Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile

Electronic Passport using
Standard Inspection Procedure with PACE
(ePass_PACE PP)

BSI-CC-PP-0068

Approved by the
Federal Ministry of Interior

Version 0.92, 30th April 2010

Foreword

This Protection Profile ‘Electronic Passport using Standard Inspection procedure with PACE (ePass_PACE PP)’ is issued by Bundesamt für Sicherheit in der Informationstechnik, Germany.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria version 3.1 [1], [2], [3], Revision 3.

Correspondence and comments to this Protection Profile should be referred to:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-53133 Bonn, Germany

Phone: **+49 228 99 9582-0**
Fax: **+49 228 99 9582-400**

Email: **bsi@bsi.bund.de**

Contents

List of Tables

1 PP Introduction

1 This section provides document management and overview information required to register the protection profile and to enable a potential user of the PP to determine, whether the PP is of interest.

1.1 PP reference

2 Title: Protection Profile 'Electronic Passport using Standard Inspection Procedure with PACE (ePass_PACE PP)'

Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
Editor(s):	Dr. Igor Furgel T-Systems GEI GmbH, SC Security Analysis & Testing
CC Version:	3.1 (Revision 3)
Assurance Level:	Minimum assurance level for this PP is EAL4 augmented.
General Status:	final
Version Number:	0.92 as of 30th April 2010
Registration:	BSI-CC-PP-0068
Keywords:	ePassport, MRTD, ICAO, PACE, Standard Inspection Procedure

1.2 TOE Overview

1.2.1 TOE definition and operational usage

3 The Target of Evaluation (TOE) addressed by the current protection profile is an electronic Passport (ePass) representing a contactless smart card programmed according to BSI TR-03110, version 2.03 [9]. This smart card provides the following application:

– the *ePassport*[1] containing the related user data[2] (incl. biometric) as well as data needed for authentication (incl. MRZ); this application is intended to be used by governmental organisations, amongst other as a machine readable travel document (MRTD).

4 For the *ePassport* application, the ePass holder can control access to his user data by conscious presenting his ePass to governmental organisations[3].

5 The ePass is integrated into a physical (plastic or paper), optically readable part of the Passport, which – as the final product – shall eventually supersede still existing, merely optically readable Passports. The plastic or paper, optically readable cover of the Passport, where the electronic Passport is embedded in, is not part of the TOE. The tying-up of the electronic Passport to the plastic Passport is achieved by physical and organisational security measures being out of scope of the current PP.

[1] as specified in [9], sec. 3.1.1; see also [7], [8].

[2] according to [9], sec. 1.1 and 3.1.1; see also chap. 7 below for definitions

[3] CAN or MRZ user authentication, see [9], sec. 3.3

6 The TOE shall comprise at least

i) the circuitry of the contactless chip incl. all IC dedicated software[4] being active in the operational phase of the TOE (the integrated circuit, IC),

ii) the IC Embedded Software (operating system)[5],

iii) the *ePassport* application and

iv) the associated guidance documentation.

7 *Application note 1:* Since contactless interface parts (e.g. antenna) may have impact on specific aspects of vulnerability assessment and, thus, be security relevant, these parts might be considered as part of the TOE. The decision upon this is up to the certification body in charge by defining the evaluation methodology for the assessment of the contactless interface.

1.2.2 TOE major security features for operational use

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

– Only terminals possessing authorisation information (a shared secret) 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 the service provider (here: inspecting governmental organisation) connected[6],
– Averting of inconspicuous tracing of the ePass,
– Self-protection of the TOE security functionality and the data stored inside.

1.2.3 TOE type

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

10 The typical life phases for the current TOE type are development[7], manufacturing[8], card issuing[9] and, finally, operational use. Operational use of the TOE is explicitly in the focus of current PP. Some single properties of the manufacturing and the card issuing life phases being significant for the security of the TOE in its operational phase are also considered by the current PP. A security evaluation/certification being conform with this PP will have to involve all life phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 2.3 'Package Claim' below).

[4] usually preloaded (and often security certified) by the Chip Manufacturer

[5] usually – together with IC – completely implementing executable functions

[6] inspecting official organisation (a kind of a service provider) is technically represented by a local RF-terminal as the end point of secure communication in the sense of this PP (local authentication)

[7] IC itself and IC embedded software

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

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

1.2.4 Non-TOE hardware/software/firmware

11 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 [15].

12 From the logical point of view, the TOE shall be able to recognise the following terminal type, which, hence, shall be available (see [9], sec. 3.2.1):

– *Basic Inspection System with PACE*: an official terminal being always operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier).

13 The TOE shall require terminals to evince possessing authorisation information (a shared secret) before access according to [9], sec. 1.1, option 'PACE' is granted. To authenticate a terminal as a basic inspection system with PACE, Standard Inspection Procedure must be used.

14 *Application note 2:* The specification [9], sec. 3.2.1 in conjunction with sec. 3.1.1 knows the following types of inspection systems:
– Basic Inspection System[10] with PACE (BIS-PACE)[11],
– Basic Inspection System with BAC (BIS-BAC)[12],
– Extended Inspection System using Advanced Inspection Procedure with PACE (EIS-AIP-PACE)[13],
– Extended Inspection System using Advanced Inspection Procedure with BAC (EIS-AIP-BAC)[14],
– Extended Inspection System using General Authentication Procedure (EIS-GAP)[15],

The current PP defines security policy for the usage of only Basic Inspection System with PACE (BIS-PACE) in the context of the ePassport application.
Using other types of inspection systems and terminals is out of the scope of the current PP.
Some developers might decide to implement their products being downwardly compatible with ICAO-terminals[16], so that they also functionally support Basic Access Control (BAC), see [9], sec. 1.1, 3.1.1 and Appendix G. However, any product *using* BAC will not be conformant to the current PP; i.e. a product implementing the TOE may *functionally* use BAC, but, while performing BAC, they are acting outside of security policy defined by the current PP. Therefore, organisations being responsible for the operation of inspection systems shall be aware of this context.

[10] a Basic Inspection Systems always uses Standard Inspection Procedure

[11] SIP with PACE means: PACE and passive authentication with SO_D according to [9], sec. 4.2, 1.1, G.1 and G.2.

[12] SIP with BAC means: BAC and passive authentication with SO_D according to [9], sec. H, 1.1, G.1 and G.2. It is commensurate with BIS in [5] and [6]; i.e. the terminal proven the possession of MRZ optically read out from the plastic part of the card.

[13] Advanced Inspection Procedure (AIP) with PACE means: PACE, chip authentication, passive authentication with SO_D and terminal authentication according to [9], sec. 4.2, 4.3 (version 1), 1.1, 4.4 (version 1), G.1 and G.3.

[14] AIP with BAC means: BAC, chip authentication, passive authentication with SO_D and terminal authentication according to [9], sec. H, 4.3 (version 1), 1.1, 4.4 (version 1), G.1 and G.3. It is commensurate with EIS in [5] and [6]; please note that this EIS also covers the General Inspection Systems (GIS) in the sense of [5] and [6].

[15] General Authentication Procedure (GAP) means: PACE, terminal authentication (version 2), passive authentication with SO_C and chip authentication (version 2) according to [9], sec. 4.2, 4.3 and 4.4.

[16] so called non-compliant inspection systems not supporting PACE, see [9], Appendix G

15 *Application note 3:* A [9]-compliant terminal[17] shall always start a communication session using PACE. If successfully, it shall then proceed with passive authentications as required by SIP in [9]. Terminal will be authorised as the BIS-PACE in the sense of [9].
If the trial with PACE failed, the [9]-compliant terminal may try to establish a communication session using other valid options as described above.

16 *Application note 4:* The authorisation level of an authenticated terminal is firmly defined by the related specification (see [9], table 1.2). It is independent of any terminal certificates may reside in the terminal connected and cannot be additionally restricted by the ePass holder. It is due to the fact that the Standard Inspection procedure neither supports a certificate-based terminal authentication nor can use Certificate Holder Authorization Template (CHAT) enabling additional restrictions by the ePass holder. Therefore, the *effective authorisation level* of the related terminal (PACE terminal) is firmly programmed in the TOE, constant one.

