also the notation 3DES*
TOE	*Target of Evaluation*
TSF	*TOE Security Functions*

Appendix Results of Cryptographic Assessment

368 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	Terminal Authentication, ECDSA-signature verification of card verifiable certificates using SHA-{1,224,256, 384, 512}	[ECCTR], [FIPS186], [FIPS180]	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[EACTR], part 3 Appendix A.6	Verification of certificates (Terminal Authentication) FCS_COP.1/SIG_VER VERIFY CERTIFICATE
2.	Authentication	PACEv2 (Generic Mapping)	[EACTR] (PACEv2), [ICAOSAC],	Length of [Nonce|=128 bit	[EACTR] part 2 sec 3.2	FIA_UID.1/PACE FIA_UAU.1/PACE FIA_UAU.4/PACE FIA_UAU.5/PACE FIA_UAU.6/PACE GENERAL AUTHENTICATE
3.	Authentication	Implicit Authentication during Secure Messaging, Triple-DES in CBC mode	[SP800-67] (DES),	112	[EACTR] [ICAOSAC]	BIS-PACE-key PACE, 1st step (opt.) FCS_COP.1/PACE_ENC FCS_COP.1/CA_ENC
4.	Authentication	Implicit Authentication during Secure Messaging, AES in CBC mode	[FIPS 197] (AES),	128, 192, 256	[EACTR] [ICAOSAC]	PACE, 1st step (opt.) FCS_COP.1/PACE_ENC FCS_COP.1/CA_ENC
5.	Authentication	Chip Authentication based on ephemeral-static ECDH	[FIPS 186]	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[EACTR], part 2 sec. 3.3 and part 3 annex A.4	FCS_CKM.1.1/CA
6.	Authentication	Terminal Authentication v.1 based on ECDSA using SHA-{1,224,256, 384, 512}	[ECCTR]	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[EACTR], part 2 sec. 3.4 and 3 annex A.6	FCS_COP.1.1/ SIG_VER EXTERNAL AUTHENTICATE
7.	Key Agreement	ECDH using SHA-{1, 256} For PACE and Chip Authentication	[FIPS 186]	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256, 320, 384, 512}r1 [RFC 5639], secp{256}r1 [FIPS186]	[EACTR], part 3 annex A.4	FCS_CKM.1/DH_PACE FCS_CKM.1/CA

8.	Confidentiality	Secure Messaging, AES/TDES in CBC mode	[FIPS197] [SP800-67]	|k|=128, 192, 256	[EACTR], part 3 annex E	FCS_COP.1/CA_ENC
9.	Integrity	Secure Messaging, AES/TDES in CMAC/Retail-MAC mode	[FIPS197] (AES), [SP800-38B] (CMAC)	|k|=128, 192, 256	[EACTR], part 3 annex E	FCS_COP.1/CA_MAC
10.	Trusted Channel	Secure messaging in ENC_MAC mode is established during PACE	[EACTR] (PACE)	-	[EACTR]	FTP_ITC.1/PACE
11.	Cryptographic Primitive	Hybrid deterministic RNG DRG.4	[AIS31]	n.a.	[ECARDTR]	FCS_RND.1
10	Cryptographic Primitive	Hash for key derivation SHA-{1,224,256, 384, 512}	[FIPS 180]	n.a.	[EACTR]	FCS_COP.1/SHA
11	Key Generation	ECDSA key generation for Chip Authentication	[ECCTR]	224, 256, 320, 384 and 512	[EACTR]	FCS_CKM.1/CA_PICC

Table 10: Cryptographic algorithms used by TCOS Passport

369 All cryptographic algorithms listed in table 10 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.

370 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 Electronic Identity Cards.

References

[AIS31]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, A proposal for Functionality classes for random number generators Version 2.0 vom 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[AIS36]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 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, 30.12.2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243

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

[BACCR]
Certification Report of the TCOS Passport Version 2.1 Release 2-BAC, BSI-DSZ-CC-0809-V2-2016: TCOS Passport Version 2.1 Release 2-BAC/P60D144, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016

[BACST]
Security Target TCOS Passport Version 2.1/Release2-BAC, Specification of the Security Target TCOS Passport Version 2.1 Release 2-BAC/P60D144, Version 2.1.2, 2016

[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, September 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

[EACTR][138]
Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents,
Part 1 – eMRTDs with BAC/PACEv2 and EACv1,

[138] The Protection Profiles refer to the version 2.05 of this Technical Guideline. The references given in the PPs are adapted in this ST to the updated version 2.10.

Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI),
Part 3 – Common Specifications, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03-20

[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

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

[FIPS186]
Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), 2013-07

[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, NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC Dedicated Software from NXP Semiconductors Germany GmbH, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016-02

[HWST]
Security Target of the underlying hardware platform, NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE , Security Target Lite Version 2.61, BSI-DSZ-CC-0978, NXP Semiconductors, 2015-10

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

[ICAOSAC]
ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, ICAO, 2010-11

[PACEPassPP]
CC Protection Profile: Machine Readable Travel Document 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, 2011-11-02

[EACPassPP]
CC Protection Profile: Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, Version 1.3.2, Registered

and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0056-V2-2012, 2012-12-05

[ISO7816]
ISO 7816-4:2005, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, ISO, 2008-10-03

[ISO9797]
ISO 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO, 2005-01-04

[ISO14443]
ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2007-2009

[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

[RFC5639]
M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[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

[SP800-67]
Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67, Revised January 2012, National Institute of Standards and Technology, 2012-01

[TCOSADM]
Administrator’s Guidance TCOS Passport Version 2.1 Release 2, T-Systems International GmbH, 2016