Security Target

Machine Readable e-Document with „ICAO Application”, Extended Access Control with PACE based on National Operating System (NOS)

NOS e-Passport (EAC with PACE) v.1.01-I

Version 1.0

Universal Information Technologies LLC

BSI-DSZ-CC-0985

Foreword

This Security Target 'Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS), NOS e-Passport (EAC with PACE) v.1.01-I' is issued by Universal Information Technologies LLC.

The document has been prepared as a Security Target following the rules and formats of Common Criteria version 3.1 [1], [2], [3], Revision 4.

For a better readability, where necessary, we notify the passages and items taken from the EAC PP [7] by [7] and from the PACE PP [8] by [8].

Universal Information Technologies LLC, Kiev, Ukraine

Contents

List of Tables

1 ST Introduction

This section provides document management and overview information required and enables a potential user of the TOE to determine, whether the TOE referred to is of interest.

1.1 ST reference

Title:	Security Target 'Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS), NOS e-Passport (EAC with PACE) v.1.01-I'
Issuer:	Universal Information Technologies LLC
Version Number:	1.0 as of 31st of August, 2018
Registration:	BSI-DSZ-CC-0985
Keywords:	ePassport, MRTD, e-Document, ICAO, PACE, EAC, SAC, National Operating System

1.2 TOE Reference

The TOE is Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS), NOS e-Passport (EAC with PACE) v.1.01-I, version 1.01, running on the microcontroller Infineon Security Controller M7892 B11 (BSI-DSZ-CC-0782-V3-2017) hosting the ePassport application as required by [7].

The TOE can be identified using GET_INFO command. The TOE returns the following value:

```
4e 4f 53 76 31 2e 30 31 2d 49 62 30 2e 33 33 64 31 37 30 32 32 30 31
 37 68
b3 3a a3 cd 85 fa 01 83
07 97 8b d1 55 a5 55 02
de d6 25 21 b5 76 18 5b
93 7d a5 20 8c 2b f8 47
```

that corresponds to ASCII notation:

`NOSv1.01-Ib0.33d17022017h<checksum>`

where:

`NOSv1.01-I` – embedded software version number;

`b0.33` – embedded software build number;

`d17022017` – date of embedded software building. Format: DDMMYYYY;

`h<checksum>` – hash value for embedded software based on cryptographic algorithm SHA-256.

1.3 TOE Overview

This Security Target defines the security objectives and requirements for the contactless smart card of machine readable electronic documents based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Password Authenticated Connection Establishment, Extended Access Control, and Chip Authentication similar to the Active Authentication in 'ICAO Doc 9303' [10].

Hereinafter in the text, the TOE defined in ch. 1.2 of the current ST, will be called as "machine readable electronic document" or "e-Document".

Explanatory note 1: In the current ST the term „Machine Readable Electronic Document" in the sense of Common Criteria is equal to „Machine Readable Travel Document" term, defined in PP [7] and 'ICAO Doc 9303' [10]. The term „Machine Readable Electronic Document" is used for the demonstration of the TOE application area extension and universalization in comparison with MRTD only.

The ePassport application is hosted on the National Operating System (NOS) running on the certified security microcontroller Infineon Security Controller M7892 B11 (BSI-DSZ-CC-0782-V3-2017 [26]) compliant with to the Protection Profile BSI-PP-0035 [9].

This microcontroller possesses both contact based and contactless interfaces. For the ePassport application, only the contactless interface is used.

The current evaluation is a composite evaluation in the sense of CCDB-2012-04-001 [5]. The TOE platform (e-Documents chip and corresponding Infineon cryptographic libraries) was certified in accordance with Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3 (see certification report [26] for details).

1.3.1 TOE definition and operational usage

The Target of Evaluation (TOE) addressed by the current Security Target is an electronic document representing a contactless smart card programmed according to ICAO Technical Report "Supplemental Access Control" [12] (which means amongst others according to the Logical Data Structure (LDS) defined in [13]) and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [10] and BSI TR-03110 [15], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011 [8].

The TOE comprises at least:

(i) the circuitry of the e-Document's chip (the integrated circuit, IC),

(ii) the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,

(iii) the IC Embedded Software (National Operating System),

(iv) the ePassport application and

(v) the associated guidance documentation.

1.3.2 TOE usage and major security features for operational use

A State or Organisation issues e-Documents to be used by the holder for person identification and/or international travel. The e-Document holder presents the e-Document to the inspection system to prove his or her identity. The e-Document in context of this Security Target contains:

(i) visual (eye readable) biographical data and portrait of the holder,

(ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and

(iii) data elements on the e-Document's chip according to LDS in case of contactless machine reading.

The authentication of the e-Document's holder is based on (i) the possession of a valid e-Document personalised for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the e-Document. The issuing State or Organisation ensures the authenticity of the data of genuine e-Document. The receiving State trusts a genuine e-Document of an issuing State or Organisation.

For this Security Target the e-Document is viewed as unit of

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

(a) the biographical data on the biographical data page of the e-Document surface,

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

(c) the printed portrait.

(ii) **the logical e-Document document** as data of the e-Document holder stored according to the Logical Data Structure as defined in [13] as specified by ICAO on the contactless integrated circuit. It presents contactlessly readable data including (but not limited to) personal data of the e-Document holder

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

(b) the digitized portrait (EF.DG2),

(c) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]

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

(e) the Document Security Object (SOD).

The issuing State or Organisation implements security features of the e-Document to maintain the authenticity and integrity of the e-Document and their data. The physical part of the e-Document and the e-Document's chip are identified by the Document Number.

[1] These biometric reference data are optional according to [10]. This ST assumes that the issuing State or Organisation uses this option and protects these data by means of extended access control.

The physical part of the e-Document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the e-Document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [10]. These security measures can include the binding of the e-Document's chip to the e-Document.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical e-Document, Active Authentication of the e-Document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [10], and Password Authenticated Connection Establishment [12]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This Security Target addresses the protection of the logical e-Document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control mechanism. This Security Target addresses the Chip Authentication Version 1 described in [15] as an alternative to the Active Authentication stated in [10].

If BAC is supported by the TOE, the e-Document has to be evaluated and certified separately. This is due to the fact that [6] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

Explanatory Note 2: The NOS implementation of Basic Access Control according to BAC-PP [6] is subject to a dedicated certification procedure.

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The e-Document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)' [8]. Note that [8] considers high attack potential.

For the PACE protocol according to [12], the following steps shall be performed:

(i) the e-Document's chip encrypts a nonce with the shared password, derived from the MRZ resp. other PACE password 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. other PACE password data data.

(iii) The e-Document's chip and terminal computer perform a Diffie-Hellman 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.

After successful key negotiation the terminal and the e-Document's chip provide private communication (secure messaging) [15], [12].

The TOE implements the Extended Access Control as defined in [15]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1. The Chip Authentication Protocol Version 1 (i) authenticates the e-Document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication Version 1 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 Version 1 can only be performed if Chip Authentication Version 1 has been successfully executed. The Terminal Authentication Protocol Version 1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organisation 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 Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.3.3 TOE life-cycle

The TOE life cycle is described in terms of the four life cycle phases (with respect to the [9], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps)[7]:

Phase 1 "Development"

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step2) The Embedded software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the ePassport application and the guidance documentation associated with these TOE components.

The Embedded Software (flash memory parts of the NOS, supporting software and guidance documentation) is securely delivered to the e-Document manufacturer.

Explanatory Note 3: According to [26] the Personalisation Agent downloads the software into the SOLID FLASH™ flash memory of Infineon M7892 B11 chip.

The manufacturing documentation of the IC including the IC Dedicated Software is securely delivered to the IC manufacturer.

Phase 2 "Manufacturing"

(Step3) In this step the TOE integrated circuit is produced containing the e-Document's chip Dedicated Software in the proprietary firmware memory. The IC manufacturer writes the flash loader IC Identification Data onto the chip to control the IC as e-Document material during the IC manufacturing and the delivery process to the e-Document manufacturer.

The IC manufacturer combines the IC with hardware for the contactless interface in the inlay.

After that the inlay and IC Identifier (transport keys) are securely delivered from the IC manufacturer to the e-Document manufacturer.

The transport keys for the IC memory access is delivered to the e-Document manufacturer by otherwise secure way.

(Step4) The e-Document manufacturer combines the inlay into the e-document (passport book etc.).

(Step5) The e-Document manufacturer (i) installs the NOS, (ii) creates the ePassport application and (iii) equips e-Document's chips with pre-personalization Data.

Explanatory Note 4: Creation of the application implies:

- For file based operating systems: the creation of MF and ICAO.DF

- For JavaCard operating systems: the Applet instantiation.

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

(Step6) The personalization of the e-Document includes (i) the survey of the e-Document holder's biographical reference data, (ii) the enrolment of the e-Document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical e-Document, (iv) the writing of the TOE User Data and TSF Data into the logical e-Document and (v) configuration of the TSF if necessary. 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.

The signing of the Document security object by the Document signer [10] finalizes the personalization of the genuine e-Document for the e-Document holder. The personalized e-Document (together with appropriate guidance for TOE use if necessary) is handed over to the e-Document holder for operational use.

Explanatory Note 5: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [1] §92) 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.

Explanatory Note 6: This security target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [10]. This approach allows but does not enforce the separation of these roles.
The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

Phase 3 "Operational Use"

(Step7) The TOE is used by the e-Document holder 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.

Explanatory Note 7: The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the ePassport application (DG 17 and subsequent data groups) in the Phase 3 "Operational Use". Data groups DG 1 - DG 16 remain unchanged and the SOD is not overwritten.

Explanatory Note 8: The typical life cycle phases for the current TOE *type* are development[2], manufacturing[3] and card issuing[4] and, finally, operational use. Operational use

[2] IC itself and IC embedded software

of the TOE is explicitly in the focus of current ST. Some single properties of the manufacturing and the card issuing life cycle phases being significant for the security of the TOE in its operational phase are also considered by the current ST. The security evaluation will involve all life cycle phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 2.3 'Package Claim' below).
The intention of the ST is to consider the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase 2. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. The national body of the issuing State or Organization is responsible for these specific production steps.

Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 3) have to be considered in the product evaluation process under AGD assurance class.

1.3.4 TOE type

The TOE type is contactless smart card with the *ePassport* application named as a whole 'electronic Passport (ePass)'.

1.3.5 Non-TOE hardware/software/firmware

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip 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 e-Document; nevertheless these parts are not inevitable for the secure operation of the TOE[7].

Explanatory Note 9: The TOE can interact with different types of inspection systems. In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless communication according to [23].

From the logical point of view, the TOE shall be able to distinguish between the following terminal types, which, hence, shall be available (see [15]):

– *Inspection System*[5]: an official terminal that is always operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier).

[3] IC manufacturing and smart card manufacturing including installation of a native card operating system

[4] including installation of the smart card application(s) and their electronic personalisation (i.e. tying the application data up to the e-Document holder)

[5] see the *Explanatory note 10* for further details

The TOE shall require the terminal of each type to authenticate itself before access according to effective terminal authorisation is granted. To authenticate a terminal as an inspection system, the related Inspection Procedures must be used.

Explanatory note 10: The specification [15] knows the following types of inspection systems (i.e. for ePassport):

– BIS-PACE: Basic Inspection System[6] with PACE[7],

– BIS-BAC: Basic Inspection System with BAC[8],

– EIS-AIP-PACE: Extended Inspection System using Advanced Inspection Procedure with PACE[9],

– EIS-AIP-BAC: Extended Inspection System using Advanced Inspection Procedure with BAC[10].

The current ST - due to compliance with [7] - defines security policy for the usage of **BIS-PACE** and **EIS-AIP-PACE** types of **inspection systems**.

Using other types of inspection systems (BIS-BAC and EIS-AIP-BAC) is out of the scope of the current ST. BIS-BAC and EIS-AIP-BAC may *functionally* be supported by the current e-Document product, but are not part of the TOE in the context of the current ST.

The authorisation level of an authenticated terminal shall be determined by the effective terminal authorisation calculated from the certificate chain presented by this terminal to the TOE[11]. All necessary certificates of the related public key infrastructure – Country Verifying Certification Authority (CVCA) Link Certificates, Document Verifiers Certificates and Inspection System (Terminal) Certificates – shall be available in a card verifiable format as specified in [16].

The following table gives an overview which types of terminals shall be supported for the *ePassport* application of the TOE, see [15] (please note that the effective ability of a terminal depends on its terminal authorisation level finally derived from the presented certificate chain as stated above):

	Basic Inspection System using SIP with PACE (BIS-PACE, official terminal)	Extended Inspection System using AIP with PACE (EIS-AIP-PACE, official terminal)

[6] A Basic Inspection Systems (BIS) always uses Standard Inspection Procedure (SIP).

[7] SIP with PACE means: PACE and passive authentication with SO_D according to [15].

[8] SIP with BAC means: BAC and passive authentication with SO_D according to [15]. It is commensurate with BIS in [6] and [7]; i.e. the terminal proven the possession of MRZ optically read out from the plastic part of the card.