17 The following table gives an overview which types of terminals shall be supported for the *ePassport* application of the TOE, see [9], sec. 3.1 – 3.3:

	Basic Inspection System with PACE (official terminal)
ePassport	Operations: reading all data groups excepting DG3 and DG4 User interaction: CAN or MRZ for PACE

Table 1: ePass application vs. terminal type

[17] see appendix G of [9] for further details

2 Conformance Claims

2.1 CC Conformance Claim

18 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009 [3]

as follows

- Part 2 extended,
- Part 3 conformant.

19 The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [4]

has to be taken into account.

2.2 PP Claim

20 This PP does not claim conformance to any protection profile.

21 The 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’ [5], however does not claim any formal conformance to it. The main reason for this decision is that the current PP does not cover BAC, though a product in question may functionally implement it. In distinction from the security policy defined in [5], the *ePassport* application of the TOE uses PACE as the mandatory communication establishment protocol.

2.3 Package Claim

22 The current PP is conformant to the following security requirements package:

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

2.4 Conformance Claim Rationale

23 Since this PP does not claim conformance to any protection profile, this section is not applicable.

2.5 Conformance statement

24 This PP requires *strict* conformance of any ST or PP claiming conformance to this PP.

3 Security Problem Definition

3.1 Introduction

Assets

25 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	Generic security property to be maintained by the current security policy
		ePassport	
1	user data stored on the TOE	All data (being not authentication data) stored in the context of the *ePassport* application of the ePass as defined in [9] and (i) being allowed to be *read out* solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [9], sec. 3.2.1). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [5].	Confidentiality[18] Integrity Authenticity
2	user data transferred between the TOE and the service provider connected (i.e. an authority represented by Basic Inspection System with PACE)	All data (being not authentication data) being transferred in the context of the *ePassport* application of the ePass as defined in [9] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [9], sec. 3.2.1). User data can be received and sent (exchange ⇔ {receive, send}).	Confidentiality[19] Integrity Authenticity
3	ePass tracing data	Technical information about the current and previous locations of the ePass gathered by inconspicuous (for the ePass	unavailability[20]

[18] Though not each data element stored on the TOE represents a secret, the specification [9] anyway requires securing their confidentiality: only terminals authenticated according to [9], sec. 4.2 (PCT) can get access to the user data stored. They have to be operated according to P.Terminal.

[19] Though not each data element being transferred represents a secret, the specification [9] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [9], sec. 4.2.2.

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
		holder) recognising the TOE knowing *neither* CAN *nor* MRZ. TOE tracing data can be provided / gathered.	

Table 2: Primary assets

26 *Application Note 5*: Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the ePass holder which also include his sensitive (biometrical) data. Hence, the general security policy defined by the current PP also secures these specific ePass holder's data as stated in the table above.

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

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

Object No.	Asset	Definition	Property to be maintained by the current security policy
		ePassport	
4	Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability
5	Genuineness of the TOE	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 MRTD's chip' in [5].	Availability
6	TOE immanent secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	TOE immanent non-secret cryptographic material	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
8	ePass	Restricted-revealable[21]	Confidentiality[21]

[20] represents a prerequisite for anonymity of the ePass holder

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

Object No.	Asset	Definition	Property to be maintained by the current security policy
	communication establishment authorisation data	authorisation information for a human user being used for verification of the authorisation attempts as authorised user (CAN, MRZ). These data are stored in the TOE and are not to convey to it.	Integrity

Table 3: Secondary assets

29 *Application Note 6*: Since the ePass does not support any secret ePass holder authentication data like PIN and PUK (see [9], sec. 3.3) and the latter may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device, a successful PACE-authentication of a terminal does not unambiguously mean that the ePass holder is using TOE.

30 *Application Note 7*: ePass communication establishment authorisation data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorisation attempt.
The TOE shall secure the reference information as well as – together with the terminal connected[22] – the verification information in the 'TOE <-> terminal' channel, if it has to be transferred to the TOE. Please note that CAN and MRZ are not to convey to the TOE.

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

Subjects and external entities

32 This protection profile considers the following subjects:

External Entity No.	Subject No.	Role	Definition
1	1	ePass holder	A person for whom the ePass Issuer has personalised the ePass[23]. This entity is commensurate with 'MRTD Holder' in [5]. Please note that an ePass holder can also be an attacker (s. below).
2	-	ePass presenter	A person presenting the ePass to a terminal[24] and claiming the identity of the ePass holder. This external entity is commensurate with 'Traveller' in [5]. Please note that an ePass presenter can also be an attacker (s. below).
3	-	Service Provider (SP)	An official organisation (inspection authority)

[22] the input device of the terminal

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

[24] in the sense of [9]

External Entity No.	Subject No.	Role	Definition
			providing inspection service which can be used by the ePass holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
4	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not PCT ('Terminal' is used by the ePass presenter). This entity is commensurate with 'Terminal' in [5].
5	3	PACE Terminal (PCT)	A technical system verifying correspondence between the password 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 (CAN or MRZ). A PCT is allowed reading User Data excepting DG3 and DG4 (see sec. 1.1 in [9]). See also *Application note 2* and par. 17 above and [9], chap. 3.3, 4.2, table 1.2 and G.2
6	4	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority[25] 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). The Basic Inspection System with PACE is a PCT additionally supporting/applying the Passive Authentication protocol and is authorised[26] by the ePass Issuer through the Document Verifier of receiving state to read a subset of data stored on the ePass. BIS-PACE in the context of [9] (and of the current PP) is similar, but not equivalent to the Basic Inspection System (BIS) as defined in [5]. See also *Application note 2* and par. 17 above and [9], chap. 3.2.1, G.1 and G.2.
7	-	Document Verifier (DV)	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.

[25] concretely, by a control officer

[26] by organisational measures

External Entity No.	Subject No.	Role	Definition
			terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a CertA, authorised by at least the national CVCA to issue certificates for national terminals, see [9], chap. 2.2.2. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this PP. 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[27] between the ePass Issuer und a foreign CVCA ensuring enforcing the ePass Issuer's privacy policy[28]). This external entity is commensurate with 'Document Verifier' in [5].
8	-	Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the ePass Issuer with respect to protection of user data stored in the ePass (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [9], chap. 2.2.1. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organisational entity within this PP. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [7]) 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 [9], sec. 2.2.1.
9	-	Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored

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

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

External Entity No.	Subject No.	Role	Definition
			on the ePass for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [9], chap. 1.1 and [7]. This role is usually delegated to a Personalisation Agent.
10	-	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 ePasss 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. [7], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [7]) 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 [9], sec. 2.2.1.
11	5	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 [9], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [7] (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 [5].
12	6	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 phase[29]. The TOE itself does not distinguish between the IC Manufacturer and

[29] cf. also par. 10 in sec. 1.2.3 above

External Entity No.	Subject No.	Role	Definition
			ePass Manufacturer using this role Manufacturer. This entity is commensurate with ‘Manufacturer’ in [5].
13	-	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most *high* attack potential. Please note that the attacker might ‘capture’ any subject role recognised by the TOE. This external entity is commensurate with ‘Attacker’ in [5].

Table 4: Subjects and external entities[30]

33 *Application Note 8*: Since the TOE does not use BAC, a Basic Inspection System with BAC (BIS-BAC) cannot be recognised by the TOE, see *Application note 2* above.

3.2 Threats

34 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.

35 The following threats are defined in the current PP (they are initially derived from the ICAO-BAC PP [5] and ICAO-EAC PP [6], then from the ID_Card PP BSI-CC-PP-0061-2009):

36 **T.Skimming** **Skimming ePass / Capturing Card-Terminal Communication**

An attacker imitates an inspection system in order to get access to the *user data stored on* or *transferred between the TOE and the service provider (inspecting authority) connected* via the contactless interface of the TOE. The attacker cannot read and does not know the correct value of the shared password (CAN, MRZ) in advance.

Application Note 9: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this PP. 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 PP; see also the *Application note 2* above.

[30] 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 does not differ between ‘subjects’ and ‘external entities’. There is no dedicated subject with the role ‘attacker’ within the current security policy, whereby an attacker might ‘capture’ any subject role recognised by the TOE.

Application Note 10: This threat also covers the item T.Read_Sensitive_Data in the ICAO-EAC PP [6]: 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.

Application Note 11: MRZ is printed and CAN is printed or stuck on the Passport. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Card-Holder.

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

An attacker is listening to the communication between the ePass and the PACE terminal (PCT) in order to gain the *user data transferred between the TOE and the service provider (inspecting authority) connected*.

Application Note 12: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this PP. 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 PP; see also the *Application note 2* above.

38 **T.Tracing** **Tracing ePass**

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. The attacker cannot read and does not know the correct values of shared passwords (CAN, MRZ) in advance.

Application Note 13: 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 PP, see also the *Application note 2* above.

39 *Application Note 14*: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the ePass'es chip (no Chip Authentication), a threat like T.Counterfeit (counterfeiting ePass)[31] cannot be averted by the current TOE.

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

An attacker fraudulently alters the User Data or/and TSF-data stored on the ePass or/and exchanged between the TOE and the service provider (inspecting authority) connected in order to outsmart the authenticated terminal (PCT) 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 service provider (represented by the terminal connected) perceives these modified data as authentic one.

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

[31] Such a threat might be formulated like: 'An attacker produces an unauthorised copy or reproduction of a genuine ePass to be used as part of a counterfeit Passport: he or she may generate a new data set or extract completely or partially the data from a genuine ePass and copy them on another functionally appropriate chip to imitate this genuine ePass. This violates the authenticity of the ePass being used for authentication of an ePass presenter as the ePass holder'.

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.

Application Note 15: 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.

42 **T.Information_Leakage Information Leakage from ePass**

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data. The information leakage may be inherent in the normal operation or caused by the attacker.

Application Note 16: Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are 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).

43 **T.Phys-Tamper Physical Tampering**

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.

Application Note 17: 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.

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

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.

Application note 18: 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

45 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.

46 **P.Pre-Operational** **Pre-operational handling of the ePass**

1) The ePass Issuer issues the ePasss 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 ePasss in their manufacturing and issuing life phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 above.

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

47 **P.Card_PKI** **PKI for Passive Authentication (issuing branch)**

Application Note 19: 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 make the CSCA Certificate (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 [7], 5.5.1. The CSCA shall

[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 PP in order to reflect an appropriate relationship between the parties involved.

create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the ePass Issuer, see [7], 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 ePasses.

48 **P.Trustworthy_PKI Trustworthiness of PKI**

1) 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 ePasss.

49 **P.Terminal Abilities and trustworthiness of terminals**

50 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.

51 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 Service Providers and by ePass holders as defined in [9], sec. 3.2.

2) They shall implement the terminal parts of the PACE protocol [9], sec. 4.2, of the Passive Authentication [9], sec. 1.1 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-Hellmann).

3) The related terminals need not to use any own credentials.

4) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data gro ups stored in the *ePassport*, [9], sec. 1.1).

5) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of CAN and MRZ, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

[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-F} 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, sec. 3.1.1 of [9]. Other branches of this figure are not covered by the security policy of the current PP.

3.4 Assumptions

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

53 The current PP does not include any assumptions.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

56 **OT.Data_Integrity 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 service provider (inspecting authority) connected (and represented by PCT) after the PACE Authentication.

57 **OT.Data_Authenticity 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 service provider (inspecting authority) connected (and represented by 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].

58 **OT.Data_Confidentiality 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 terminal (PCT) connected.
The TOE must ensure confidentiality of the User Data and the TSF-data[41] during their exchange between the TOE and the service provider (inspecting authority) connected (and represented by PCT) after the PACE Authentication.

Application note 20: Since the Standard Inspection Procedure does not support any certificate-based authorisation of the terminal connected (no CHAT), the effective terminal authorisation level is firmly predefined as specified in [9], sec. 1.1 (option PACE) and can neither additionally be restricted by the ePass holder. This fixed effective terminal authorisation level does not allow any access to sensitive biometrical data (DG3, DG4).

[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 [9], sec. 4.2.2

[41] where appropriate, see Table 3 above

59 **OT.Tracing** **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 (CAN, MRZ) in advance.

60 *Application note 21:* Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the ePass'es chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of ePass authenticity)[42] cannot be achieved by the current TOE.

61 **OT.Prot_Abuse-Func** **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.

62 **OT.Prot_Inf_Leak** **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.

Application note 22: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

63 **OT.Prot_Phys-Tamper** **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

[42] Such a security objective might be formulated like: 'The TOE must enable the terminal connected to verify the authenticity of the ePass as a whole device as issued by the ePass Issuer (issuing PKI branch of the ePass Issuer) by means of the Passive and Chip Authentication as defined in [9], sec. 4.3'.

– reverse-engineering to understand the design and its properties and functionality.

64 **OT.Prot_Malfunction Protection against Malfunctions**

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

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

66 **OT.Identification Identification of the TOE**

The TOE must provide means to store Initialisation[43] 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 phases of the ePass.

67 **OT.Personalisation Personalisation of ePass**

The TOE must ensure that the user data (amongst other those concerning the ePass holder[44]) and the TSF-data permanently stored in the TOE can be written by authorised Personalisation Agents only. The Document Security Object can be updated by authorised Personalisation Agents (in the role of DS), if the related data have been modified.

4.2 Security Objectives for Operational Environment

I. ePass Issuer as the general responsible

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

69 **OE.Legislative_Compliance**

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

II. ePass Issuer and CSCA: ePass'es PKI (issuing) branch

70 The ePass Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the *Application Note 19* above):

71 **OE.Passive_Auth_Sign Authentication of ePass by Signature**

[43] amongst other, IC Identification data

[44] biographical and biometrical data

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) 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[45]. 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 [7], sec. A.10.4.

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.

72 **OE.Personalisation 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 [9], sec. 1.1[46], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [7] (in the role of a DS).

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

73 For Standard Inspection Procedure, there is only issuing PKI branch. Nevertheless, the ePass Issuer and the related domestic CVCA as well as the foreign CVCAs under agreement (with the ePass Issuer)[47] will implement the following security objectives for the TOE environment:

74 **OE.Terminal Terminal operating**

The Service Providers (inspection authorities / official organisations) participating in the current PKI[48] (and, hence, acting in accordance with the policy of the related DV) must operate their terminals as follows:

1) The related terminals (basic inspection systems, cf. Table 1 above) are used by Service Providers and by ePass holders as defined in [9], sec. 3.2.

2) The related terminals implement the terminal parts of the PACE protocol [9], sec. 4.2, of the Passive Authentication [9], sec. 1.1 (by verification of the signature of the Document

[45] CVCAs represent the roots of receiving branch, see below

[46] see also [7], sec. 10

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

[48] there is only issuing branch for Standard Inspection Procedure; the receiving branch is completely absent.

Security Object) and use them in this order[49]. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3) The related terminals need not to use any own credentials.

4) 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*, [9], sec. 1.1).

5) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of CAN and MRZ, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

IV. ePass holder Obligations

75 **OE.Card-Holder** **ePass holder Obligations**

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

4.3 Security Objective Rationale

76 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.Personalisation	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_Malfuntion	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Card-Holder	OE.Legislative_Compliance
T.Skimming			x	x	x									x	
T.Eavesdropping					x										

[49] This order is only commensurate with the branch leftmost in Fig. 3.1, sec. 3.1.1 of [9]. Other branches of this figure are not covered by the security policy of the current PP.

	OT.Identification	OT.Personalisation	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_Malfuntion	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Card-Holder	OE.Legislative_Compliance
T.Tracing						x								x	
T.Forgery		x	x	x			x		x			x	x		
T.Abuse-Func							x								
T.Information_Leakage								x							
T.Phys-Tamper									x						
T.Malfunction										x					
P.Pre-Operational	x	x									x				x
P.Terminal													x		
P.Card_PKI												x			
P.Trustworthy_PKI												x			

Table 5: Security Objective Rationale

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

78 The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the Service Provider) using the TOE’s contactless interface. This threat is countered by the security objectives OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality through the PACE authentication. The objective OE.Card-Holder ensures that a PACE session can only be established either by the ePass holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

79 The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a rightful terminal in order to gain the User Data transferred there. This threat is countered by the security objective OT.Data_Confidentiality through a trusted channel based on the PACE authentication.