[9] Advanced Inspection Procedure (AIP) with PACE means: PACE, Chip Authentication Version 1, Passive Authentication with SO_D and Terminal Authentication Version 1 according to [15]

[10] AIP with BAC means: BAC, Chip Authentication Version 1, Passive Authentication with SO_D and Terminal Authentication Version 1 according to [15]. It is commensurate with EIS in [6] and [7]; please note that this EIS in the sense of [6].

[11] It is based on Certificate Holder Authorization Template (CHAT), see [16]. A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the ePass holder's restricting input at the terminal. This final CHAT reflects the *effective authorisation level*, see [16].

	Basic Inspection System using SIP with PACE (BIS-PACE, official terminal)	Extended Inspection System using AIP with PACE (EIS-AIP-PACE, official terminal)
ePassport	Operations: reading all data groups excepting DG3 and DG4 User interaction: PACE password (e.g. MRZ or other PACE password)	Operations: reading only DG3 and DG4 and optional DG5-DG13[12] User interaction: PACE password (e.g. MRZ or other PACE password)

Table 1: ePassport application vs. terminal types

1.4 TOE Description

The physical scope of the TOE has already been described in sec. 1.3.1.

The logical scope of the TOE is described by the purpose of TOE as a Machine Readable Electronic Document with „ICAO Application" using Extended Access Control with PACE. The TOE offers all the related security services as specified in [12] and [15].

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

- Only terminals possessing valid authorisation information can get access to the user data stored on the TOE and use security functionality of the ePass under control of the ePass holder,
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and inspecting governmental organisation connected,
- Averting of inconspicuous tracing of the ePass,
- Self-protection of the TOE security functionality and the data stored inside.

[12] cf. table 3 in [15].

2 Conformance Claims

2.1 CC Conformance Claim

This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2012-09-001, Version 3.1, revision 4, September 2012, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2012-09-002, Version 3.1, revision 4, September 2012, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2012-09-003, Version 3.1, revision 4, September 2012, [3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation. Evaluation methodology; CCMB-2012-09-004, Version 3.1, revision 4, September 2012, [4]

has to be taken into account.

2.2 PP Claim

This ST claims strict conformance to the BSI-CC-PP-0056-V2-2012, version 1.3.2, 5th December 2012 [7].

Explanatory Note 11: Part of the security policy for the *ePassport* application of the TOE is contextually in a tight connection with the protection profile 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, version 1.10, 25th March 2009' [6], however the ST does not claim any formal conformance to it. The main reason for this decision is that the current ST does not cover BAC, though a product in question may functionally implement it. The NOS implementation of Basic Access Control according to BAC-PP [6] is subject to a dedicated certification procedure.

2.3 Package Claim

The current ST is conformant to the following security requirements package:

– Assurance package EAL4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in the CC, part 3 [3].

2.4 Conformance Claim Rationale

The current ST claims *strict* conformance to the ICAO-EAC PP [7].

TOE Type

The PP [7] does not explicitly state any TOE type, but it can be inferred from the TOE definition in sec. 1.1 there: '... TOE ... is an electronic travel document representing a contactless / contact smart card programmed according to ICAO Technical Report "Supplemental Access Control" [12]'.

This TOE type is obviously commensurate with the current TOE type in the part being provided by the ePassport application, see sec. 1.3.1 and 1.3.4 above.

SPD Statement

The security problem definition (SPD) of the current ST contains the security problem definition of the PP [7]. The current SPD includes the same threats, organisational security policies and assumptions as for the TOE in [7].

Security Objectives Statement

The security objectives statement for the TOE in the current ST includes all the security objectives for the TOE of the PP [7], see chap. 4.1 below.

The security objectives statement for the TOE's operational environment in the current ST includes all security objectives for the operational environment of the PP [7], see chap. 4.2 below.

Security Requirements Statement

The PP [7] conforms to CC v3.1, revision 3, the current ST – to CC v3.1, revision 4. In respect to this, it is to rely on the statement of CCMB that respective assurance levels achieved by applying different CC revisions are equivalent to each other.

The SFR statement for the TOE in the current ST includes all the SFRs for the TOE of the PP [7], see chap. 6.1 below.

The SAR statement for the TOE in the current ST includes all the SARs for the TOE of the PP [7] as stated in chap. 6.2 below.

Explanatory note 12: Strict conformance allows that the security requirements for the TOE of the current ST may be hierarchically stronger than those items of each PP to which the conformance is being claimed.

Explanatory note 13: The EAC PP [7] refers to version 2.10 of TR-03110 as of 20.03.2012. This ST refers to version 2.20 of TR-03110 as of 26.02.2015. Since version 2.20 is downward compatible with version 2.10, this deviation does not weaken the TOE security functionality required by [7].

3 Security Problem Definition

3.1 Introduction

Assets[7], [8]

Assets to be protected by the security policy of the current ST are inherited from [7] and [8].

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

Object No.	Asset	Definition	[8]Generic security property to be maintained by the current security policy (inherited from [8])
ePassport			
1	user data stored on the TOE[8]	All data (being not authentication data) stored in the context of the *ePassport* application of the ePass as defined in [15] and being allowed to be *read out* solely by an authenticated terminal acting as Inspection System (in the sense of [15]). This asset covers 'User Data on the e-Document's chip', 'Logical e-Document Data' and 'Sensitive User Data' in [6].	Confidentiality[13] Integrity Authenticity
2	user data transferred between the TOE and the terminal connected[8]	All data (being not authentication data) being transferred in the context of the *ePassport* application of the ePass as defined in [15] between the TOE and an authenticated terminal acting as Inspection System (in the sense of [15]). User data can be received and sent (exchange ⇔ {receive, send}).	Confidentiality[14] Integrity Authenticity
3	ePass tracing data[8]	Technical information about the current and previous locations of the ePass gathered by inconspicuous (for the ePass	unavailability[15]

[13] Though not each data element stored on the TOE represents a secret, the specification [15] anyway requires securing their confidentiality: only terminals authenticated according to [15] (PCT) can get access to the user data stored.

[14] Though not each data element being transferred represents a secret, the specification [15] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [15].

[15] Represents a prerequisite for anonymity of the ePass holder

Object No.	Asset	Definition	[8]Generic security property to be maintained by the current security policy (inherited from [8])
		holder) recognising the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.	
4	logical e-Document sensitive User Data[7]	Sensitive biometric reference data (EF.DG3, EF.DG4) *Explanatory Note 14*: Please note that user data being referred to above include, amongst other, individual-related (personal) data of the ePass holder which also include his sensitive (biometrical) data (EF.DG3, EF.DG4).	Confidentiality[16] Integrity Authenticity

Table 2: Primary assets

Explanatory Note 15: Due to interoperability reasons the 'ICAO Doc 9303' [10] requires that Basic Inspection Systems may have access to logical e-Document data DG1, DG2, DG5 to DG16. The TOE is **not** in certified mode, if it is accessed using BAC [10]. Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [6]). If supported, it is therefore recommended to use PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication Version 1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks.

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

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	[8]Property to be maintained by the current security policy (inherited from [8])
ePassport			
5	Accessibility to the TOE functions and data only for	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability[17]

[16] Though not each data element stored on the TOE represents a secret, the specification [15] anyway requires securing their confidentiality: only terminals authenticated according to [15] (PCT) can get access to the user data stored.

[17] In the sense 'exist'

Object No.	Asset	Definition	[8]Property to be maintained by the current security policy (inherited from [8])
	authorised subjects[8]		
6	Genuineness of the TOE[8]	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the e-Document's chip' in [6].	Availability[18]
7	TOE intrinsic (immanent) secret cryptographic keys[8]	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
8	TOE immanent non-secret cryptographic material[8]	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
9	e-Document communication establishment authorisation data [8]	Restricted-revealable[19] authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to convey to it.	Confidentiality[19] Integrity
10	Authenticity of the e-Document's chip[7]	The authenticity of the e-Document's chip personalised by the issuing State or Organisation for the ePass holder is used by him to prove his possession of a genuine e-Document.	Availability[20]

Table 3: Secondary assets

Explanatory Note 16: Since the ePass does not support any secret ePass holder authentication data and the latter may reveal, if necessary, his or her verification values of PACE

[18] in the sense 'exist'

[19] The ePass holder may reveal, if necessary, his or her verification values of MRZ or other PACE password to an authorised person or device who definitely act according to respective regulations and are trustworthy.

[20] in the sense 'exist'

password to an authorised person or device, a successful PACE-authentication of a terminal does not unambiguously mean that the ePass holder is using TOE. Please note that the PACE password is not to convey to the TOE.

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

Subjects and external entities [7], [8]

This Security Target considers the following external entities and subjects inherited from [7] and [8]:

External Entity No.	Subject No.	Role	Definition
1	1	ePass holder[8]	A person for whom the ePass Issuer has personalised the e- ePass[21]. This entity is commensurate with 'MRTD Holder' in [6]. Please note that an ePass holder can also be an attacker (s. below).
2	-	ePass presenter[8]	A person presenting the ePass to a terminal[22] and claiming the identity of the ePass holder. This external entity is commensurate with 'Traveller' in [6]. Please note that an ePass presenter can also be an attacker (s. below).
3	2	Terminal[8], [7]	A terminal is any technical system communicating with the TOE through the contactless interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated (PCT) ('Terminal' is used by the ePass presenter). This entity is commensurate with 'Terminal' in [6].
4 *Explanatory Note 17*: This terminal type is implicitly addressed in [8] as 'PACE	3	PACE Terminal (PCT)	A technical system verifying correspondence between the passwords stored in the ePass and the related value presented to the terminal by the ePass presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ePass using a shared password (PACE password). A PCT is allowed reading 'User Data stored in the TOE' excepting DG3 and DG4 (see [15]).

[21] i.e. this person is uniquely associated with a concrete electronic Passport

[22] in the sense of [15]

External Entity No.	Subject No.	Role	Definition
authenticated terminal', but not explicitly defined as the related role. Since the TOE type addressed in this ST is able to recognise this role (by a successful PACE authentication), we formally added this role here.			
5	4	Basic Inspection System with PACE (BIS-PACE) [8]	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ePass presenter as the ePass holder (for *ePassport*: by comparing the real biometrical data (face) of the ePass presenter with the stored biometrical data (DG2) of the ePass 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. *Explanatory Note 18*: The Basic Inspection System with PACE is a PACE authenticated terminal (PCT) additionally supporting/applying the Passive Authentication protocol and is authorised[23] by the ePass Issuer through the Document Verifier of receiving state to read a subset of data stored on the ePass. BIS-PACE and PACE authenticated terminal (PCT) possess same Terminal Authorisation Level. BIS-PACE in the context of [15] (and of the current ST) is similar, but not equivalent to the Basic Inspection System (BIS) as defined in [6].

[23] By organisational measures

External Entity No.	Subject No.	Role	Definition
6	5	Extended Inspection System (EIS)[7]	A technical system performing the Advanced Inspection Procedure[24] and therefore (i) containing a terminal for the communication with the travel document's chip, (ii) implementing the terminals part of PACE (and/or BAC); (iii) getting the authorization to read the logical travel document either under PACE (or BAC) by optical reading the travel document providing this information. (iv) implementing the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [15] and (v) being authorized by the issuing State or Organisation 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. *Explanatory Note 19:* A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ePass presenter as the e ePass holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the ePass presenter with the stored biometrical data (DG2 – DG4) of the ePass holder). EIS-AIP-PACE is a PCT additionally supporting/applying Chip Authentication Version 1, the Passive Authentication and Terminal Authentication Version 1 protocols and is authorised[25] by the ePass Issuer through the Document Verifier of receiving state to read a subset of data stored on the ePass. EIS-AIP-PACE in the context of [15] (and of the current ST) is equivalent to the Extended Inspection System (EIS) as defined in [7].
7	6	Document Verifier (DV)[7]	An organisation enforcing the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the

[24] In this ST: only with PACE (EIS-AIP-PACE). Advanced Inspection Procedure (AIP) with PACE means: PACE, Chip Authentication Version 1, Passive Authentication with SO_D and Terminal Authentication Version 1 according to [15].