80 The threat **T.Tracing** addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE, whereby the attacker does not a priori know the correct values of CAN or MRZ). This threat is directly countered by security objectives OT.Tracing (no gathering TOE tracing data) and OE.Card-Holder (the attacker does not a priori know the correct values of the shared passwords).

81 The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the Service Provider. The security objective OT.Personalisation requires the TOE to limit the write access for the ePass

to the trustworthy Personalisation Agent (cf. OE.Personalisation). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives OT.Data_Integrity and OT.Data_Authenticity, respectively. The objectives OT.Prot_Phys-Tamper and OT.Prot_Abuse-Func contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A Service Provider operating his terminals according to OE.Terminal and performing the Passive Authentication using the Document Security Object as aimed by OE.Passive_Auth_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE.

82 The threat **T.Abuse-Func** addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-coded security functionality. The security objective OT.Prot_Abuse-Func ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

83 The threats **T.Information_Leakage**, **T.Phys-Tamper** and **T.Malfunction** are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is obviously addressed by the directly related security objectives OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper and OT.Prot_Malfunction, respectively.

84 The OSP **P.Pre-Operational** is enforced by the following security objectives:
OT.Identification is affine to the OSP's property 'traceability before the operational phase';
OT.Personalisation and OE.Personalisation together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents';
OE.Legislative_Compliance is affine to the OSP's property 'compliance with laws and regulations'.

85 The OSP **P.Terminal** is obviously enforced by the objective OE.Terminal, whereby the one-to-one mapping between the related properties is applicable.

86 The OSP **P.Card_PKI** is enforced by establishing the issuing PKI branch as aimed by the objectives OE.Passive_Auth_Sign (for the Document Security Object).

87 The OSP **P.Trustworthy_PKI** is enforced by OE.Passive_Auth_Sign (for CSCA, issuing PKI branch).

5 Extended Components Definition

88 This protection profile uses components defined as extensions to CC part 2. Most of them are drawn from [6].

5.1 Definition of the Family FAU_SAS

89 To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

90 The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behaviour

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

Component levelling

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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components

Dependencies: No dependencies

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

5.2 Definition of the Family FCS_RND

91 To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is

not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

92 The family ‘Generation of random numbers (FCS_RND)’ is specified as follows:

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers intended to be used for cryptographic purposes.

Component levelling:

FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3 Definition of the Family FIA_APO

93 To describe the IT security functional requirements of the TOE, the family FIA_APO of the class FIA (Identification and authentication) is defined here. This family describes the functional requirements for proof of the claimed origin for the authentication verification by an external entity, where the other families of the class FIA address the verification of the identity[50] of an external entity.

94 *Application note 23:* Other families of the class FIA describe only the authentication verification of user’s identity performed by the TOE and do not describe the functionality of the TOE to prove its own origin. The following paragraph defines the family FIA_APO in the style of the Common Criteria part 2 (cf. [3], chapter ‘Extended components definition (APE_ECD)’) from a TOE point of view.

[50] and in a certain sense also the origin

FIA_APO Authentication Proof of Origin

Family behaviour

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

Component levelling:

FIA_APO.1 Authentication Proof of Origin.

Management: FIA_APO.1

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

Audit: FIA_APO.1

There are no actions defined to be auditable.

FIA_APO.1 Authentication Proof of Origin

Hierarchical to: No other components

Dependencies: No dependencies

FIA_APO.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the origin of the [assignment: *authorised user or role*].

5.4 Definition of the Family FMT_LIM

95 The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.

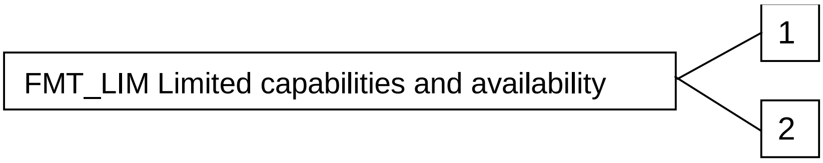
96 The family ‘Limited capabilities and availability (FMT_LIM)’ is specified as follows:

FMT_LIM Limited capabilities and availability

Family behaviour

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

Component levelling:



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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components

Dependencies: FMT_LIM.2 Limited availability

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components

Dependencies: FMT_LIM.1 Limited capabilities

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

97 *Application note 24:* The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced or conversely

(ii) the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

5.5 Definition of the Family FPT_EMSEC

98 The family FPT_EMSEC (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [2].

99 The family 'TOE Emanation (FPT_EMSEC)' is specified as follows:

FPT_EMSEC TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components
Dependencies: No dependencies
FPT_EMSEC.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of

[assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

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

6 Security Requirements

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

101 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 PP.

102 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~~.

103 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

104 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicised*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicised like *this*.

105 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

106 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 PP defined the security functional groups and allocated the functional requirements described in the following sections to them:

Security Functional Groups	Security Functional Requirements concerned
Access control to the User Data stored in the TOE	– {FDP_ACC.1/TRM, FDP_ACF.1/TRM} Supported by: – FIA_UAU.1/PACE: PACE Authentication (PCT)
Secure data exchange between the ePass and the service provider (inspecting	– FTP_ITC.1/PACE: trusted channel

Security Functional Groups	Security Functional Requirements concerned
authority) connected	Supported by: – FCS_COP.1/AES: encryption/decryption – FCS_COP.1/CMAC: MAC generation/verification – FIA_APO.1/PA: Passive Authentication – FIA_UAU.1/PACE: PACE Authentication (PCT)
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (PCT) – FIA_UAU.1/PACE: PACE Authentication (PCT) – FIA_APO.1/PA: Passive Authentication – FIA_UAU.4: single-use of authentication data – FIA_UAU.5: multiple authentication mechanisms – FIA_UAU.6: Re-authentication of Terminal – 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 (PCT) – FCS_CKM.2/DH: Diffie-Hellmann key distribution within PACE authentication – FCS_CKM.4: session keys destruction (authentication expiration) – FCS_RND.1: random numbers generation – FMT_SMR.1: 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.

Security Functional Groups	Security Functional Requirements concerned
	Supported by: – the entire class FIA: user identification / authentication
Accuracy of the TOE security functionality / Self-protection	– The entire class FPT – FDP_RIP.1: enforced memory/storage cleaning Supported by: – the entire class FMT.

Table 6: Security functional groups vs. SFRs

107 The following table provides an overview of the keys and certificates used for enforcing the security policy defined in the current PP:

Name	Data
Receiving PKI branch	
	No receiving PKI branch is necessary for the current TOE due to applying Standard Inspection Procedure
Issuing PKI branch	
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 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. [7], 5.5.1.
Document Signer Key Pairs and Certificates	The Document Signer Certificate C_{DS} is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK_{DS}) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object (SO_D) of the ePass with the Document Signer Private Key (SK_{DS}) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK_{DS}).
Session keys	
PACE Session Keys (PACE-K_{MAC}, PACE-K_{Enc})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) agreed between the TOE and a terminal (PCT[51]) as result of the PACE Protocol, see [9], sec. A.3, F.2.2, A.2.3.2.
Ephemeral keys	
PACE authentication ephemeral key pair (ephem-SK_{PICC}-PACE,	The ephemeral PACE Authentication Key Pair {ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE } is used for Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or

[51] From the point of view of the terminal's rights, there is no difference beween PCT and BIS-PACE, cf. glossary

Name	Data
ephem-PK_{PICC}-PACE)	Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 [11], cf. [9], table. A.2.

Table 7: Keys and Certificates

6.1.2 Class FCS Cryptographic Support

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

108 **FCS_CKM.1/DH_PACE 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]: fulfilled by FCS_CKM.2/DH.

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

FCS_CKM.1.1/ DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [11]*][52] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [9], Appendix A.3 [53].

109 *Application note 25:* The TOE generates a shared secret value *K* with the terminal during the PACE protocol, see [9], sec. 4.2 and A.3. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [13]) or on the ECDH compliant to TR-03111 [11] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [9], Appendix A.3 and [11] for details). The shared secret value *K* is used for deriving the AES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [9], F.2.2 and A.2.3.2 for the TSF required by FCS_COP.1/AES and FCS_COP.1/CMAC.