[25] By issuing Inspection System (Terminal) certificates

External Entity No.	Subject No.	Role	Definition
			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 Organisations in the form of the Document Verifier Certificates. *Explanatory Note 20:* An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Inspection System (Terminal) Certificates. A Document Verifier is therefore a CertA, authorised by at least the national CVCA to issue certificates for national terminals, see [15]. Please note that while using Standard Inspection Procedure, the TOE cannot recognise a DV as a subject, because the SIP does not imply any certificate-based terminal authentication; in this case DV merely represents an organisational entity within this ST. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the ePass Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement[26] between the ePass Issuer und a foreign CVCA ensuring enforcing the ePass Issuer's privacy policy[27]). This external entity is commensurate with 'Document Verifier' in [6].
8	7	Country Verifying Certification Authority (CVCA)[7]	An organisation enforcing the privacy policy of the issuing State or Organisation with respect to the protection of sensitive biometric reference data stored in the e-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-

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

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

External Entity No.	Subject No.	Role	Definition
			Certificates, see [15]. *Explanatory Note 21:* Please note that while using Standard Inspection Procedure, the TOE cannot recognise a CVCA as a subject, because the SIP does not imply any certificate-based terminal authentication; in this case CVCA merely represents an organisational entity within this ST. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [10]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [15].
9	-	Document Signer (DS) [8]	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the ePass for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [15] and [10]. This role is usually delegated to a Personalisation Agent.
10	-	Country Signing Certification Authority (CSCA) [8]	An organisation enforcing the policy of the ePass Issuer with respect to confirming correctness of user and TSF data stored in the ePass. The CSCA represents the country specific root of the PKI for the ePass 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. [10]. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [10]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [15].
11	8	Personalisation Agent[8]	An organisation acting on behalf of the ePass Issuer to personalise the ePass for the ePass holder by some or all of the following activities: (i) establishing the identity of the ePass holder for the biographic data in the ePass, (ii) enrolling the biometric reference data of the ePass holder, (iii) writing a subset of these data on the physical Passport (optical personalisation) and

External Entity No.	Subject No.	Role	Definition
			storing them in the ePass (electronic personalisation) for the ePass holder as defined in [15], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [10] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the ePass Issuer. This entity is commensurate with 'Personalisation agent' in [6].
12	9	Manufacturer[8]	Generic term for the IC Manufacturer producing integrated circuit and the ePass Manufacturer completing the IC to the ePass. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase[28]. The TOE itself does not distinguish between the IC Manufacturer and ePass Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [6].
13	-	Attacker[8]	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most *high* attack potential. [7]Concretely, a threat agent tries (i) to manipulate the logical e-Document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine e-Document, or (iv) to trace a e-Document, see [7]. Please note that the attacker might 'capture' any subject role recognised by the TOE. This external entity is commensurate with 'Attacker' in [6].

Table 4: Subjects and external entities[29]

[28] Cf. also sec. 1.3.4 above

[29] This table defines external entities and subjects in the sense of [1]. Subjects can be recognised 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 [1]). From this point of view, the TOE itself perceives only 'subjects' and, for them, does not differ between 'subjects' and 'external entities'. There is no

Explanatory Note 22: Since the TOE does not use BAC, a Basic Inspection System with BAC (BIS-BAC)[30] as well as an Extended Inspection System using Advanced Inspection Procedure with BAC (EIS-AIP-BAC)[31] cannot be recognised by the TOE.

3.2 Threats

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

The following threats are defined in the current ST (they completely and accurately repeat the threats defined in ICAO-EAC PP [7]):

T.Skimming[8] **Skimming ePass / Capturing Card-Terminal Communication**

Adverse action: 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.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical travel document data.

Explanatory Note 23: 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 might be averted only with respect to a selected data groups (DG3, DG4) within the ePassport application, but it is out of the scope of the current ST; see also the *Explanatory note 10* above.

Explanatory Note 24: This threat also covers the item T.Read_Sensitive_Data in the ICAO-EAC PP [7]: sensitive biometric reference data stored on the ePass are part of the asset *user data stored on the TOE*. Knowledge of the Document Basic Access Keys is here not applicable, because the TOE does not cover the BAC protocol and, therefore, the Document Basic Access Keys are not existent for the TOE.

Explanatory Note 25: MRZ is printed and other PACE passwords may be printed or stuck on the Passport. Please note that neither MRZ nor PACE passwords effectively represent secrets, but are restricted-revealable, cf. OE.Card-Holder.

---

dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognised by the TOE.

[30] SIP (Standard Inspection procedure) with BAC means: BAC and passive authentication with SO_D according to [15]. It is commensurate with BIS in [6] and [7]; i.e. the terminal proven the possession of MRZ optically read out from the plastic part of the card.

[31] AIP (Advanced Inspection procedure) with BAC means: BAC, Chip Authentication Version 1, Passive Authentication with SO_D and Terminal Authentication Version 1 according to [15]. It is commensurate with EIS in [6].

T.Read_Sensitive_Data[7] **Read the sensitive biometric reference data**

Adverse action: An attacker tries to gain the sensitive biometric reference data (DG3 and DG4) through the communication interface of the e-Document's chip.

The attack T.Read_Sensitive_Data is similar to the threat T.Skimming in respect of the attack path (communication interface) and the motivation (to get data stored on the e-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 shared password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the e-Document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the e-Document as well.

Threat agent: having high attack potential, knowing the PACE Password (i.e. PACE shared password), being in possession of a legitimate e-Document.

Asset: confidentiality of logical e-Document sensitive user data (i.e. sensitive biometric reference data).

T.Eavesdropping[8] **Eavesdropping on the communication between the TOE and the PACE terminal**

Adverse action: An attacker is listening to the communication between the ePass and the PACE authenticated BIS-PACE terminal in order to gain the *user data transferred between the TOE and the terminal connected*.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical travel document data.

Explanatory Note 26: 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 might be averted only with respect to a selected data groups (DG3, DG4) within the ePassport application, but it is out of the scope of the current ST; see also the *Explanatory note 10* above.

T.Tracing[8] **Tracing ePass**

Adverse action: An attacker tries to gather *TOE tracing data* (i.e. to trace the movement of the ePass) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: privacy of the travel document holder.

Explanatory Note 27: 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 this ST, see also the *Explanatory note 10* above.

T.Counterfeit[7] **Counterfeit of e-Document chip data**

Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine e-Document's chip to be used as part of a counterfeit e-Document. This violates the authenticity of the e-Document's chip used for authentication of a document holder by possession of a e-Document.

The attacker may generate a new data set or extract completely or partially the data from a genuine e-Document's chip and copy them to another appropriate chip to imitate this genuine e-Document's chip.

Threat agent: having high attack potential, being in possession of one or more legitimate e-Document.

Asset: authenticity of user data stored on the TOE.

Explanatory Note 28: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the ePass'es chip (no Chip Authentication), the threat T.Counterfeit (counterfeiting ePass) cannot be averted by the current TOE while using the Standard Inspection Procedure.

T.Forgery[8] **Forgery of Data**

Adverse action: An attacker fraudulently alters the *User Data* or/and *TSF-data stored on the ePass* or/and *exchanged between the TOE and the terminal connected* in order to outsmart the PACE authenticated Inspection System by means of changed ePass 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.

Threat agent: Having high attack potential.

Asset: Integrity of the travel document.

T.Abuse-Func[8] **Abuse of Functionality**

Adverse action: 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 initialisation and personalisation in the operational phase after delivery to the ePass holder.

Threat agent: Having high attack potential, being in possession of one or more legitimate e-Documents.

Asset: Integrity and authenticity of the e-Document, availability of the functionality of the e-Document.

Explanatory Note 29: 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[8] **Information Leakage from ePass**

Adverse action: 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 ePass* 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.

Threat agent: Having high attack potential.

Asset: Confidentiality of User Data and TSF-data of the travel document.

Explanatory note 30: 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 **t**ransmission, 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 Differential Electromagnetic Analysis (DEMA) and 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[8] **Physical Tampering**

Adverse action: An attacker may perform physical probing of the ePass in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the ePass in order to alter (i) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the ePass.

Threat agent: Having high attack potential, being in possession of one or more legitimate e-Documents.

Asset: Integrity and authenticity of the travel document, availability of the functionality of the e-Document, confidentiality of User Data and TSF-data of the e-Document.

Explanatory Note 31: 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 ePass) 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 a direct interaction with the ePass'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[8] **Malfunction due to Environmental Stress**

Adverse action: An attacker may cause a malfunction the ePass'es 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 ePass outside the normal operating conditions, exploiting errors in the ePass'es Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: Having high attack potential, being in possession of one or more legitimate e-Documents, having information about the functional operation.

Asset: Integrity and authenticity of the e-Document, availability of the functionality of the e-Document, confidentiality of User Data and TSF-data of the e-Document.

Explanatory Note 32 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 TOE's internals.

3.3 Organisational Security Policies

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

The following OSPs are defined in the current ST (they completely and accurately repeat the OSPs defined in ICAO-EAC PP [7]).

P.Manufact[8] **Manufacturing of the *e-Document's* chip**

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

P.Pre-Operational[8] **Pre-operational handling of the ePass**

1) The ePass Issuer issues the ePass and approves using the terminals complying with all applicable laws and regulations.

2) The ePass Issuer guarantees correctness of the user data (amongst other of those, concerning the ePass holder) and of the TSF-data permanently stored in the TOE[32].

3) The ePass Issuer uses only such TOE's technical components (IC) which enable traceability of the ePass in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. sec. 1.3.4 above.

4) If the e-Document Issuer authorises a Personalisation Agent to personalise the ePass for ePass holders, the ePass Issuer has to ensure that the Personalisation Agent acts in accordance with the ePass Issuer's policy.

P.Card_PKI[8] **PKI for Passive Authentication (issuing branch)**

Explanatory Note 33: The description below states the responsibilities of 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 ePass Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the ePass. For this aim, he runs a Country Signing Certification Authority (CSCA). The ePass Issuer shall publish the CSCA Certificate (C_{CSCA}).
Explanatory Note 34: The ePass Issuer shall make C_{CSCA} and the Document Signer Certificates (C_{DS}) available to the CVCAs under agreement[33] (who shall finally distribute them to their terminals).

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 ePass Issuer by strictly secure means, see [10], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the ePass Issuer, see [10], 5.5.1.

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 Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of the ePasses.

P.Trustworthy_PKI[8] **Trustworthiness of PKI**

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

P.Terminal[8] **Abilities and trustworthiness of terminals**

[32] cf. Table 2 and Table 3 above

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

Explanatory Note 35: The ePass Issuer usually runs a domestic Country Verifying Certification Authority (domestic CVCA) and may use already existing foreign CVCAs[34]. However, for Standard Inspection Procedure, there is only issuing PKI branch. Hence, the related infrastructure (CVCAs, DVs) shall only be used for distributing C_{CSCA} and C_{DS} to the terminals of the BIS with PACE. Therefore, CVCAs and DVs represent merely organisation entities from the TOE's point of view.

The Basic Inspection Systems with PACE (BIS-PACE) participating in the current PKI[35] (and, hence, acting in accordance with the policy of the related DV) shall operate their terminals as follows:

1) The related terminals (basic inspection system, cf. Table 1 above) shall be used by terminal operators and by ePass holders as defined in [15].

2) They shall implement the terminal parts of the PACE protocol [10], of the Passive Authentication [12] and use them in this order[36]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellman).

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 *ePassport*, [10]).

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, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

P.Sensitive_Data[7] **Privacy of sensitive biometric reference data**

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the *e-Document* holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the *e-Document* is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation 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 *e-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 Version 1.

---

[34] In this case there shall be an appropriate agreement between the ePass Issuer und a foreign CVCA ensuring enforcing the ePass Issuer's privacy policy. Existence of such an agreement may technically be reflected by means of issuing a C_{CVCA} for the Public Key of the foreign CVCA signed by the domestic CVCA.

[35] For Standard Inspection Procedure, there is only issuing PKI branch; the receiving branch is completely absent.

[36] This order is only commensurate with the branch leftmost in Fig. 3.1 of [15]. Other branches of this figure are not covered by the security policy of the current ST.

P.Personalisation[7] **Personalisation of the *e-Document* by issuing State or Organisation only**

The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical *e-Document* with respect to the *e-Document* holder. The personalisation of the *e-Document* for the holder is performed by an agent authorized by the issuing State or Organisation only.

3.4 Assumptions

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

The following assumptions are defined in the current ST (they completely and accurately repeat the OSPs defined in ICAO-EAC PP [7]):

A.Passive_Auth[8] **PKI for Passive Authentication**

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical e-Document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the e-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 [10].

Explanatory Note 36: The assumption A.Passive_Auth is equivalent with OSP P.Card_PKI above.

A.Insp_Sys[7] **Inspection Systems for global interoperability**

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [12] and/or BAC [6]. BAC may only be *functionally* used if supported by the ePass product. If both PACE and BAC are supported by the ePass product and the inspection system, PACE must be used. The EIS reads the logical e-Document under PACE or BAC and performs the Chip Authentication Version 1 to verify the logical *e-Document* and establishes secure messaging. EIS supports the Terminal Authentication Protocol Version 1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Justification:

The assumption A.Insp_Sys does not confine the security objectives of the [8] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality of the TOE.

A.Auth_PKI[7] **PKI for Inspection Systems (receiving branch for using the Advanced Inspection Procedure)**

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities (CVCA), the Document Verifier (DV) 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 Organisations are signing the certificates of the Document Verifier (C_{DV}) and the Document Verifiers are signing the certificates of the Extended Inspection Systems (C_{IS}) of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their e-Document's chip.

Explanatory Note 37: Additionally, an inspection authority shall (i) generate the Terminal (Inspection System) Authentication Key Pairs {SK_{IS}, PK_{IS}}, (ii) hand over the Terminal Authentication Public Keys (PK_{IS}) to the DV for certification, (iii) keep the Terminal Authentication Private Keys (SK_{IS}) secret, (iv) securely use the Terminal Authentication Private Keys for the Terminal Authentication as defined in [15] and (v) install C_{IS}, C_{DV} and C_{CVCA} in the rightful terminals operated by him.

Justification:

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 [8] 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 Version 1.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

The following TOE objectives are defined in the current ST (they completely and accurately repeat the OTs defined in ICAO-EAC PP [7]).

OT.Data_Integrity[8] **Integrity of Data**

The TOE must ensure integrity of the User Data and the TSF-data[37] stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).
The TOE must ensure integrity of the User Data and the TSF-data[37] during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE (PCT)) after the PACE Authentication.

OT.Data_Authenticity[8] **Authenticity of Data**

The TOE must ensure authenticity of the User Data and the TSF-data[38] stored on it by enabling verification of their authenticity at the terminal-side[39].
The TOE must ensure authenticity of the User Data and the TSF-data[38] during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE (PCT)) after the PACE 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 TOE)[40].

OT.Data_Confidentiality[8] **Confidentiality of Data**

The TOE must ensure confidentiality of the User Data and the TSF-data[41] by granting read access only to the PACE authenticated BIS-PACE (PCT) terminal connected.
The TOE must ensure confidentiality of the User Data and the TSF-data[41] during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE (PCT)) after the PACE Authentication.

Explanatory note 38: Since the Standard Inspection Procedure does not support any certificate-based authorisation of the terminal connected (no CHAT), the

[37] Where appropriate, see Table 3 above

[38] Where appropriate, see Table 3 above

[39] Verification of SO_D

[40] Secure messaging after the PACE authentication, see also [15]

[41] Where appropriate, see Table 3 above

effective terminal authorisation level is firmly predefined as specified in [15] (option PACE) and cannot additionally be restricted by the ePass holder. This fixed effective terminal authorisation level for the Standard Inspection Procedure does not allow any access to sensitive biometrical data (DG3, DG4).

OT.Sens_Data_Conf[7] **Confidentiality of sensitive biometric reference data**

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to an 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 Organisation. The TOE must ensure the confidentiality of the logical *e-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.Tracing[8] **Tracing ePass**

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

OT.Chip_Auth_Proof[7] **Proof of the *e-Document's* chip authenticity**

The TOE must support the Inspection Systems to verify the identity and authenticity of the e-Document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in [15]. The authenticity proof provided by e-Document's chip shall be protected against attacks with high attack potential.

Explanatory note 39: The OT.Chip_Auth_Proof implies the e-Document's chip to have (i) a unique identity as given by the e-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 e-Document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the e-Document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [10] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

Explanatory note 40: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the e-Document's chip (no Chip Authentication), a security objective OT.Chip_Auth_Proof (proof of ePass authenticity) cannot be achieved by the current TOE while using the Standard Inspection Procedure.

OT.Prot_Abuse-Func[8] **Protection against Abuse of Functionality**

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[8] **Protection against Information Leakage**

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

- 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.

Explanatory note 41: 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[8] **Protection against Physical Tampering**

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the ePass'es 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[8] **Protection against Malfunctions**

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have 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.

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

OT.Identification[8] **Identification of the TOE**

The TOE must provide means to store Initialisation[42] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the ePass. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

OT.AC_Pers[8] **Access Control for Personalisation of logical e-Document**

The TOE must ensure that the logical e-Document data in EF.DG1 to EF.DG16[43], the Document Security Object according to LDS [10] and the TSF-data permanently stored in the TOE can be written by authorised Personalisation Agents only. The logical e-Document data in EF.DG1 to EF.DG16 and the TSF-data may be written only during and cannot be changed after personalisation of the document.

4.2 Security Objectives for Operational Environment

I. ePass Issuer as the general responsible

The ePass Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

The following environmental objectives are defined in the current ST (they completely and accurately repeat the OEs defined in ICAO-EAC PP [7]).

OE.Legislative_Compliance[8] **Issuing e-Document**

The ePass Issuer must issue the ePass and approve using the terminals complying with all applicable laws and regulations.

II. ePass Issuer and CSCA: e-Document's PKI (issuing) branch

The ePass Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the *Explanatory Note 33* above):

OE.Auth_Key_Travel_Document[7] ***e-Document* Authentication Key**

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the e-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 Organisations to verify the authenticity of the e-Document's chip used for genuine *e-Document* by certification of the Chip Authentication

[42] amongst other, IC Identification data

[43] User Data, amongst other those concerning the ePass holder biographical and biometrical data

Public Key by means of the Document Security Object.

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in this Protection Profile and not in [8].

OE.Passive_Auth_Sign[8] **Authentication of ePass by Signature**

The ePass Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the ePass Issuer must (i) generate a cryptographically 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})[44]. Hereby authenticity and integrity of these certificates are being maintained.
A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically 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 ePasss in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [10]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [10].
The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects having to be stored on ePasss.

OE.Personalisation[8] **Personalisation of ePass**

The ePass Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the ePass holder and create the biographical data for the ePass, (ii) enrol the biometric reference data of the ePass holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the ePass (electronic personalisation) for the ePass holder as defined in [10][45], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [10] (in the role of a DS).

III. ePass Issuer and CVCA: Terminal's PKI (receiving) branch

The ePass Issuer and the related domestic CVCA as well as the foreign CVCAs under agreement (with the ePass Issuer) will implement the following security objectives for the TOE environment:

OE.Terminal[8] **Terminal operating**

[44] i.e. shall make the Certificate of the CSCA Public Key (C_{CSCA}) and the Document Signer Certificates (C_{DS}) available to the ePass Issuer, who makes them available to his own (domestic) CVCA as well as to the foreign CVCAs under agreement. CVCAs represent the roots of receiving branch.

[45] see also [15]

The terminal operators (inspection authorities) participating in the current PKI (and, hence, acting in accordance with the policy of the related DV) must operate their terminals as follows:

a) Basic Inspection System using Standard Inspection Protocol with PACE (BIS-PACE)

1) The related terminals (BIS, cf. Table 1 above) are used by terminal operators and by ePass holders as defined in [10] (see also [15]).

2) The related terminals implement the terminal parts of the PACE protocol [12] (see also [15]), of the Passive Authentication [15] (by verification of the signature of the Document Security Object; see also [15]) and use them in this order[46]. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellman).

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 ePass (determination of the authenticity of data groups stored in the *ePassport* [10], see also [15]).

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, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

b) Extended Inspection System using Advanced Inspection Procedure with PACE (EIS-AIP-PACE)

For EIS-AIP-PACE see OE.Authoriz_Sens_Data below.

OE.Exam_e-Document[7] **Examination of the physical part of the e-Document**

The inspection system of the receiving State or Organisation must examine the e-Document presented by the document presenter to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the e-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 Organisation, and (ii) implements the terminal part of PACE [12] and/or the Basic Access Control [10]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented e-Document's chip.

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [8] and therefore also counters T.Forgery and A.Passive_Auth from [8]. This is done because a new

[46] This order is only commensurate with the branch leftmost in Fig. 1 in [15].

type of Inspection System is introduced in this PP as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

OE.Authoriz_Sens_Data[7] **Authorization for Use of Sensitive Biometric Reference Data**

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

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in this Protection Profile and not in [8].

OE.Ext_Insp_Systems[7] **Authorization of Extended Inspection Systems**

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

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

OE.Prot_Logical_Travel_Document[7] **Protection of data from the logical e-Document**

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical *e-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 Version 1.

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

IV. ePass holder Obligations

OE.e-Document_Holder[8] ***ePass* holder Obligations**

The ePass Holder may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device who definitely act according to respective regulations and are trustworthy.

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for sufficiency and necessity of the objectives defined. 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.Identification	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Sens_Data_Conf	OT.Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Auth_Key_Travel_Document	OE.Exam_Travel_Document	OE.Authoriz_Sens_Data	OE.Ext_Insp_Systems	OE.Prot_Logical_Travel_Document	OE.Travel_Document_Holder	OE.Legislative_Compliance
T.Skimming			x	x	x																x	
T.Read_Sensitive_Data						x												x	x			
T.Eavesdropping					x																	
T.Tracing							x														x	
T.Counterfeit								x								x	x					
T.Forgery		x	x	x					x		x		x	x	x		x					
T.Abuse-Func									x													
T.Information_Leakage										x												
T.Phys-Tamper											x											
T.Malfunction												x										
P.Manufact	x																					
P.Pre-Operational	x	x											x									x
P.Terminal															x		x					
P.Card_PKI														x								
P.Trustworthy_PKI														x								
P.Sensitive_Data						x												x	x			
P.Personalisation	x	x											x									
A.Insp_Sys																	x			x		

	OT.Identification	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Sens_Data_Conf	OT.Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Auth_Key_Travel_Document	OE.Exam_Travel_Document	OE.Authoriz_Sens_Data	OE.Ext_Insp_Systems	OE.Prot_Logical_Travel_Document	OE.Travel_Document_Holder	OE.Legislative_Compliance
A.Auth_PKI																		x	x			
A.Passive_Auth														x								

Table 5: Security Objective Rationale

A detailed justification required for *suitability* of the security objectives to coup with the security problem definition is given below.

Since all the security objectives, threats, OSPs and assumptions in the current ST completely and accurately repeat all the related items defined in ICAO-EAC PP [7], the related rational given and certified in [7] is also valid for the current ST.

5 Extended Components Definition

This ST includes all Extended Component Definitions from the ICAO-EAC PP [7] chap. 5, namely FAU_SAS.1, FCS_RND.1, FIA_API.1, FMT_LIM.1, FMT_LIM.2, FPT_EMS.1. These definitions are taken over as described in [7], therefore they are not repeated here.

6 Security Requirements

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.

The CC allows several operations to be performed on security requirements (on the component level); *refinement*, *selection*, *assignment* and *iteration* are defined in sec. 8.1 of Part 1 [1] of the CC. Each of these operations is used in this ST.

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 words are ~~crossed out~~.

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 ST author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection has to be made, [selection:], and are *italicised*.

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 ST author are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment has to be made [assignment:], and are *italicised*.

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.

6.1 Security Functional Requirements for the TOE

6.1.1 Overview

In order to give an overview of the security functional requirements in the context of the security services offered by the TOE, the author of the ST defined the security functional groups and allocated the functional requirements described in the following sections to them:

Security Functional Groups[8]	Security Functional Requirements concerned
Access control to User Data stored in the TOE	– {FDP_ACC.1/TRM, FDP_ACF.1/TRM} Supported by: – FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE) – FDP_RIP.1: enforced memory/storage cleaning
Secure data exchange between the ePass and the service provider (inspecting authority) connected	– FTP_ITC.1/PACE: trusted channel – FDP_UIT.1/TRM: data exchange integrity – FDP_UCT.1/TRM: data exchange

Security Functional Groups[8]	Security Functional Requirements concerned
	confidentiality Supported by: – FCS_COP.1/PACE_ENC: encryption/decryption – FCS_COP.1/PACE_MAC: MAC generation/verification – FCS_COP.1/CA_ENC: encryption/decryption (EIS) – FCS_COP.1/CA_MAC: MAC generation/verification (EIS) – FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE) – FCS_CKM.1/CA: Chip Authentication – FIA_API.1 – FIA_UAU.5/PACE – FIA_UAU.6/EAC: Chip Authentication
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Authentication (PACE authenticated BIS-PACE) – FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE) – FIA_API.1: Chip Authentication – FIA_UAU.4/PACE: single-use of authentication data – FIA_UAU.5/PACE: multiple authentication mechanisms – FIA_UAU.6/PACE, FIA_UAU.6/EAC: Re-authentication of Terminal – FCS_COP.1/SIG_VER: digital signature verification for Terminal Authentication – FIA_AFL.1/PACE: reaction to unsuccessful authentication attempts for establishing PACE communication using *non-blocking* authentication and authorisation data Supported by: – FCS_CKM.1/DH_PACE: PACE Authentication (PACE authenticated BIS-PACE)) – FCS_CKM.1/CA: Chip Authentication – FCS_CKM.4: session keys destruction (authentication expiration)

Security Functional Groups[8]	Security Functional Requirements concerned
	– FCS_RND.1: random numbers generation – FMT_MTD.3: only valid certificates chain – FMT_SMR.1/PACE: security roles definition.
Audit	– FAU_SAS.1 : Audit storage Supported by: – FMT_MTD.1/INI_ENA: Writing Initialisation and Pre-personalisation – FMT_MTD.1/INI_DIS: Disabling access to Initialisation and Pre-personalisation 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
Accuracy of the TOE security functionality / Self-protection	– The entire class FPT Supported by: – the entire class FMT.

Table 6: Security functional groups vs. SFRs

Definition of security attributes[7]: **security attribute**	**values**	**meaning**
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [15]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [15]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1

	DV (foreign)	roles defined in the certificate used for authentication (cf. [15]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [15]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [15])
	DG3 (Fingerprint)	Read access to DG3: (cf. [15])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [15])

Table 7: Definition of security attributes

The following table provides an overview of the keys and certificates used for enforcing the security policy defined in the current ST[7],[8]:

Name	Data
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. [15] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.