110 **FCS_CKM.2/DH Cryptographic key distribution – Diffie-Hellman**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: fulfilled by FCS_CKM.1/DH_PACE
FCS_CKM.4: fulfilled by FCS_CKM.4

[52] [*assignment: cryptographic key generation algorithm*]

[53] [assignment: *list of standards*]

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the list below[54] that meets the following:

a) PACE: as specified in [9], sec. 4.2 and A.3[55].

111 **FCS_CKM.4** **Cryptographic key destruction – Session keys**

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.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

112 *Application note 26:* The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

6.1.2.2 Cryptographic operation (FCS_COP.1)

113 **FCS_COP.1/AES** **Cryptographic operation – Encryption / Decryption AES**

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/AES The TSF shall perform secure messaging – encryption and decryption [56] in accordance with a specified cryptographic algorithm AES in CBC mode [57] and cryptographic key sizes [selection: *128, 192, 256*] bit [58] that meet the following: FIPS 197 [12] and [9] Appendix F.2.2[59].

[54] [assignment: *cryptographic key distribution method*]

[55] [assignment: *list of standards*]

[56] [assignment: *list of cryptographic operations*]

[57] [assignment: *cryptographic algorithm*]

[58] [assignment: *cryptographic key sizes*]

114 *Application note 27:* This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{Enc}). Note that in accordance with [9] Appendix F.2.1 and A.2.3.1 the (two-key) Triple-DES could be used in CBC mode for secure messaging. Due to the fact that the (two-key) Triple-DES is not recommended any more (cf. [10], sec. 1.3), Triple-DES in any mode is no longer applicable within this PP.

115 **FCS_COP.1/CMAC** **Cryptographic operation – CMAC**

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/ CMAC	The TSF shall perform secure messaging – message authentication code [60] in accordance with a specified cryptographic algorithm CMAC [61] and cryptographic key sizes [selection: *128, 192, 256*] bit [62] that meet the following: 'The CMAC Mode for Authentication, NIST Special Publication 800-38B' [14] and [9] Appendix F.2.2[63].

116 *Application note 28*: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}). Note that in accordance with [9] Appendix F.2.1 and A.2.3.1 the (two-key) Triple-DES could be used in Retail mode for secure messaging. Due to the fact that the (two-key) Triple-DES is not recommended any more (cf. [10], sec. 1.3), Triple-DES in any mode is no longer applicable within this PP.

6.1.2.3 Random Number Generation (FCS_RND.1)

117 **FCS_RND.1** **Quality metric for random numbers**

Hierarchical to:	No other components.

[59] [assignment: *list of standards*]

[60] [assignment: *list of cryptographic operations*]

[61] [assignment: *cryptographic algorithm*]

[62] [assignment: *cryptographic key sizes*]

[63] [assignment: *list of standards*]

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

118 *Application note 29*: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4.

6.1.3 Class FIA Identification and Authentication

119 For the sake of better readability, Table 8 provides an overview of the authentication mechanisms used:

Name	SFR for the TOE	Comments
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5 FIA_AFL.1/PACE	as required by FCS_CKM.1/DH_PACE
Passive Authentication	FIA_APO.1/PA, FIA_UAU.5	no related cryptographic operations by the TOE

Table 8: Overview of authentication SFRs

120 **FIA_AFL.1/PACE** **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 1[64] unsuccessful authentication attempt~~s~~ occur**s** related to authentication attempts using CAN and MRZ as shared passwords for PACE[65].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[66], the TSF shall [assignment: *list of actions*].

121 *Application Note 30*: The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (CAN, MRZ, see [9], sec. G.1) or for an arbitrary subset of them or may

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

[65] [assignment: *list of authentication events*]

[66] [selection: *met ,surpassed*]

also separately be defined for each datum in question.

Since all non-blocking authorisation data (CAN and MRZ) being used as a shared secret within the PACE protocol do not possess a sufficient entropy[67], the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack[68] requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the current PP.

One of some opportunities for performing this operation might be '*consecutively increase the reaction time of the TOE to the next authentication attempt using CAN and MRZ*'.

122 *Application Note 31*: Please note that since guessing CAN and MRZ requires an attack potential beyond high according to the current PP, monitoring SO_D in the context of passive authentication will also fail (due to FTP_ITC.1/PACE), so that it is not essential, whether SO_D 'ePass-generation / batch' or 'ePass-individual' data are. In fact, according to [7], sec. A.10.4, SO_D can only be 'ePass-individual'.

123 **FIA_APO.1/PA** **Authentication Proof of Origin**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_APO.1.1	The TSF shall provide the Passive Authentication according to [9], sec. 1.1 [69] to prove the origin of the ePassport [70].

124 *Application note 32:* The Passive Authentication making evident the authenticity/origin of data stored in the *ePassport* application by verifying the Document Security Object (SO_D) up to CSCA shall be triggered by the PCT immediately after the selection of *ePassport.*

Please note that this SFR does not require authentication of any TOE's user, but providing evidence enabling an external entity (the terminal connected) to prove the origin of *ePassport* application.

Independent of the result of Passive Authentication, secure messaging is continued using the previously established session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

125 **FIA_UID.1/PACE** **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 [9], sec. 4.2[71]

[67] ≥ 100 bits; a theoretical maximum of entropy which can be delivered by a character string is N*ld(C), whereby N is the length of the string, C – the number of different characters which can be used within the string.

[68] guessing CAN or MRZ, see T.Skimming above

[69] [assignment: *authentication mechanism*]

[70] [assignment: *authorised user or role*]

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

126 *Application note 33:* User identified after a successfully performed PACE protocol is a PACE terminal (PCT). Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. it is either the ePass holder itself or an authorised other person or device (BIS-PACE).

127 *Application note 34:* In the life 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).

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

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FIA_UAU.1.1	The TSF shall allow 1. establishing a communication channel, 2. carrying out the PACE Protocol according to [9], sec. 4.2[72],[73] 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.

129 *Application note 35:* The user authenticated after a successfully performed PACE protocol is a PACE terminal (PCT). Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. it is either the ePass holder itself or an authorised other person or device (BIS-PACE).
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.

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

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

[72] ePass identifies itself within the PACE protocol by selection of the authentication key ephem-PK_{PICC}-PACE

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

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 [9], sec. 4.2[74].

131 *Application note 36:* For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits length being (almost) uniformly distributed (the current PP supports the key derivation function based on AES; see [9], sec. A.3.3 and A.2.3).

132 **FIA_UAU.5** **Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

the Standard Inspection Procedure as the sequence

1. PACE Protocol according to [9], sec. 4.2,
2. Passive Authentication according to [9], sec. 1.1

and

3. Secure messaging in encrypt-then-authenticate mode according to [9], Appendix F [75]

to support user authentication.

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.[76]

133 *Application note 37:* 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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal. [77]

135 *Application note 38:* The PACE protocol specified in [9] 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 CMAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CMAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

6.1.4 Class FDP User Data Protection

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

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACF.1/TRM
FDP_ACC.1.1	The TSF shall enforce the Terminal Access Control SFP [78] on terminals gaining write, read, modification and usage access to the User Data stored in the ePass [79].

137 **FDP_ACF.1/TRM** **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.

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

[78] [assignment: *access control SFP*]

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

FDP_ACF.1.1 The TSF shall enforce the Terminal Access Control SFP[80] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. PACE Terminal (PCT);
2. Objects:
   User Data stored in the TOE;
3. Security attributes:
   a. Authentication status of terminals[81].

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

1. A PCT (BIS-PACE) is allowed to read User Data (except DG3[82] and DG4[83]) according to [9], sec. 1.1 and G.2 after a successful PACE authentication as required by FIA_UAU.1/PACE.[84]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[85].

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 PCT is not allowed to read, to write, to modify, to use any User Data stored on the ePass.
2. Nobody is allowed to read, to write, to modify, to use DG3 and DG4 stored on the ePass.
3. Nobody is allowed to read 'TOE immanent secret cryptographic keys' stored on the ePass[86][87].

138 *Application note 39*: Please note that the Document Security Object (SO_D) stored in EF.SOD (see [7], sec. A.10.4) does not belong to the user data, but to the TSF-data. The Document Security Object can be read out by the PCT, see [9], G.1.

139 *Application note 40*: Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.