Name	Data
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) an 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 (terminal) Certificate (C_{IS})	The Inspection System (Terminal) Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System (Terminal) Public Key (PK_{IS}) as authentication reference data, (ii) the coded access control rights of the terminal (EIS-AIP-PACE), the Certificate Effective Date and the Certificate Expiration Date as security attributes.
	Please note that the receiving PKI branch is not used by the TOE while applying Standard Inspection Procedure.
Issuing PKI branch	
Chip Authentication Public Key Pair	The static Chip Authentication Key Pair {SK_{ICC}, PK_{ICC}} is used for Key Agreement Protocol: Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to ISO 11770-3 [25].
Chip Authentication Public Key (PK_{ICC})	PK_{ICC} is stored in EF.DG14 on the TOE and used by the inspection system (terminal) for the Chip Authentication Version 1. It is part of the data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	SK_{ICC} is used by the TOE to authenticate itself as an authentic e-Document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the ePass Issuer 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 receiving terminal (e.g. an EIS) 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. [10].
Document Signer Key Pairs and Certificates	Document Signer of the issuing State or Organisation acting under the policy of the CSCA signs the Document Security Object (SO_D) of the logical e-Document with the Document Signer Private Key (SK_{DS}) and the signature will be verified as the Passive Authentication by an Extended Inspection System (EIS) of the receiving State or Organisation with the Document Signer Public Key (PK_{DS}). 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.

Name	Data
Session keys	
PACE Session Keys (PACE-K_{MAC}, PACE-K_{ENC})	Secure messaging keys for message authentication and for message encryption agreed between the TOE and a terminal (PCT) as result of the PACE Protocol, see [16].
Chip Authentication Session Keys (CA-K_{MAC}, CA-K_{ENC})	Secure messaging keys for message authentication and for message encryption agreed between the TOE and a terminal (EIS-AIP-PACE) as result of the Chip Authentication Protocol Version 1, see [16].
Ephemeral keys	
PACE authentication ephemeral key pair (ephem-SK_{ICC}-PACE, ephem-PK_{ICC}-PACE)	The ephemeral PACE Authentication Key Pair {ephem-SK_{ICC}-PACE, ephem-PK_{ICC}-PACE} is used for Key Agreement Protocol: Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 [17].

Table 8: Keys and Certificates

6.1.2 Class FCS Cryptographic Support

FCS_CKM.1/DH_PACE[8] **Cryptographic key generation – Diffie-Hellman for PACE session keys**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: not fulfilled, but justified: A Diffie-Hellman 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 to [17][47] and specified cryptographic key sizes 112 bits[48] that meet the following: [12][49].

Explanatory note 42: The TOE generates a shared secret value *K* with the terminal during the PACE protocol, see [12]. This protocol may be based on the ECDH compliant to TR-03111 [17] (i.e. the elliptic curve cryptographic

47 [assignment: *cryptographic key generation algorithm*]

48 3DES only

49 [assignment: *list of standards*]

algorithm ECKA, cf. [15] and [17] for details). The shared secret value *K* is used for deriving the DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{ENC}) according to [15] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Explanatory note 43: FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [12].

FCS_CKM.1/CA[7] **Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys**

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: not fulfilled, but justified: A Diffie-Hellman 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 to [17][50] and specified cryptographic key sizes 112 bits[51] that meet the following: [17][52].

Explanatory note 44: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [12].

Explanatory note 45: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [17]. This protocol may be based on the ECDH compliant to TR-03111 [17] (i.e. an elliptic curve cryptography algorithm, cf. [15] and [17] for details). The shared secret value is used to derive the Chip Authentication session keys (CA-K_{MAC}, CA-K_{ENC}) for message encryption and message authentication for secure messaging (defined in Key Derivation Function [17]).

FCS_CKM.4[8] **Cryptographic key destruction – Session keys**

Hierarchical to:	No other components.

50 [assignment: *cryptographic key generation algorithm*]

51 3DES only

52 [assignment: *list of standards*]

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion of key value[53] that meets the following: FIPS 140-2 [21] [54].

Explanatory note 46: The TOE shall destroy the PACE and Chip Authentication session keys after detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol Version 1.
(iii) The TOE shall destroy the PACE session keys after generation of Chip Authentication session keys and changing the secure messaging to the Chip Authentication session keys.
(iv) The TOE shall clear 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. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

FCS_COP.1/PACE_ENC[8] Cryptographic operation – Encryption / Decryption 3DES

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.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1	The TSF shall perform secure messaging – encryption and decryption [55] in accordance with a specified cryptographic algorithm 3DES in CBC mode [56] and cryptographic key sizes 112 bit [57] that meet the following: [12][58].

Explanatory note 47: This SFR requires the TOE to implement the cryptographic primitive 3DES for secure messaging with encryption of transmitted data and

53 [assignment: *cryptographic key destruction method*]

54 [assignment: *list of standards*]

55 [assignment: *list of cryptographic operations*]

56 [assignment: *cryptographic algorithm*]

57 [assignment: *cryptographic key sizes*]

58 [assignment: *list of standards*]

encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{ENC}).

Explanatory note 48: Additionally, the TOE supports AES-CBC-128 (key sizes 128 bit) encryption/decryption cryptographic algorithms defined in [16] for the secure messaging during the TOE pre- and personalization.

FCS_COP.1/PACE_MAC[8] 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 FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1	The TSF shall perform secure messaging – message authentication code [59] in accordance with a specified cryptographic algorithm Retail-MAC[60] and cryptographic key sizes 112 bit[61] that meet the following: [12][62].

Explanatory note 49: The TOE supports the following cryptographic algorithms for the secure messaging:
- 3DES-CBC-CBC (key sizes 112 bit) – at the operational phase,
- AES-CBC-CMAC-128 (key sizes 128 bit) – during the TOE personalization procedure only,

defined in [16].

Explanatory note 50: 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 the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}). Note that in accordance with [12] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

FCS_COP.1/SIG_VER[7] Cryptographic operation – Signature verification

59 [assignment: *list of cryptographic operations*]

60 [assignment: *cryptographic algorithm*]

61 [assignment: *cryptographic key sizes*]

62 [assignment: *list of standards*]

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 personalisation (in the card issuing life cycle phase)[63]. Since importing the respective certificates (C_{IS}, C_{DV}) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3 below), the current ST does not contain any dedicated requirement like FDP_ITC.2 for the import function. FCS_CKM.4 Cryptographic key destruction: not fulfilled, but **justified** Cryptographic keys used for the purpose of the current SFR (PK_{IS}, PK_{DV}, PK_{CVCA}) are public keys; they do not represent any secret and, hence, needn't to be destroyed.
FCS_COP.1.1	The TSF shall perform digital signature verification [64] in accordance with a specified cryptographic algorithm ECDSA with SHA-256[65] and cryptographic key sizes 256 bits (BP, NIST)[66] that meet the following: [17] [67].

Explanatory note 51: This SFR concerns the implementation of the TOE part of the Terminal Authentication Protocol Version 1. 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 [17]. The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge. The related static public keys (PK_{IS}, PK_{DV}) are imported within the respective certificates (C_{IS}, C_{DV}) during the TA and are extracted by the TOE using PK_{CVCA} as the root key stored in the TOE during its personalisation (see A.Auth_PKI).

Explanatory note 52: Signature verification algorithm based on ECDSA for domain BrainpoolP256r1 that is recommended by BSI (see [16] for details).

FCS_COP.1/CA_ENC[7] **Cryptographic operation – Symmetric Encryption / Decryption**

Hierarchical to: No other components.

63 As already mentioned, operational use of the TOE is explicitly in focus of the current ST

64 [assignment: *list of cryptographic operations*]

65 [assignment: *cryptographic algorithm*]

66 [assignment: *cryptographic key sizes*]

67 [assignment: *list of standards*]

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/CA FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1	The TSF shall perform secure messaging – encryption and decryption [68] in accordance with a specified cryptographic algorithm 3DES in CBC mode [69] and cryptographic key sizes 112 bit [70] that meet the following: [12][71].

Explanatory note 53: This SFR requires the TOE to implement the cryptographic primitive Triple-DES for secure messaging with encryption of transmitted data. The related session keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA (CA-K_{Enc}).

FCS_COP.1/CA_MAC[7] 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 FCS_CKM.1/CA FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1	The TSF shall perform secure messaging – message authentication code [72] in accordance with a specified cryptographic algorithm, Retail-MAC[73] and cryptographic key sizes 112 bit[74] that meet the following: [12][75].

Explanatory note 54: The TOE supports following cryptographic algorithm for the secure messaging:
- 3DES-CBC-CBC (key sizes 112 bit),

that is defined in [16].

68 [assignment: *list of cryptographic operations*]

69 [assignment: *cryptographic algorithm*]

70 [assignment: *cryptographic key sizes*]

71 [assignment: *list of standards*]

72 [assignment: *list of cryptographic operations*]

73 [assignment: *cryptographic algorithm*]

74 [assignment: *cryptographic key sizes*]

75 [assignment: *list of standards*]

Explanatory note 55: 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 the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA (CA-K_{MAC}). Note that in accordance with [12] the (two-key) Triple-DES could be used in Retail mode for secure messaging. Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the authentication mechanism.

FCS_RND.1[8] **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 i) Test procedure A, as defined in [22] does not distinguish the internal random numbers from output sequences of an ideal RNG, ii) The average Shannon entropy per internal random bit exceeds 0.997[76].

Explanatory note 56: This SFR requires the TOE to generate random numbers used for authentication protocols, e.g. as required by FIA_UAU.4/PACE (random nonce for PACE).

6.1.3 Class FIA Identification and Authentication

For the sake of better readability, Table 9 provides an overview of the authentication mechanisms used:

Name[7], [8]	SFR for the TOE
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_UAU.6/PACE FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/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.1/PACE FIA_UAU.5/PACE
Authentication Mechanism	FIA_UAU.5/PACE

76 [assignment: *a defined quality metric*]

Name[7], [8]	SFR for the TOE
for Personalisation Agents	

Table 9: Overview of authentication SFRs

FIA_AFL.1/PACE[8] **Authentication failure handling – PACE authentication using non-blocking authorisation data**

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1	The TSF shall detect when **at most** 15[77] unsuccessful authentication attempts occur related to authentication attempts using the PACE password as shared password[78].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met[79], the TSF shall consecutively increase the reaction time of the TOE to the next authentication attempt using PACE password.

FIA_UID.1/PACE[7] **Timing of identification**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow 1. establishing a communication channel, 2. carrying out the PACE Protocol according to [12] , 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[80], 4. to carry out the Chip Authentication Protocol Version 1 according to [15][81], 5. to carry out the Terminal Authentication Protocol Version 1 according to [15][82] on behalf of the user to be performed before the user is identified.

77 [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

78 [assignment: *list of authentication events*]

79 [selection: *met ,surpassed*]

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

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

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

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

Explanatory note 57: In the life cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC.
Please note that a Personalisation Agent acts on behalf of the ePass Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

FIA_UAU.1/PACE[7] 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 The TSF shall allow

1. establishing a communication channel,
2. carrying out the PACE Protocol according to [12] [83],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[84],
4. to identify themselves by selection of the authentication key[85],
5. to carry out the Chip Authentication Protocol Version 1 according to [15],
6. to carry out the Terminal Authentication Protocol Version 1 according to [15][86]

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

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

Explanatory note 58: The user authenticated after a successfully performed PACE protocol is a PACE terminal (PCT). Please note that PACE passwords do not effectively represent, but are restricted-revealable; i.e. it is either the ePass holder itself or an authorised other person or device (BIS-PACE).

---

83 e-Document identifies itself within the PACE protocol by selection of the authentication key ephem-PK_{ICC}-PACE

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

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

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

If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{ENC}), cf. FTP_ITC.1/PACE.

FIA_UAU.4/PACE[7] Single-use authentication of the Terminals by the TOE

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. PACE Protocol according to [12], 2. Authentication Mechanism based on Triple-DES[87], 3. Terminal Authentication Protocol v.1 according to [15][88].

Explanatory note 59: The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

FIA_UAU.5/PACE[7] Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide 1. PACE Protocol according to [12], 2. Passive Authentication according to [10], 3. Secure messaging in MAC-ENC mode according to [12] , 4. Symmetric Authentication Mechanism based on Triple-DES[89], 5. Terminal Authentication Protocol v.1 according to [15][90] to support user authentication.

87 [selection: *Triple-DES, AES or other approved algorithms*]

88 [assignment: *identified authentication mechanism(*s)]

89 [selection: *Triple-DES, AES or other approved algorithms*]

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

FIA_UAU.5.2 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 Personalisation Agent by the Authentication Mechanism with Personalisation Agent Key,
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 v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1[91]

Explanatory note 60: Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of *ePassport* application.

FIA_UAU.6/PACE[8] Re-authenticating of Terminal by the TOE

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.[92]

Explanatory note 61: The PACE protocol specified in [12] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_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.

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

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

FIA_UAU.6/EAC[7]	**Re-authenticating of Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication protocol Version 1 shall be verified as being sent by the Inspection System.[93]

Explanatory note 62: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [10] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm 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 user for each received command and accepts only those commands received from the previously authenticated user.

FIA_API.1[7]	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a Chip Authentication Protocol Version 1 according to [15] [94] to prove the identity of the TOE [95]

Explanatory note 63: This SFR requires the TOE to implement the Chip Authentication Mechanism Version 1 specified in [15]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [10]. The terminal verifies by means of secure messaging whether the e-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).

6.1.4 Class FDP User Data Protection

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

94 [assignment: *authentication mechanism*]

95 [assignment: *authorised user or role*]

FDP_ACC.1/TRM[7] Subset access control – Terminal Access

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACF.1/TRM
FDP_ACC.1.1	The TSF shall enforce the Access Control SFP [96] on terminals gaining access to the User Data and data stored in EF.SOD of the logical ~~travel document~~ **e-Document**[97].

FDP_ACF.1/TRM[7] Security attribute based access control – Terminal Access

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM FMT_MSA.3 Static attribute initialisation: not fulfilled, but **justified** The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalisation 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	The TSF shall enforce the Access Control SFP[98] to objects based on the following: 1. Subjects: a. Terminal, b. BIS-PACE c. Extended Inspection System[99] 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~~ **e-Document**, b. data in EF.DG3 of the logical ~~travel document~~ **e-Document**, c. data in EF.DG4 of the logical ~~travel document~~ **e-Document**, d. all TOE intrinsic secret cryptographic keys stored in the ~~travel document~~ **e-Document**[100]; 3. Security attributes: a. PACE authentication b. Terminal Authentication v.1 c. Authorisation of the Terminal[101].

96 [assignment: *access control SFP*]

97 [assignment: *list of subjects*, *objects, and operations among subjects and objects covered by the SFP*]

98 [assignment: *access control SFP*]

99 EIS-AIP-PACE Terminal (see *Explanatory note 9* for details)

100 E.g. Chip Authentication Version 1 and ephemeral keys

FDP_ACF.1.2 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 of FDP_ACF.1/TRM **(except DG3[102] and DG4[103])** according to [12], after a successful PACE authentication as required by FIA_UAU.1/PACE.[104]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[105].

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

1. Any terminal being not authenticated as PACE authenticated as BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the ~~travel document~~ **e-Document**.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the ~~travel document~~ **e-Document**.
3. Any terminal being not successfully authenticated as Extended Inspection System[106] 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[107] 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 object 2d) of FDP_ACF.1.1.
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4[108].

Explanatory note 64: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [15]. 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

---

101 [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*]

102 Biometric: finger

103 Biometric: iris

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

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

106 EIS-AIP-PACE Terminal (see *Explanatory note 9* for details)

107 EIS-AIP-PACE Terminal (see *Explanatory note 9* for details)

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

Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

Explanatory note 65: Please note that the Document Security Object (SO_D) stored in EF.SOD does not belong to the user data, but to the TSF-data. The Document Security Object can be read out by the PCT, see [10].

Explanatory note 66: Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE. 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 Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol Version 1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

FDP_RIP.1[8] 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 deallocation of the resource from[109] the following objects:

1. Session Keys (immediately after closing related communication session),
2. the ephemeral private key ephem-SK_{ICC}-PACE (by having generated a DH shared secret K[110])[111].

Explanatory note 67: The functional family FDP_RIP possesses such a general character, so that it 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 in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

FDP_UCT.1/TRM[8] Basic data exchange confidentiality – e-Document

[109] [selection: *allocation of the resources to, deallocation of the resource from*]

[110] according to [12]

[111] [assignment: *list of objects*]

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	The TSF shall enforce the Access Control SFP[112] to be able to transmit and receive[113] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/TRM[8] 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	The TSF shall enforce the Access Control SFP[114] to be able to transmit and receive[115] user data in a manner protected from modification, deletion, insertion and replay[116] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[117] has occurred.

6.1.5 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE[8] Inter-TSF trusted channel after PACE

[112] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[113] [selection: *transmit, receive*]

[114] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[115] [selection: *transmit, receive*]

[116] [selection: *modification, deletion, insertion, replay*]

[117] [selection: *modification, deletion, insertion, replay*]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	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	The TSF shall permit another trusted IT product[118] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal[119].

Explanatory note 68: 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 Passive Authentication and the required properties of *operational* trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.
The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

Explanatory note 69: Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

6.1.6 Class FAU Security Audit

FAU_SAS.1[8] **Audit storage**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer[120] with the capability to store the Initialisation and Pre-Personalisation Data [121] in the audit records.

Explanatory note 70: The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the e-

[118] [*selection: the TSF, another trusted IT product*]

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

[120] [assignment: *authorised users*]

[121] [assignment: *list of audit information*]

Document manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE. The audit records are usually write-only-once data of the ePass (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.

6.1.7 Class FMT Security Management

The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements on the management of the TSF data.

FMT_SMF.1[8] 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. Initialisation, 2. Pre-Personalisation, 2. Personalisation, 3. Configuration.[122]

FMT_SMR.1/PACE[7] Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE see also the *Explanatory note 71* below.
FMT_SMR.1.1	The TSF shall maintain the roles 1. Manufacturer, 2. Personalisation Agent, 3. Terminal, 4. PACE authenticated BIS-PACE, 5. Country Verifying Certification Authority, 6. Document Verifier, 7. Domestic Extended Inspection System **(domestic EIS-AIP-PACE)** 8. Foreign Extended Inspection System **(foreign EIS-AIP-PACE)** [123].

[122] [assignment: *list of management functions to be provided by the TSF*]

[123] [assignment: *the authorised identified roles*]

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

Explanatory note 71: For explanation on the role Manufacturer please refer to the *Explanatory note 70*; on the role Personalisation Agent – to the *Explanatory note 57*. The role Terminal is the default role for any terminal being recognised by the TOE as not PCT ('Terminal' is used by the ePass presenter).
The TOE recognises an authorised person or device (BIS-PACE or EIS-AIP-PACE) by using FIA_UAU.1/PACE.
The roles CVCA and DV exist within the receiving branch by analysing the current Inspection System Certificate C_{IS}.

The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

FMT_LIM.1[7] 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,
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.[124]

FMT_LIM.2[7] Limited availability

Hierarchical to: No other components.

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

[124] [assignment: *Limited capability and availability policy*]

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced:

Deploying Test Features after TOE delivery 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.[125]

Explanatory note 72: Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software

FMT_MTD.1/CVCA_INI[7] Management of TSF data – Initialisation 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/PACE

FMT_MTD.1.1 The TSF shall restrict the ability to write [126] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date

to the Personalisation Agent[127].

Explanatory note 73: The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalisation phase or by the Personalisation Agent (cf. [15]). 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 initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

FMT_MTD.1/CVCA_UPD[7] Management of TSF data – Country Verifying Certification Authority

125 [assignment: *Limited capability and availability policy*]

126 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

127 [assignment: *the authorised identified roles*]

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	The TSF shall restrict the ability to update [128] the 1. Country Verifying Certification Authority Public Key, 2. Country Verifying Certification Authority Certificate, to Country Verifying Certification Authority. [129]

Explanatory note 74: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [15]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [15]).

FMT_MTD.1/DATE[7] 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/PACE
FMT_MTD.1.1	The TSF shall restrict the ability to modify [130] the Current Date[131] to 1. Country Verifying Certification Authority, 2. Document Verifier, 3. Domestic Extended Inspection System **(domestic EIS-AIP-PACE)**[132].

Explanatory note 75: The authorized roles are identified in their certificate (cf. [15]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication Version 1 (cf. to [15]).

128 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

129 [assignment: *the authorised identified roles*]

130 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

131 [assignment: *list of TSF data*]

132 [assignment: *the authorised identified roles*]

FMT_MTD.1/CAPK[7] Management of TSF data – Chip Authentication Private Key

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	The TSF shall restrict the ability to load [133] the Chip Authentication Private Key[134] to the Personalisation Agent[135].

FMT_MTD.1/KEY_READ[7] 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: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1	The TSF shall restrict the ability to read [136] the 1. PACE passwords **(stored in the TOE),** 2. Chip Authentication Private Key, 3. Personalisation Agent Key [137] to none. [138]

FMT_MTD.1/INI_ENA[8] Management of TSF data – Writing Initialisation and Pre-personalisation 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/PACE
FMT_MTD.1.1	The TSF shall restrict the ability to write [139] the Initialisation Data and Pre-personalisation Data[140] to the Manufacturer. [141]

133 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

134 [assignment: *list of TSF data*]

135 [assignment: *the authorised identified roles*]

136 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

137 [assignment: *list of TSF data*]

138 [assignment: *the authorised identified roles*]

FMT_MTD.1/INI_DIS[8] Management of TSF data – Reading and Using Initialisation and Pre-personalisation 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/PACE
FMT_MTD.1.1	The TSF shall restrict the ability to read out[142] the Initialisation Data and the Pre-Personalisation Data [143] to the Personalisation Agent. [144]

Explanatory note 76: The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation 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 Initialisation 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 cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read access to the Initialisation Data and Pre-Personalisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'. Please also refer to the *Explanatory note 57*.

FMT_MTD.1/PA[8] Management of TSF data – Personalisation Agent

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	The TSF shall restrict the ability to write [145] the Document Security Object ($EF.SO_D$)**, EF.DG1 to EF.DG16 and EF.COM** [146] to the Personalisation Agent. [147]

[139] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[140] [assignment: *list of TSF data*]

[141] [assignment: *the authorised identified roles*]

[142] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[143] [assignment: *list of TSF data*]

[144] [assignment: *the authorised identified roles*]

[145] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[146] [assignment: *list of TSF data*]

Explanatory note 77: By writing SO_D into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF-data. On the role 'Personalisation Agent' please refer to the Explanatory note 57.
Additionally to the related SFR from [7], current SFR additionally restricted the ability for writing EF.SOD, EF.DG1 to EF.DG16 and EF.COM to the Personalisation Agent. This strengths the TSP described by the current ST and, hence, does not contradict strict conformance to [7].

FMT_MTD.3[7] 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.[148]

Refinement: The certificate chain is valid if and only if

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

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

(3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.

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

The intersection of the Certificate Holder Authorisations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorisation Level of a successfully authenticated Extended Inspection System.

147 [assignment: *the authorised identified roles*]

148 [assignment: list of TSF data]

Explanatory note 78: The Terminal Authentication v.1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

6.1.8 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for the 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 design measures to be described within the SAR 'Security architecture description' (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of the TOE security functionality.

FPT_EMS.1[7] TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit information about IC power consumption and command execution time[149] in excess of non-useful information[150] enabling access to 1. Chip Authentication Session Keys 2. PACE Session Keys (PACE-K_{MAC}, PACE-K_{Enc}), 3. the ephemeral private key ephem-SK_{ICC}-PACE, 4. current date, file system service data, Public Key of CV certificate, 5. Personalisation Agent Key(s), 6. Chip Authentication Private Key[151] and 7. no user data[152].
FPT_EMS.1.2	The TSF shall ensure any users [153] are unable to use the following interface ~~smart card~~ **e-Document's** circuit contacts **and contactless interface** [154] 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_{ICC}-PACE,

[149] [*assignment: types of emissions*]

[150] [assignment: *specified limits*]

[151] [assignment: *list of types of TSF data*]

[152] [assignment: *list of types of user data*]

[153] [assignment: *type of users*]

[154] [assignment: *type of connection*]

4. current date, file system service data, Public Key of CV certificate,
5. Personalisation Agent Key(s) and
6. Chip Authentication Private Key[155] and
7. no user data[156].

Explanatory note 79: 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 e-Document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). 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.

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

FPT_FLS.1[8] Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions causing a TOE malfunction, 2. Failure detected by TSF according to FPT_TST.1[157],

FPT_TST.1[8] 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, at the conditions 'reset of the TOE' [158] to demonstrate the correct operation of the TSF[159].

[155] [assignment: *list of types of TSF data*]

[156] [assignment: *list of types of user data*]

[157] [assignment: *list of types of failures in the TSF*]

FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[160].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[161].

FPT_PHP.3[8] 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 [162] to the TSF [163] by responding automatically such that the SFRs are always enforced.

Explanatory note 80: The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

6.2 Security Assurance Requirements for the TOE

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).