140 **FDP_RIP.1** **Subset residual information protection**

[80] [assignment: *access control SFP*]

[81] [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*]

[82] biometric: finger

[83] biometric: iris

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

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

[86] for the current TOE, there are no *permanently* stored secret cyrptographic keys

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

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 [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: 1. session keys (PACE-K_{MAC}, PACE-K_{Enc}) (by closing related communication session), 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret *K*[88]), 3. [assignment: *list of objects*].

141 *Application note 41*: 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_EMSEC. 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.

6.1.5 Class FTP Trusted Path/Channels

142 **FTP_ITC.1/PACE** **Inter-TSF trusted channel after PACE**

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~~ **PACE terminal (PCT) after PACE** 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~~ **the PCT**[89] 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 PCT after PACE. [90]

143 *Application note 42*: 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

[88] according to [9], sec. 4.2.1, #3.b

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

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

of *operational* trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/AES and FCS_COP.1/CMAC.
The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

144 *Application note 43*: 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

145 **FAU_SAS.1** **Audit storage**

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[91] with the capability to store the Initialisation and Pre-Personalisation Data [92] in the audit records.

146 *Application note 44*: The Manufacturer role is the default user identity assumed by the TOE in the life phase ‘manufacturing’. The IC manufacturer and the ePass 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

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Initialisation,

[91] [assignment: *authorised users*]

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

2. Personalisation,
3. Configuration.[93]

149 **FMT_SMR.1** **Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE see also the *Application note 45* below.

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalisation Agent,
3. Terminal,
4. PACE Terminal (PCT),
5. ePass holder. [94]

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

150 *Application note 45*: For explanation on the role Manufacturer please refer to the *Application note 44*; on the role Personalisation Agent – to the *Application note 34*. 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 the ePass holder or an authorised other person or device (BIS-PACE) by using PCT (FIA_UAU.1/PACE).
The roles CVCA and DV may exist within the receiving branch cannot be recognised by the TOE due to the fact that SIP does not presume any analysing the current Terminal Certificate C_T.

151 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.

152 **FMT_LIM.1** **Limited capabilities**

Hierarchical to: No other components.

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

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

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

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. embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[95]

153 **FMT_LIM.2** **Limited availability**

Hierarchical to: No other components.

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

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

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[96]

154 **FMT_MTD.1/INI_ENA** **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

FMT_MTD.1.1 The TSF shall restrict the ability to write [97] the Initialisation Data and Pre-personalisation Data[98] to the Manufacturer. [99]

155 **FMT_MTD.1/INI_DIS** **Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data**

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

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

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

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

[99] [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

FMT_MTD.1.1 The TSF shall restrict the ability to read out and to use [100] the Initialisation Data [101] to the Personalisation Agent. [102]

156 *Application note 46:* 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 phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life phase 'issuing' to the life phase 'operational use'. Please also refer to the *Application note 34*.

157 **FMT_MTD.1/PA_UPD** **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

FMT_MTD.1.1 The TSF shall restrict the ability to write [103] the Document Security Object (SO_D)[104] to the Personalisation Agent. [105]

158 *Application note 47*: 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. The latter consist of user- and TSF- data, as well. Due to this fact and to the scope of the SFR FMT_MTD.1 (management of TSF-data), the entire set of the personalisation data is formally not addressed above. Nevertheless, FMT_MTD.1/PA_UPD shall be understood in the following way: 'The TSF shall restrict the ability to write the personalisation data to the Personalisation Agent.' On the role 'Personalisation Agent' please refer to the *Application note 34*.

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

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

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

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

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

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

6.1.8 Class FPT Protection of the Security Functions

159 The TOE shall prevent inherent and forced illicit information leakage for the User Data and TSF-data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements 'Failure with preservation of secure state (FPT_FLS.1)' and 'TSF testing (FPT_TST.1)' on the one hand and 'Resistance to physical attack (FPT_PHP.3)' on the other. The SFRs 'Limited capabilities (FMT_LIM.1)', 'Limited availability (FMT_LIM.2)' and 'Resistance to physical attack (FPT_PHP.3)' together with the 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.

160 **FPT_EMSEC.1** **TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. session keys (PACE-K_{MAC}, PACE-K_{Enc}),
2. the ephemeral private key ephem-SK_{PICC}-PACE,
3. [assignment: *list of types of TSF data*]

and

4. [assignment: *list of types of user data*].

FPT_EMSEC.1.2 The TSF shall ensure any users [106] are unable to use the following interface ePass'es contactless interface and circuit contacts [107] to gain access to

1. session keys (PACE-K_{MAC}, PACE-K_{Enc}),
2. the ephemeral private key ephem-SK_{PICC}-PACE,
3. [assignment: *list of types of TSF data*]

and

4. [assignment: *list of types of user data*].

161 *Application note 48*: The TOE shall prevent 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 ePass'es chip has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in

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

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

the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1,
3. [assignment: *list of types of failures in the TSF*].

164 **FPT_TST.1** **TSF testing**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [*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]*] to demonstrate the correct operation of the TSF[108].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[109].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[110].

165 *Application note 49*: If the ePass'es chip uses state of the art smart card technology, it will run some self tests at the request of an authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the 'authorised user' Manufacturer in the life phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

166 **FPT_PHP.3** **Resistance to physical attack**

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

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing [111] to the TSF [112] by responding automatically such that the SFRs are always enforced.

167 *Application note 50*: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

6.2 Security Assurance Requirements for the TOE

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

- ALC_DVS.2 (Sufficiency of security measures),
- ATE_DPT.2 (Testing: security enforcing modules) and
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.Identification	OT.Personalisation	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_Malfuntion
FCS_CKM.1/DH_PACE			x	x	x					
FCS_CKM.2/DH			x	x	x					

[111] [assignment: *physical tampering scenarios*]

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

	OT.Identification	OT.Personalisation	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_Malfuntion
FCS_CKM.4			x	x	x					
FCS_COP.1/AES					x					
FCS_COP.1/CMAC			x	x						
FCS_RND.1			x	x	x					
FIA_AFL.1/PACE						x				
FIA_APO.1/PA			x	x						
FIA_UID.1/PACE			x	x	x					
FIA_UAU.1/PACE			x	x	x					
FIA_UAU.4			x	x	x					
FIA_UAU.5			x	x	x					
FIA_UAU.6			x	x	x					
FDP_ACC.1/TRM			x		x					
FDP_ACF.1/TRM			x		x					
FDP_RIP.1			x	x	x					
FTP_ITC.1/PACE			x	x	x	x				
FAU_SAS.1	x	x								
FMT_SMF.1	x	x	x	x	x					
FMT_SMR.1	x	x	x	x	x					
FMT_LIM.1							x			
FMT_LIM.2							x			
FMT_MTD.1/INI_ENA	x	x								
FMT_MTD.1/INI_DIS	x	x								
FMT_MTD.1/PA_UPD		x	x	x	x					
FPT_EMSEC.1								x		
FPT_FLS.1								x		x
FPT_TST.1								x		x
FPT_PHP.3			x					x	x	

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

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

171 The security objective **OT.Identification** addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip.
This will be ensured by TSF according to SFR FAU_SAS.1.
The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data

in the life phase ‘operational use’.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

172 The security objective **OT.Personalisation** aims that only Personalisation Agent can write the User- and the TSF-data into the TOE.
The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data.
FMT_MTD.1/PA_UPD covers the related property of OT.Personalisation (writing/updating SO_D and, in generally, personalisation data).
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

173 The security objective **OT.Data_Integrity** aims that the TOE always ensures integrity of the User- and TSF-data stored and, after the PACE authentication, of these data exchanged (physical manipulation and unauthorised modifying).
Physical manipulation is addressed by FPT_PHP.3.
Logical manipulation of stored user data is addressed by (FDP_ACC.1, FDP_ACF.1).
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used.
Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/CMAC. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and FCS_CKM.2/DH and possessing the special properties FIA_UAU.5, FIA_UAU.6. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}). FIA_APO.1/PA requires performing Passive Authentication using SO_D for enabling the verification of the integrity of User Data stored on the TOE.
FMT_MTD.1/PA_UPD requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be modified by the Personalisation Agent only and, hence, is to consider as trustworthily.
The SFR FCS_RND.1 represents a general support for cryptographic operations needed.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

174 The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF-data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself.
This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/CMAC. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and FCS_CKM.2/DH and possessing the special properties FIA_UAU.5, FIA_UAU.6. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}). FIA_APO.1/PA requires performing Passive Authentication using SO_D for enabling the verification of the authenticity of User Data stored on the TOE.
FMT_MTD.1/PA_UPD requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be modified by the Personalisation Agent only and, hence, is to consider as trustworthily.
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used.
The SFR FCS_RND.1 represents a general support for cryptographic operations needed.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

175 The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication, of these data

exchanged.
This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM).
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used.
This objective for the data exchanged is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/AES. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and FCS_CKM.2/DH and possessing the special properties FIA_UAU.5, FIA_UAU.6. FDP_RIP.1 requires erasing the values of session keys (here: for K_{Enc}).
FMT_MTD.1/PA_UPD requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be modified by the Personalisation Agent only and, hence, is to consider as trustworthily.
The SFR FCS_RND.1 represents the general support for cryptographic operations needed.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

176 The security objective **OT.Tracing** aims that the TOE prevents 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 a priori knowledge of the correct values of shared passwords (CAN, MRZ).
This objective is achieved as follows:
(i) while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;
(ii) for listening to PACE communication (is of importance for the current PP, since SO_D is card-individual) – FTP_ITC.1/PACE.

177 The security objective **OT.Prot_Abuse_Func** aims preventing TOE's functions being not intended to be used in the operational phase from manipulating and disclosing the User- and TSF-data.
This objective is achieved by FMT_LIM.1 and FMT_LIM.2 preventing misuse of test and other functionality of the TOE having not to be used in the TOE's operational life phase.

178 The security objective **OT.Prot_Inf_Leak** aims protection against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE.
This objective is achieved
- by FPT_EMSEC.1 for 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 FPT_FLS.1 and FPT_TST.1 for forcing a malfunction of the TOE, and
- by FPT_PHP.3 for a physical manipulation of the TOE.

179 The security objective **OT.Prot_Phys-Tamper** aims protection of the confidentiality and integrity of the User- and TSF-data as well as embedded software stored in the TOE.
This objective is completely covered by FPT_PHP.3 in an obvious way.

180 The security objective **OT.Prot_Malfunction** aims ensuring a correct operation of the TOE by preventing its operation outside the normal operating conditions.
This objective is covered by FPT_TST.1 requiring self tests to demonstrate the correct operation of the TOE and tests of authorised users to verify the integrity of the TSF-data and the embedded software (TSF code) as well as by FPT_FLS.1 requiring entering a secure state of the TOE in case of detected failure or operating conditions possibly causing a malfunction.

6.3.2 Rationale for SFR's Dependencies

181 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.

182 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

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

184 The selection of the component ALC_DVS.2 provides a higher assurance of the security of the ePass's development and manufacturing, especially for the secure handling of sensitive material.

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

186 The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 4, entry 'Attacker'). This decision represents a part of the conscious security policy for the ePass required by the ePass Issuer and reflected by the current PP.

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

188 The augmentation of EAL4 chosen comprises the following assurance components:

– ALC_DVS.2,

– ATE_DPT.2 and

– AVA_VAN.5.

189 For these additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL4)		

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
ALC_DVS.2	no dependencies	-
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

Table 10: SAR Dependencies

6.3.4 Security Requirements – Internal Consistency

190 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.

191 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.

192 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 Glossary and Acronyms

Glossary

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the ePass's chip to produce Terminal Certificates with the correct certificate effective date, see [9], sec. 2.2.5.
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between an ePass and a terminal as required by [9], sec. G.3, 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 PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the ePass's chip to store the Initialisation Data and Pre-personalisation Data.
Authentication terminal (ATT)	A technical system being operated and used either by a governmental organisation (Official Domestic Document Verifier) or by any other, also commercial organisation and (i) verifying the ePass presenter as the ePass holder (using the secret eID-PIN[113]), (ii) updating a subset of data of the *eID* application and (iii) activating the eSign application. See also [9], chap. 3.2 and C.4. For the *eSign* application, it is equivalent to CGA.
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 [7] by which means the MRTD'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 MRTD's chip according to LDS.
Basic Inspection System with Basic Access Control protocol (BIS-BAC)	A technical system being used by an official organisation[114] 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 *Application note 2*, [9], chap. G.1 and H; also [7].

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

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

Term	Definition
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). The Basic Inspection System with PACE is a 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 in the context of [9] (and of the current PP) is similar, but not equivalent to the Basic Inspection System (BIS) as defined in [5]. See also [9], sec. 3.2.1, G.1 and G.2.
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 [9], sec. 3.3
Card Security Object (SO_C)	An RFC 3852 CMS Signed Data Structure signed by the Document Signer (DS). It is stored in the ID_Card (EF.CardSecurity, see [9], table A.1 and sec. A.1.2) and carries the hash values of different Data Groups as defined in [9], Appendix A. It shall also carry the Document Signer Certificate (C_{DS}), [9], A.1.2. Please note that [9] uses the same notation SO_C for Card and Chip Security Objects. Card and Chip Security Objects may differ with respect to the contained Chip Authentication Public Key (PK_{PICC}): If, for privacy reasons, multiple ID_Cards share the same Chip Authentication Public Keys (i.e. generation keys), the Card Security Object shall contain generation PK_{PICC} and Chip Security Object – chip-individual PK_{PICC}., cf. [9], sec. A.1.2.
Certificate chain	Hierarchical sequence of Terminal Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Certification Service Provider (CSP)	An organisation issuing certificates or providing other services related to electronic signatures. There can be 'common' CSP, who cannot issue qualified certificates and 'qualified' CSP, who can also issue qualified certificates.
Chip Security Object (SO_C)	An RFC 3852 CMS Signed Data Structure signed by the Document Signer (DS). It is stored in the ID_Card (EF.ChipSecurity, see [9], table A.1 and sec. A.1.2) and carries the hash values of different Data Groups as defined

Term	Definition
	in [9], Appendix A. It shall also carry the Document Signer Certificate (C_{DS}), [9], A.1.2. Please note that [9] uses the same notation SO_C for Card and Chip Security Objects. Card and Chip Security Objects may differ with respect to the contained Chip Authentication Public Key (PK_{PICC}): If, for privacy reasons, multiple ID_Cards share the same Chip Authentication Public Keys (i.e. generation keys), the Card Security Object shall contain generation PK_{PICC} and Chip Security Object – chip-individual PK_{PICC}., cf. [9], sec. A.1.2.
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means. [7]
Country Signing CertA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority and stored in the rightful terminals.
Country Signing Certification Authority (CSCA)	An 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 ePasss 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. [7], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [7]) 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 [9], sec. 2.2.1.
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the ePass Issuer with respect to protection of user data stored in the ePass (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [9], chap. 2.2.1. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organisational entity within this PP. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [7]) 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 [9], sec. 2.2.1.
Current date	The most recent certificate effective date contained in a valid CVCA Link Certificate, a DV Certificate or an Accurate Terminal Certificate known to the TOE, see [9], sec. 2.2.5.
CV Certificate	Card Verifiable Certificate according to [9], 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	according to the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on "*a Community framework for electronic signatures*" a digital signature qualifies as an electronic signature, if it is:

Term	Definition
	- uniquely linked to the signatory; - capable of identifying the signatory; - created using means that the signatory can maintain under his sole control, and - linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
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 [7]. 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 [9], H.1.
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 *ePassport* application (EF.SOD) of the ePass. It may carry the Document Signer Certificate (C_{DS}); see [7], sec. A.10.4.
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 (C_{DS}), see [9], chap. 1.1 and [7]. This role is usually delegated to a Personalisation Agent.
Document Verifier (DV)	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 Terminal Certificates. A Document Verifier is therefore a CertA, authorised by at least the national CVCA to issue certificates for national terminals, see [9], chap. 2.2.2. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this PP. 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). [115,116]
Eavesdropper	A threat agent reading the communication between the ePass and the Service Provider to gain the data on the ePass.