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

159 [selection: *[assignment: parts of TSF], the TSF*]

160 [selection: *[assignment: parts of TSF], TSF data*]

161 [selection: *[assignment: parts of TSF], TSF*]

162 [assignment: *physical tampering scenarios*]

163 [assignment: *list of TSF devices/elements*]

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proff	OT.Identification	OT.AC_Pers	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
FCS_CKM.1/DH_PACE					x	x	x					
FCS_CKM.1/CA	x	x		x	x	x	x					
FCS_CKM.4	x			x	x	x	x					
FCS_COP.1/PACE_ENC							x					
FCS_COP.1/PACE_MAC					x	x						
FCS_COP.1/SIG_VER	x			x								
FCS_COP.1/CA_ENC	x	x		x	x		x					
FCS_COP.1/CA_MAC	x	x		x	x							
FCS_RND.1	x			x	x	x	x					
FIA_AFL.1/PACE								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					
FIA_API.1		x										
FDP_ACC.1/TRM	x			x	x		x					
FDP_ACF.1/TRM	x			x	x		x					
FDP_RIP.1					x	x	x					

	OT.Sens_Data_Conf	OT.Chip_Auth_Proff	OT.Identification	OT.AC_Pers	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
FDP_UCT.1/TRM	x				x		x					
FDP_UIT.1/TRM					x		x					
FTP_ITC.1/PACE					x	x	x	x				
FAU_SAS.1			x	x								
FMT_SMF.1		x	x	x	x	x	x					
FMT_SMR.1/PACE		x	x	x	x	x	x					
FMT_LIM.1									x			
FMT_LIM.2									x			
FMT_MTD.1/CVCA_INI	x											
FMT_MTD.1/CVCA_UPD	x											
FMT_MTD.1/DATE	x											
FMT_MTD.1/CAPK	x	x			x							
FMT_MTD.1/KEY_READ	x	x		x	x	x	x					
FMT_MTD.1/INI_ENA			x	x								
FMT_MTD.1/INI_DIS			x	x								
FMT_MTD.1/PA				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 10: Coverage of Security Objectives for the TOE by SFR

A detailed justification required for *suitability* of the security functional requirements to achieve the security objectives is given below.

Since all the SFRs and TOE security objectives in the current ST completely and accurately repeat all the related items defined in ICAO-EAC PP [7], the related rational given and certified in [7] is also valid for the current ST.

6.3.2 Rationale for SFR's Dependencies

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained.

The dependency analysis has directly been made within the description of each SFR in sec. 6.1 above. All dependencies being expected by CC part 2 and by extended components definition in chap. 5 are either fulfilled or their non-fulfilment is justified.

6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the pre-defined assurance package EAL4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

The assurance package chosen in the current ST fully comprises the assurance package required in ICAO-EAC PP [7] (EAL4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5).

Since all the SARs in the current ST completely and accurately repeat all the related items defined in ICAO-EAC PP [7], the related rational given and certified in [7] is also valid for the current ST.

6.3.4 Security Requirements – Internal Consistency

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

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

The dependency analysis in section 6.3.2 'Rationale for SFR's Dependencies' for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed 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 behaviour of these 'shared' items.

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 'Security Assurance Requirements Rationale' shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met: an opportunity shown not to arise in sections 6.3.2 'Rationale for SFR's Dependencies' and 6.3.3 'Security Assurance Requirements Rationale'. Furthermore, as also discussed in section 6.3.3 'Security Assurance Requirements

Rationale', the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specification

This chapter gives an overview description of the TOE Security Services composing the TSF of the current TOE.

7.1 TSS_Access_Control

The TOE provides access control mechanisms for restricting access to a set of objects stored in the TOE dependent (i) on the subject (role) known within the TOE requesting this access and (ii) on the type of the access requested.

In the TOE *operational phase*, only terminals recognised by the TOE as Inspection Systems (Basic or Extended) are allowed to get reading access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM.

In order to get reading access to EF.DG3 (fingerprint) and EF.DG4 (iris), the terminal recognised by the TOE must be Extended Inspection System.

Any other kind of access of an Inspection Systems to the data stored in the TOE is not allowed. TOE intrinsic secret cryptographic keys stored in the TOE cannot be accessed by any kind of terminal (FDP_ACC.1/TRM, FDP_ACF.1/TRM; FMT_MTD.1/KEY_READ).

The access control mechanism of the TOE enforces that only the Country Verifying Certification Authority can update the CVCA Public Key and the CVCA Certificate (FMT_MTD.1/CVCA_UPD). Additionally, Country Verifying Certification Authority, Document Verifier and Domestic Extended Inspection System are granted to modify the current date stored in the TOE (FMT_MTD.1/DATE).

The TOE access control mechanisms restricts the following actions exclusively to the Personalisation Agent:

- to write the initial CVCA Public Key, the initial CVCA Certificate, and the initial Current Date (FMT_MTD.1/CVCA_INI),
- to load the Chip Authentication Private Key (FMT_MTD.1/CAPK),
- to read out the Initialisation Data and the Pre-Personalisation Data (FMT_MTD.1/INI_DIS). Read access for other users to these data is disabled.
- to write the Document Security Object (EF.SOD) as well as the personalisation data (EF.DG1 to EF.DG16, EF.COM) (FMT_MTD.1/PA).

The TOE access control mechanisms restricts the following actions exclusively to the TOE Manufacturer:

- to write the Initialisation Data and Pre-personalisation Data (FMT_MTD.1/INI_ENA, FAU_SAS.1).

Users of role Manufacturer are assumed default users by the TOE during the manufacturing phase.

The TOE provides the necessary management functions (FMT_SMF.1): Initialisation, Pre-Personalisation, Personalisation and Configuration as well as maintains security relevant roles (FMT_SMR.1/PACE).

In order to prevent access to temporarily stored secrets the TOE destroys the PACE and Chip Authentication 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 Version 1. (iii) The TOE destroys the PACE session keys after generation of Chip Authentication session keys and changing the

secure messaging to the Chip Authentication session keys. (iv) The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session (FCS_CKM.4).

The TOE makes the related information content unavailable upon the deallocation of these resources; it is also valid for the ephemeral private key ephem-SK_{ICC}-PACE (FDP_RIP.1).

7.2 TSS_Trusted_Channel

This TOE security service enforces establishment and operation of the following secure channels:

1) Basic Inspection Procedure

   As a result of a successful PACE authentication (see TSS_Authentication), the TOE and the Basic Inspection System (BIS-PACE) establish a trusted channel maintaining confidentiality and integrity of all the data exchanged between them (FTP_ITC.1/PACE, FDP_UIT.1/TRM, FDP_UCT.1/TRM). The cryptographic properties of this trusted channel are defined in FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC. The related session key generation is modelled by FCS_CKM.1/DH_PACE.

2) Advanced Inspection Procedure

   As a result of a successful Chip Authentication Version 1 (see TSS_Authentication), the TOE and the Inspection System (a concrete type of the Inspection System is known to the TOE first after a successful Terminal Authentication Version 1) finishes the PACE trusted channel and immediately establish a new trusted channel maintaining confidentiality and integrity of all the data exchanged between them (FTP_ITC.1/PACE, FDP_UIT.1/TRM, FDP_UCT.1/TRM). The cryptographic properties of this new trusted channel are defined in FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC. The related session key generation is modelled by FCS_CKM.1/CA.

7.3 TSS_Authentication

This TOE security service enforces the following authentication procedures, whereby the possible pre-defined security roles (as results of authentication) are listed in FMT_SMR.1/PACE:

1) Authentication Mechanism for Personalisation Agents

   The Personalisation Agent authenticates himself to the TOE by using a symmetric challenge-response mechanism. This mechanism uses Personalisation Agent Key shared between the TOE and the Personalisation Agent (FIA_UAU.5/PACE).

2) PACE protocol

   After a terminal to which the TOE is connected has determined TOE's ability to establish a PACE session, the terminal requests for the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE). As a result of a successful PACE authentication, the TOE and the Basic Inspection System (BIS-PACE) establish a PACE trusted channel (see TSS_Trusted_Channel). The related cryptographic primitives is modelled by FCS_CKM.1/DH_PACE.

   The authentication mechanism uses a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt (FIA_UAU.4/PACE, FCS_RND.1).

The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_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 (FIA_UAU.6/EAC, FCS_COP.1/PACE_MAC).

When PACE authentication and PACE session become invalid, the related session keys are physically erased (FCS_CKM.4).

The establishing phase of the PACE trusted channel is implemented in such a way that tracing of the e-document while using PACE is not possible (FIA_AFL.1/PACE).

3) Chip Authentication Protocol version 1 (for Advanced Inspection Procedure)

After the terminal (PCT) operating a valid PACE session with the TOE has determined TOE's ability to perform a Chip Authentication Version 1, the terminal requests for the Chip Authentication Version 1 (FIA_API.1, FIA_UAU.5/PACE). As a result of a successful Chip Authentication Version 1, the TOE and the Inspection System establish a new trusted channel (see TSS_Trusted_Channel). The related cryptographic primitives is modelled by FCS_CKM.1/CA.

The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm 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 user for each received command and accepts only those commands received from the previously authenticated user (FIA_UAU.6/EAC, FCS_COP.1/CA_MAC).

When Chip Authentication and the related session become invalid, the related session keys are physically erased (FCS_CKM.4).

The authentication mechanism uses a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt (FIA_UAU.4/PACE, FCS_RND.1).

4) Passive Authentication

The terminal operating either a PACE session (for Basic Inspection Procedure) or a Chip Authentication session reads out (and the TOE explicitly permits this) the content of the file EF.SOD (FIA_UAU.5/PACE).

5) Terminal Authentication Protocol version 1 (for Advanced Inspection Procedure)

The terminal operating a Chip Authentication session with the TOE initiates performing Terminal Authentication protocol v.1 (FIA_UAU.1/PACE, FIA_UAU.5/PACE).

The authentication mechanism uses a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt (FIA_UAU.4/PACE, FCS_RND.1).

Only secure values of the certificate chain are accepted by the TOE for the Terminal Authentication Protocol (FMT_MTD.3). For the validation of the certificate chain the TOE uses the related cryptographic primitives as described in FCS_COP.1/SIG_VER.

The certificate chain is valid if and only if

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

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

(3) the digital signature of the Certificate of the Country Verifying Certification Authority (C_{CVCA}) 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 C_{CVCA} is not before the Current Date of the TOE.

The Inspection System public key (PK_{IS}) contained in the C_{IS} in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorisations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorisation Level of a successfully authenticated Extended Inspection System.

7.4 TSS_Self-Protection

The TOE enforces this TOE security service in order to protect its own genuineness (TSF and TSF-data) and to support the protection of user data stored in the TOE.

The TOE prevents misuse of specific test features of the TOE over the life cycle phases. Specific test features of the TOE used by the TOE manufacturer are not available for the users in the personalisation and operational phases. This supports preventing manipulation and re-engineering of the TOE software, manipulation and disclosure of TSF data as well as manipulation and disclosure of User Data incl. sensitive biometric data reference (EF.DG3 and EF.DG4), see FMT_LIM.1, FMT_LIM.2.

The TOE monitors the integrity of the TSF data and stored TSF executable code verifying the absence of fault injections. They are secured by a symmetric cryptographic check sum. In the case of test failures and fault injections during the operation of the TSF the TOE preserves a secure state (FPT_TST.1, FPT_FLS.1).

The TOE makes information about IC power consumption and command execution time leaked during TOE operation non useful for gaining the values of Chip Authentication Session Keys, PACE session Keys, the ephemeral private key ephem-SK_{ICC}-PACE, Personalisation Agent Key(s), Chip Authentication Private Key.

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. 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 (FPT_EMS.1).

The TOE implements the following measures to continuously counter physical manipulation and physical probing:

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency and temperature. If one of the above mentioned sensors reports that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analysing and physical tampering (FPT_PHP.3).

8 Glossary and Acronyms

Glossary

Term	Definition
Accurate Inspection System (Terminal) Certificate	An Inspection System (Terminal) Certificate is accurate, if the issuing Document Verifier is trusted by the ePass's chip to produce Inspection System Certificates with the correct certificate effective date, see [15].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between an ePass and a terminal as required by [15], namely (i) PACE, (ii) Chip Authentication Version 1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication Version 1. AIP can generally be used by EIS-AIP-PACE and EIS-AIP-BAC.
Agreement	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Audit records	Write-only-once non-volatile memory area of the e-Document's chip to store the Initialisation Data and Pre-personalisation Data.
Authenticity	Ability to confirm that the ePass itself and the data elements stored in were issued by the ePass Issuer
Basic Access Control (BAC)	Security mechanism defined in [10] by which means the e-Document's chip proves and the basic inspection system (with BAC) protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on e-Document's chip according to LDS.
Basic Inspection System with Basic Access Control protocol (BIS-BAC)	A technical system being used by an official organisation[164] and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying correspondence between the stored and printed MRZ. BIS-BAC implements the terminal's part of the Basic Access Control protocol and authenticates itself to the ePass using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (ePass document details data and biographical data) stored on the ePass. See also *Explanatory note 10*, [15]; also [10].
Basic Inspection System with PACE protocol (BIS-PACE)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ePass presenter as the ePass holder (for *ePassport*: by comparing the real biometrical data (face) of the ePass presenter with the stored biometrical data (DG2) of the ePass holder).