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

[116] 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
eID application	A part of the ID_Card containing the non-executable, related user data and the data needed for authentication; this application is intended to be used for accessing official and commercial services, which require access to the user data stored in the context of this application. See [9], sec. 3.1.2.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity; see [7].
ePass (electronic)	The contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.
ePass holder	A person for whom the ePass Issuer has personalised the 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 travel document (MRTD). See [9], sec. 3.1.1.
eSign application	A part of the ID_Card containing the non-executable data needed for generating advanced or qualified electronic (concretely: digital) signatures on behalf of the ID_Card holder as well as for authentication; this application is intended to be used in the context of official and commercial services, where an advanced or qualified digital signature of the ID_Card holder is required. The eSign application is optional: it means that it can optionally be activated[117] on the ID_Card by a Certification Service Provider (or on his behalf) using the ATT with an appropriate effective authorisation level. See [9], sec. 3.1.3.
Extended Access Control	Security mechanism identified in [7] by which means the MRTD'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 RP_Card presenter as the RP_Card holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the RP_Card presenter with the stored biometrical data (DG2 – DG4) of the RP_Card holder). EIS-AIP-BAC is a Basic Inspection System (BIS) in the sense of [5] additionally supporting/applying Chip Authentication (incl. passive authentication) and Terminal Authentication protocols in the context of AIP and is authorised by the RP_Card Issuer through the Document Verifier of receiving state to read a subset of data stored on the RP_Card.

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

Term	Definition
	EIS-AIP-BAC in the context of [9] is equivalent to the Extended Inspection System (EIS) as defined in [6].
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[118] (i.e. an Official Domestic or Foreign Document Verifier) and verifying the RP_Card presenter as the RP_Card holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the RP_Card presenter with the stored biometrical data (DG2 – DG4) of the RP_Card holder). EIS-AIP-PACE is a PCT additionally supporting/applying Chip Authentication (incl. passive authentication) and Terminal Authentication protocols in the context of AIP and is authorised by the RP_Card Issuer through the Document Verifier of receiving state to read a subset of data stored on the RP_Card. EIS-AIP-PACE in the context of [9] is similar, but not equivalent to the Extended Inspection System (EIS) as defined in [6].
Extended Inspection System using GAP (EIS-GAP)	A technical system being used by an official organisation[119] 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 of the ePass presenter with the stored biometrical data of the ePass holder). EIS-GAP is a PCT additionally supporting/applying Chip Authentication (incl. passive authentication) and Terminal Authentication protocols in the context of GAP and is authorised by the RP_Card Issuer through the Document Verifier of receiving state to read a subset of data stored on the RP_Card. The specification [9], sec. 3.2 differ between Basic and Extended Inspection Systems, whereby - the BIS can only perform Standard Inspection Procedure according to [9], sec. G.2 and - the EIS can perform (i) Advanced Inspection Procedure according to [9], sec. G.3 or (ii) General Authentication Procedure according to [9], sec. 3.1.1. All roles and authorisation levels as described in C.4 of [9] exclusively refer to EIS.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [7].
General Authentication Procedure	A specific order of authentication steps between an ePass and a terminal as required by [9], sec. 3.4, namely (i) PACE, (ii) Terminal Authentication (version 2), (iii) Passive Authentication with SO_C and (iv) Chip Authentication (version 2) (and an additional Passive Authentication with SO_D, see [9], sec. 3.1.1). GAP is used by EIS-GAP, ATT and SGT.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data

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

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

Term	Definition
	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 MRTDs; see [7].
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
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 [7].
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required; see [7].
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 [7].
Inspection system	see BIS-PACE for this PP. see also EIS-GAP, EIS-AIP-PACE, EIS-AIP-BAC and BIS-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 travel document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [7].
Issuing State	The country issuing the MRTD; see [7].
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [7]. The capacity expansion technology used is the MRTD's chip.
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 [7].
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing

Term	Definition
	mandatory and optional data for machine reading using OCR methods; see [7]. 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 travel document in a form that can be read and verified by machine; see [7].
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).
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 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 [9], sec. C.1.3. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date, - Certificate Extensions (optional).
PACE Terminal (PCT)	A technical system verifying correspondence between the password 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 (CAN or MRZ). See [9], chap. 3.3, 4.2, table 1.2 and G.2.
Passive authentication	Security mechanism implementing (i) verification of the digital signature of the Card/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 [9], sec. 1.1.
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 (PACE)	A communication establishment protocol defined in [9], sec. 4.2. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also

Term	Definition
	provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personal Identification Number (PIN)	A short secret password being only known to the ID_Card holder. PIN is a blocking password, see [9], sec. 3.3.
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 [9], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [7] (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*.
PIN Unblock Key (PUK)	A long secret password being only known to the ID_Card holder. The PUK is a non-blocking password, see [9], sec. 3.3.
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	ID_Card'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 [7].
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Remote terminal	A remote device directly communicating with the TOE and using the technical infrastructure between them (Internet, a local RF-terminal) merely as a message carrier. Only after Chip Authentication when a secure end-to-end connection between the TOE and remote terminal is established, the TOE grants access to the data of the *eID* application, see [9], sec. 3.4.1.
Restricted Identification	Restricted Identification aims providing a temporary ID_Card identifier being specific for a terminal sector (pseudo-anonymisation) and supporting revocation features (sec. 2.3, 4.1.2, 4.5 of [9]). The security status of ID_Card is not affected by Restricted Identification.

Term	Definition
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443
Rightful equipment (rightful terminal or rightful Card)	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 BIS-PACE (see *Inspection System*) or ATT or SGT. 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 [7].
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the ePass holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Signature terminal (SGT)	A technical system used for generation of digital signatures. See also par. 17 above and [9], chap. 3.2 and C.4. It is equivalent – as a general term – to SCA and HID.
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 and CAN data.
Standard Inspection Procedure	A specific order of authentication steps between an ePass and a terminal as required by [9], sec. G.2, 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 PCT ('Terminal' is used by the ePass presenter).
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the 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 ID_Card 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 [7].
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalised ePass	ePass material prepared to produce a personalised ePass containing an initialised and pre-personalised ePass'es chip.
User Data	All data (being not authentication data) stored in the context of the *ePassport* application of the ePass as defined in [9] and (ii) being allowed to be *read out* solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [9], sec. 3.2.1).

Term	Definition
	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, [9], sec. 3.1.1
ATT	Authentication Terminal as defined in [9], sec. 3.2
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [5])
BIS-PACE	Basic Inspection System with PACE (see [9], sec. 3.1.1, 3.2.1)
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')
CGA	Certificate generation application. In the current context, it is represented by ATT for the *eSign* application.
CHAT	Certificate Holder Authorization Template
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
EAC	Extended Access Control
EIS-AIP-BAC	Extended Inspection System with BAC (equivalent to EIS as used in [6])
EIS-AIP-PACE	Extended Inspection System with PACE (see [9], sec. 3.1.1, 3.2.1)
EIS-GAP	Extended Inspection System using GAP (see [9], sec. 3.1.1, 3.2.1)
GAP	General Authentication Procedure (see [9], sec. 3.4)
HID	Human Interface Device. It is equivalent to SGT in the context of ID_Card.
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PCT	PACE-authenticated terminal
PICC	Proximity Integrated Circuit Chip
PIN	Personal Identification Number
PP	Protection Profile
PUK	PIN Unblock Key
RAD	Reference Authentication Data
RF	Radio Frequency
SAR	Security assurance requirements
SCA	Signature creation application. It is equivalent to SGT in the context of ID_Card.
SCD	Signature Creation Data; the term 'private signature key within the *eSign* application' is synonym in the context of ID_Card.

Acronym	Term
SFR	Security functional requirement
SGT	Signature Terminal as defined in [9], sec. 3.2
SIP	Standard Inspection Procedure, see [9], sec. 3.1.1
SVD	Signature Verification Data
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)
VAD	Verification Authentication Data

8 Bibliography

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

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

Protection Profiles

[5] 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] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-2009, version 1.10, 25th March 2009

ICAO

[7] 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

[8] 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.

Technical Guidelines and Directives

[9] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI), TR-03110, version 2.03, 24.03.2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)[120]

[10] Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, version 1.00, 2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[11] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 1.11, 17.04.2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[120] please note that there may be an errata sheet published on www.bsi.bund.de (Publikationen -> Technische Richtlinien -> Technische Richtlinie Advanced Security Mechanisms for Machine Readable Travel Documents (BSI TR-03110).

Cryptography

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

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

[14] 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

Other Sources

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