[164] an inspecting authority

Term	Definition
	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. Explanatory Note 18: The Basic Inspection System with PACE is a PACE authenticated terminal (PCT) additionally supporting/applying the Passive Authentication protocol and is authorised by the ePass Issuer through the Document Verifier of receiving state to read a subset of data stored on the ePass. BIS-PACE and PACE authenticated terminal (PCT) possess same Terminal Authorisation Level. BIS-PACE in the context of [15] (and of the current ST) is similar, but not equivalent to the Basic Inspection System (BIS) as defined in [6]. See also [15].
Biographical data (biodata)	The personalised details of the ePass holder appearing as text in the visual and machine readable zones of and electronically stored in the ePass. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the ePass holder in the ePass as (i) digital portrait and (ii) optional biometric reference data (e.g. finger and iris).
Card Access Number (CAN)	A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Passport), semi-static (e.g. printed on a label on the Passport) or dynamic (randomly chosen by the electronic ePass and displayed by it using e.g. ePaper, OLED or similar technologies), see [15].
Certificate chain	Hierarchical sequence of Inspection System (Terminal) Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means. [10]
Country Signing CertA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (PK_{CSCA}) issued by Country Signing Certification Authority and stored in the rightful terminals.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the ePass Issuer with respect to confirming correctness of user and TSF data stored in the ePass. The CSCA represents the country specific root of the PKI for the ePass 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. [10].

Term	Definition
	The Country Signing Certification Authority issuing certificates for Document Signers (cf. [10]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [15].
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the issuing State or Organisation with respect to the protection of sensitive biometric reference data stored in the e-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, see [15]. Explanatory Note 21: Please note that while using Standard Inspection Procedure, the TOE cannot recognise a CVCA as a subject, because the SIP does not imply any certificate-based terminal authentication; in this case CVCA merely represents an organisational entity within this ST. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [10]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [15].
Current date	The most recent certificate effective date contained in a valid CVCA Link Certificate, a DV Certificate or an Accurate Inspection System (Terminal) Certificate known to the TOE, see [15].
CV Certificate	Card Verifiable Certificate according to [15], appendix C.
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.
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient; see [24].
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KB_{ENC}) and message authentication (key KB_{MAC}) of data transmitted between the TOE and an inspection system using BAC [10]. They are derived from the MRZ and used within BAC to authenticate an entity able to read the printed MRZ of the passport book; see [15].
Document Details Data	Data printed on and electronically stored in the ePass 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 RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups: A hash for each Data Group in use shall be stored in the Security Data. It is stored in the

Term	Definition
	ePassport application (EF.SOD) of the ePass. It may carry the Document Signer Certificate (C_{DS}); see [10].
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the ePass for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [15] and [10]. This role is usually delegated to a Personalisation Agent.
Document Verifier (DV)	An organisation enforcing 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 Organisations in the form of the Document Verifier Certificates. Explanatory Note 20: An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Inspection System (Terminal) Certificates. A Document Verifier is therefore a CertA, authorised by at least the national CVCA to issue certificates for national terminals, see [15]. Please note that while using Standard Inspection Procedure, the TOE cannot recognise a DV as a subject, because the SIP does not imply any certificate-based terminal authentication; in this case DV merely represents an organisational entity within this ST. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the ePass 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 ePass Issuer und a foreign CVCA ensuring enforcing the ePass Issuer's privacy policy)..[165,166]
Eavesdropper	A threat agent reading the communication between the ePass and the Service Provider to gain the data on the ePass.
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; see [10].
ePass (electronic)	The contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.

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

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

Term	Definition
ePass holder	A person for whom the ePass Issuer has personalised the e- ePass.
ePass Issuer (issuing authority)	Organisation authorised to issue an electronic Passport to the ePass holder
ePass presenter	A person presenting the ePass to a terminal and claiming the identity of the ePass holder.
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 electronic document (e-Document). See [15].
Explanatory note	Optional informative part of a PP / ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
Extended Access Control	Security mechanism identified in [10] by which means the e-Document's chip (i) verifies the authentication of the inspection systems authorised 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 using AIP with BAC (EIS-AIP-BAC)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ePass presenter as the ePass holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the ePass presenter with the stored biometrical data (DG2 – DG4) of the ePass holder). EIS-AIP-BAC is a Basic Inspection System (BIS) in the sense of [6] additionally supporting/applying Chip Authentication (incl. passive authentication) and Terminal Authentication protocols in the context of AIP and is authorised by the ePass Issuer through the Document Verifier of receiving state to read a subset of data stored on the ePass. EIS-AIP-BAC in the context of [15] is equivalent to the Extended Inspection System (EIS) as defined in [7].
Extended Inspection System using AIP with PACE (EIS-AIP-PACE)	A technical system being used by an inspecting authority and operated by a governmental organisation[167] (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ePass presenter as the ePass holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the ePass presenter with the stored biometrical data (DG2 – DG4) of the ePass holder). EIS-AIP-PACE is a PCT additionally supporting/applying Chip Authentication (incl. passive authentication) and Terminal Authentication

[167] an inspecting authority; concretely, by a control officer

Term	Definition
	protocols in the context of AIP and is authorised by the ePass Issuer through the Document Verifier of receiving state to read a subset of data stored on the ePass. EIS-AIP-PACE in the context of [15] is similar, but not equivalent to the Extended Inspection System (EIS) as defined in [7].
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [10].
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 utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all e-Documents; see [10].
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 cycle phases.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.
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; see [10].
Improperly documented person	(in the context of the MRTD) 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; see [10].
Initialisation Data	Any data defined by the ePass manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as ePass material (IC identification data).
Inspection	The act of an official organisation (inspection authority) examining an ePass presented to it by an ePass presenter and verifying its authenticity as the ePass holder. See also [10].
Inspecting authority	see *Service Provider* below
Inspection system	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder, see [7].

Term	Definition
	See BIS-PACE and EIS-AIP-PACE for the current ST. See also BIS-BAC and EIS-AIP-BAC for general information.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The ePass's chip is an integrated circuit.
Integrity	Ability to confirm the ePass and its data elements stored upon have not been altered from that created by the ePass Issuer.
Issuing Organisation	Organisation authorised to issue an official e-Document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [10].
Issuing State	The country issuing the e-Document; see [10].
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [10]. The capacity expansion technology used is the e-Document's chip.
Machine readable electronic Document (e-Document)	(in the context of the current ST) Official document issued by a state or organisation which is used by the holder for different applications (international travel, e.g. passport, visa, official document of identity, passport of a citizen etc.) 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 [10]. In the current ST the term „Machine Readable Electronic Document" in the sense of Common Criteria is equal to „Machine Readable Travel Document" term, defined in PP [7] and 'ICAO Doc 9303' [10].
Machine readable travel document (MRTD)	Official document issued by a state or organisation 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 [10].
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the e-Document Data Page or, in the case of the TD1, the back of the e-Document, containing mandatory and optional data for machine reading using OCR methods; see [10]. The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for both PACE and BAC.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a e-Document in a form that can be read and verified by machine; see [10].
Malicious equipment	A technical device being expected, but not possessing a valid, certified key pair for its authentication (if required); validity of its certificate is not verifiable up to the respective root CertA (CVCA for a terminal and CSCA for an ID_Card).

Term	Definition
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the ePass Manufacturer completing the IC to the ePass. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and ePass Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [16]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date, - Certificate Extensions (optional).
PACE password	A password needed for PACE authentication, e.g. MRZ or other PACE passwords. Passwords used as input for PACE. This may be, for example, the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, or any other appropriate data, see [12].
PACE Terminal (PCT)	A technical system verifying correspondence between the passwords stored in the ePass and the related value presented to the terminal by the ePass presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ePass using a shared password (PACE password). See [15]
Passive authentication	Security mechanism implementing (i) verification of the digital signature of the Card/Chip or Document Security Object and (ii) comparing the hash values of the read data fields with the hash values contained in the Card/Chip or Document Security Object. See [15].
Passport (physical and electronic)	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Passport is used in order to verify that identity claimed by the Passport presenter is commensurate with the identity of the Passport holder stored on/in the card.
Password Authenticated Connection Establishment	A communication establishment protocol defined in [15]. 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

Term	Definition
(PACE)	the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the ePass.
Personalisation Agent	An organisation acting on behalf of the ePass Issuer to personalise the ePass for the ePass holder by some or all of the following activities: (i) establishing the identity of the ePass holder for the biographic data in the ePass, (ii) enrolling the biometric reference data of the ePass holder, (iii) writing a subset of these data on the physical Passport (optical personalisation) and storing them in the ePass (electronic personalisation) for the ePass holder as defined in [15], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [10] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the ePass Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalisation Data	A set of data incl. (i) individual-related data (biographic and biometric data, signature key pair(s) for the eSign application, if installed) of the ePass holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life cycle phase *card issuing*.
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised ePass and/or to secure shipment within or between the life cycle phases *manufacturing* and *card issuing*.
Pre-personalised ePass's chip	e-Document's chip equipped with a unique identifier and a unique asymmetric Authentication Key Pair of the chip.
Receiving State	The Country to which the ePass holder is applying for entry; see [10].
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
Rightful equipment (rightful terminal or rightful proximity	A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either

Term	Definition
card)	BIS-PACE or EIS-AIP-PACE (see *Inspection System*). A terminal as well as a Card can represent the rightful equipment, whereby the root CertA for a terminal is CVCA and for a Card – CSCA.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [10].
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
sensitive (biometrical) data also called *logical e-Document sensitive User Data*	The content of the DG3 and DG4 acc. to [15].
Service Provider	An official organisation (inspecting authority) providing inspection service which can be used by the ePass holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of a rightful terminal to read the ePass or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data or other PACE passwords.
Standard Inspection Procedure	A specific order of authentication steps between an ePass and a terminal as required by [15], namely (i) PACE 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 through the contactless interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated (PCT) ('Terminal' is used by the ePass presenter).
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Inspection System (Terminal) Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date. It can additionally be restricted at terminal by ePass holder using CHAT.
TOE tracing data	Technical information about the current and previous locations of the ePass gathered by inconspicuous (for the ePass holder) recognising the ePass
Travel document	A passport or other official document of identity issued by a state or organisation which may be used by the rightful holder for international travel; see [10].
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).

Term	Definition
Unpersonalised ePass	ePass material prepared to produce a personalised ePass containing an initialised and pre-personalised ePass'es chip.
User Data	See Table 2: Primary assets above. 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 [1]). 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 [2]).
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
AIP	Advanced Inspection Procedure, [15]
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [6])
BIS-PACE	Basic Inspection System with PACE (see [15])
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority (the author dispensed with the usual abbreviation 'CA' in order to avoid a collision with 'Chip Authentication')
CHAT	Certificate Holder Authorization Template
EAC	Extended Access Control
EIS-AIP-BAC	Extended Inspection System with BAC (equivalent to EIS as used in [7])
EIS-AIP-PACE	Extended Inspection System with PACE (see [15])
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCT	PACE-authenticated terminal
PP	Protection Profile
RAD	Reference Authentication Data
RF	Radio Frequency
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure, see [15]
TA	Terminal Authentication
TOE	Target of Evaluation

Acronym	Term
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)
TSS	TOE Security Service
VAD	Verification Authentication Data

9 Bibliography

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2012-09-001, Version 3.1, revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2012-09-002, Version 3.1, revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2012-09-003, Version 3.1, revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation. Evaluation methodology; CCMB-2012-09-004, Version 3.1, revision 4, September 2012

[5] Common Criteria Supporting Document. Mandatory Document. Composite product evaluation for Smart Cards and similar devices, CCDB-2012-04-001, Version 1.2, April 2012

Protection Profiles

[6] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, version 1.10, 25th March 2009

[7] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, version 1.3.2, 5th December 2012

[8] 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, 22th July. 2014

[9] Common Criteria Protection Profile Security IC Platform Protection Profile, BSI-PP-0035-2007, Version 1.0, 15th June 2007

ICAO

[10] 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

[11] ICAO Doc 9303-3, Specifications for electronically enabled official travel documents with biometric identification capabilities. In *Machine Readable Travel Documents – Part 3: Machine Readable Official Travel Documents*, volume 2, ICAO, 3rd edition, 2008.

[12] ICAO TR-SAC, MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT: Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

[13] ICAO TR-LDS, MACHINE READABLE TRAVEL DOCUMENTS, Technical Report: Development of a Logical Data Structure - LDS - for optional Capacity Expansion Technologies, May 2004

[14] ICAO TR-PKI, Technical Report: PKI for Machine Readable Travel Documents offering ICC read-only access, V1.1, 01.10.2004.

Technical Guidelines and Directives

[15] TR-03110-1, version 2.20, Technical Guideline: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26.02.2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[16] TR-03110-3, version 2.11, Technical Guideline: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specification, Version 2.11, 12.07.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[17] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 2.0, 28.06.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Cryptography

[18] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[19] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

[20] 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

[21] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001

[22] AIS31-V.2: Functionality classes and evaluation methodology for physical random number generators AIS31, Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik

Other Sources

[23] ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2000

[24] ISO 7498-2 (1989): 'Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture'

[25] ISO/IEC 11770-3:2008, Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, ISO/IEC, second edition, 15.07.2008

[26] Certification report BSI-DSZ-CC-0782-V3-2017. Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013, and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG.