Bundesamt
für Sicherheit in der
Informationstechnik

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
ANSSI

Common Criteria Protection Profile

Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)

Common Criteria

BSI-CC-PP-0068-V2-2011

Foreword

This Protection Profile ‘Electronic Passport using Standard Inspection procedure with PACE (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.

Throughout this document, the term PACE refers to PACE Version 2.

The ICAO Technical Report "Supplemental Access Control" [4] describes how to migrate from the current access control mechanism, Basic Access Control, to PACE, a new cryptographically strong access control mechanism that is initially provided supplementary to Basic Access Control:

"There is no straightforward way to strengthen Basic Access Control as its limitations are inherent to the design of the protocol based on symmetric (“secret key”) cryptography. A cryptographically strong access control mechanism must (additionally) use asymmetric (“public key”) cryptography.

This Technical Report specifies PACE as an access control mechanism that is supplemental to Basic Access Control. PACE MAY be implemented in addition to Basic Access Control, i.e.

States MUST NOT implement PACE without implementing Basic Access Control if global interoperability is required.

Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip.

Note: Basic Access Control will remain the “default” access control mechanism for globally interoperable machine readable travel documents as long as Basic Access Control provides sufficient security. Basic Access Control may however become deprecated in the future. In this case PACE v2 will become the default access control mechanism.

The inspection system SHALL use either BAC or PACE but not both in the same session."

Within the migration period, some developers will have to implement their products to functionally support both, PACE and Basic Access Control (BAC), i.e. Supplemental Access Control (SAC). 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.

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**

Content

1 PP Introduction

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

Title:	Protection Profile ‘Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)’
Editor/Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Supported by:	Agence nationale de la sécurité des systèmes d’information (ANSSI)
CC Version:	3.1 (Revision 3)
Assurance Level:	Minimum assurance level for this PP is EAL4 augmented.
General Status:	final
Version Number:	1.0 as of 2nd November 2011
Registration:	BSI-CC-PP-0068-V2-2011
Keywords:	ePassport, travel document, ICAO, PACE, Standard Inspection Procedure, Supplemental Access Control (SAC)

1.2 TOE Overview

1.2.1 TOE definition and operational usage

The Target of Evaluation (TOE) addressed by the current protection profile is an electronic travel document representing a contactless / contact smart card[1] programmed according to ICAO Technical Report "Supplemental Access Control" [4]. This smart card / passport provides the following application:

– the travel document containing the related user data[2] (incl. biometric if applicable) as well as data needed for authentication (incl. PACE passwords[3]); this application is intended to be used by governmental organisations, amongst other as a machine readable travel document (MRTD).

[1] may be also contained in a booklet

[2] according to [4]; see also chap. 7 below for definitions

[3] see Glossary chap. 7 below for definition

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

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

The TOE shall comprise at least

i) the circuitry of the contactless/contact chip incl. all IC dedicated software[5] being active in the operational phase of the TOE (the integrated circuit, IC),

ii) the IC Embedded Software (operating system)[6],

iii) the *ePassport* application and

iv) the associated guidance documentation.

1.2.2 TOE major security features for operational use

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

- Only terminals possessing authorisation information (a shared secret, the shared secret may be e.g. CAN or MRZ optically retrieved by the terminal) can get access to the user data stored on the TOE and use security functionality of the travel document under control of the travel document holder,
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the terminal connected[7],
- Averting of inconspicuous tracing of the travel document,
- Self-protection of the TOE security functionality and the data stored inside.

1.2.3 TOE type

The TOE type is contactless/contact smart card with the *ePassport* application named as a whole 'travel document'.

[4] CAN or MRZ user authentication, see [4]

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

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

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

The typical life cycle phases for the current TOE type are development[8], manufacturing[9], card issuing[10] 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 cycle 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 cycle phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 2.3 'Package Claim' below).

1.2.4 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [5], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

Phase 1 "Development"

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

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

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the ePassport application and the guidance documentation is securely delivered to the travel document manufacturer.

Phase 2 "Manufacturing"

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

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

[8] IC itself and IC embedded software

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

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

(Step4 optional) The travel document manufacturer combines the IC with hardware for the contact based/contactless interface in the travel document unless the travel document consists of the card only.

(Step5) The travel document manufacturer (i) adds the IC Embedded Software or part of it in the non-volatile programmable memories (for instance EEPROM or FLASH) if necessary, (ii) creates the ePassport application, and (iii) equips travel document's chips with pre-personalization Data.

Application note 1: Creation of the application implies:

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

The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation to the Personalisation Agent.

Phase 3 "Personalisation of the travel document"

(Step6) The personalisation of the travel document includes (i) the survey of the travel document holder's biographical data, (ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical part of the travel document, (iv) the writing of the TOE User Data and TSF Data into the logical travel document and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalisation Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object.

The signing of the Document security object by the Document signer [6] finalizes the personalisation of the genuine travel document for the travel document holder. The personalised travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

Application note 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [1] §92) comprise (but are not limited to) the Personalisation Agent Authentication Key(s).

Application note 3: This protection profile distinguishes between the Personalisation Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [6]. This approach allows but does not enforce the separation of these roles.

Phase 4 "Operational Use"

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

Application note 4: The intention of the PP is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

Note that the personalisation process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalisation and the related security objectives into aspects relevant before vs. after TOE delivery.

Some production steps, e.g. Step 4 in Phase 2 may also take place in the Phase 3.

1.2.5 Non-TOE hardware/software/firmware

In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless/contact based communication according to [7] and [8].

From the logical point of view, the TOE shall be able to recognise the following terminal type, which, hence, shall be available:
– *Basic Inspection System with PACE.*

The TOE shall require terminals to evince possessing authorisation information (a shared secret) before access according to [4], option 'PACE' is granted. To authenticate a terminal as a basic inspection system with PACE, Standard Inspection Procedure must be used.

In scope of this Protection Profile the following types of inspection systems shall be distinguished (for a more detailed description see Glossary):

- BIS-PACE: Basic Inspection System[11] with PACE[12],
- BIS-BAC: Basic Inspection System with BAC[13],

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[14], so that they also functionally support Basic Access Control (BAC). However, any product *using* BAC will not be conformant to the current PP; i.e. a product implementing the

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

[12] SIP with PACE means: PACE and passive authentication with SO_D

[13] SIP with BAC means: BAC and passive authentication with SO_D. It is commensurate with BIS in [9]; i.e. the terminal proven the possession of MRZ optically read out from the plastic part of the card.

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.

Application note 5: A terminal[15] shall always start a communication session using PACE. If successfully, it should then proceed with passive authentications.If the trial with PACE failed, the terminal may try to establish a communication session using other valid options as described above.

[14] so called non-compliant inspection systems not supporting PACE

[15] see [4] for further details

2 Conformance Claims

2.1 CC Conformance Claim

This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2007-09-001, Version 3.1, Revision 3, July 2009 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2007-09-002, Version 3.1, Revision 3, July 2009 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2007-09-003, Version 3.1, Revision 3, July 2009 [3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2007-09-004, Version 3.1, Revision 3, July 2009, [10]

has to be taken into account.

2.2 PP Claim

This PP does not claim conformance to any protection profile.

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'[9], 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 [9], the *ePassport* application of the TOE uses PACE as the mandatory communication establishment protocol.

2.3 Package Claim

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

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

2.5 Conformance statement

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

3 Security Problem Definition

3.1 Introduction

Assets

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
		travel document	
1	user data stored on the TOE	All data (being not authentication data) stored in the context of the *ePassport* application of the travel document as defined in [4] and being allowed to be *read out* solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [4]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [9].	Confidentiality[16] Integrity Authenticity
2	user data transferred between the TOE and the terminal 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 travel document as defined in [4] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [4]). User data can be received and sent (exchange ⇔ {receive, send}).	Confidentiality[17] Integrity Authenticity
3	travel document	Technical information about the	unavailability[18]

[16] Though not each data element stored on the TOE represents a secret, the specification [4] anyway requires securing their confidentiality: only terminals authenticated according to [4] can get access to the user data stored. They have to be operated according to P.Terminal.

[17] Though not each data element being transferred represents a secret, the specification [4] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [4].

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
	tracing data	current and previous locations of the travel document gathered unnoticeable by the travel document holder recognising the TOE not knowing any PAC E password. TOE tracing data can be provided / gathered.	

Table 1: Primary assets

Application Note 6: Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the travel document holder which also include his sensitive (i.e. biometric) data. Hence, the general security policy defined by the current PP also secures these specific travel document holder's data as stated in the table above.

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

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

Object No.	Asset	Definition	Property to be maintained by the current security policy
travel document			
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 [9].	Availability
6	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	TOE internal non-secret	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document	Integrity Authenticity

[18] represents a prerequisite for anonymity of the travel document holder

Object No.	Asset	Definition	Property to be maintained by the current security policy
	cryptographic material	Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality.	
8	travel document communication establishment authorisation data	Restricted-revealable[19] authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.	Confidentiality Integrity

Table 2: Secondary assets

Application Note 7: Since the travel document does not support any secret travel document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.

Application Note 8: travel document 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[20] – the verification information in the 'TOE ↔ terminal' channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be send to the TOE.

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

Subjects and external entities

This protection profile considers the following external entities and subjects:

External Entity No.	Subject No.	Role	Definition
1	1	travel document holder	A person for whom the travel document Issuer has personalised the travel document[21]. This entity is commensurate with 'MRTD Holder' in [9]. Please note that a travel document holder can also be an

[19] The travel document 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.

[20] the input device of the terminal

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

External Entity No.	Subject No.	Role	Definition
			attacker (s. below).
2	-	travel document presenter (traveller)	A person presenting the travel document to a terminal[22] and claiming the identity of the travel document holder. This external entity is commensurate with ‘Traveller’ in [9]. Please note that a travel document presenter can also be an attacker (s. below).
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role ‘Terminal’ is the default role for any terminal being recognised by the TOE as not being PACE authenticated (‘Terminal’ is used by the travel document presenter). This entity is commensurate with ‘Terminal’ in [9].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority[23] and verifying the travel document presenter as the travel document holder (for *ePassport*: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal’s part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. See also par. 1.2.5 above.
5	-	Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [6]. This role is usually delegated to a Personalisation Agent.
6	-	Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate

[22] in the sense of [4]

[23] concretely, by a control officer

External Entity No.	Subject No.	Role	Definition
			(C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [6], 5.5.1.
7	4	Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [6], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [6] (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 travel document Issuer. This entity is commensurate with 'Personalisation agent' in [9].
8	5	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase[24]. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [9].
9	-	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. 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 [9].

Table 3: Subjects and external entities[25]

[24] cf. also par. 1.2.3 in sec. 1.2.3 above

[25] 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

Application Note 9: Since the TOE does not use BAC, a Basic Inspection System with BAC (BIS-BAC) cannot be recognised by the TOE, see par. 1.2.5 above.

3.2 Threats

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

The following threats are defined in the current PP (they are initially derived from the ICAO-BAC PP [9] and ICAO-EAC PP [11]):

T.Skimming Skimming travel document / Capturing Card-Terminal Communication

Adverse action: An attacker imitates an inspection system in order to get access to the *user data stored on* or *transferred between the TOE and the inspecting authority connected* via the contactless/contact interface of the TOE.

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

Asset: confidentiality of logical travel document data

Application Note 10: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this PP.

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

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

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

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

Asset: confidentiality of logical travel document data

authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [1]). From this point of view, the TOE itself perceives only 'subjects' and, for them, does not differ between 'subjects' and 'external entities'. There is no 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 12: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this PP.

T.Tracing **Tracing travel document**

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

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

Asset: privacy of the travel document holder

Application Note 13: This Threat completely covers and extends "T.Chip-ID" from BAC PP [9].

Application Note 14: A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this PP, see also the par. 1.2.5 above.

Application Note 15: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document)[26] cannot be averted by the current TOE.

T.Forgery **Forgery of Data**

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

Threat agent: having high attack potential

Asset: integrity of the travel document

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

Adverse action: An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose 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

[26] Such a threat might be formulated like: 'An attacker produces an unauthorised copy or reproduction of a *genuine* travel document 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 travel document and copy them on another functionally appropriate chip to imitate this genuine travel document. This violates the authenticity of the travel document being used for authentication of an travel document presenter as the travel document holder'.

personalisation in the operational phase after delivery to the travel document holder.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document

Application Note 16: Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage Information Leakage from travel document

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

Threat agent: having high attack potential

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

Application Note 17: 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).

T.Phys-Tamper Physical Tampering

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

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

Application Note 18: Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g.

authentication key of the travel document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

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

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

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

Application note 19: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

3.3 Organisational Security Policies

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

P.Manufact **Manufacturing of the travel document's chip**

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

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

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

2.) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE[27].

3.) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 above.

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

P.Card_PKI PKI for Passive Authentication (issuing branch)

Application Note 20: 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 travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (C_{CSCA}) .

2.) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [6], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [6], 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 travel documents.

P.Trustworthy_PKI Trustworthiness of PKI

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

[27] cf. Table 1 and Table 2 above

P.Terminal Abilities and trustworthiness of terminals

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

1.) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [6].

2.) They shall implement the terminal parts of the PACE protocol [4], of the Passive Authentication [6] and use them in this order[28]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

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

4.) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [6]).

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

3.4 Assumptions

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

A.Passive_Auth PKI for Passive Authentication

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [6].

[28] This order is commensurate with [4].

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

OT.Data_Integrity Integrity of Data

The TOE must ensure integrity of the User Data and the TSF-data[29] 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 during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Data_Authenticity Authenticity of Data

The TOE must ensure authenticity of the User Data and the TSF-data[30] stored on it by enabling verification of their authenticity at the terminal-side[31].
The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) 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)[32].

OT.Data_Confidentiality Confidentiality of Data

The TOE must ensure confidentiality of the User Data and the TSF-data[33] by granting read access only to the PACE authenticated BIS-PACE connected.
The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Tracing Tracing travel document

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact

[29] where appropriate, see Table 2 above

[30] where appropriate, see Table 2 above

[31] verification of SO_D

[32] secure messaging after the PACE authentication, see also [4]

[33] where appropriate, see Table 2 above

interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

Application note 21: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity)[34] cannot be achieved by the current TOE.

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.

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 travel document

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

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.

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 travel document's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security functionality, as well as
- controlled manipulation of memory contents (User Data, TSF-data)

[34] Such a security objective might be formulated like: 'The TOE must enable the terminal connected to verify the authenticity of the travel document as a whole device as issued by the travel document Issuer (issuing PKI branch of the travel document Issuer) by means of the Passive and Chip Authentication as defined in [6]'.

with a prior

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

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.

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

OT.Identification Identification of the TOE

The TOE must provide means to store Initialisation[35] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

OT.AC_Pers Access Control for Personalisation of logical MRTD

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [6] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

Application note *23*: The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

4.2 Security Objectives for Operational Environment

Travel document Issuer as the general responsible

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

OE.Legislative_Compliance Issuing of the travel document

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

[35] amongst other, IC Identification data

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

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the Application Note 20 above):

OE.Passive_Auth_Sign Authentication of travel document by Signature

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (C_{CSCA}). 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 travel documents 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 [6]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [6]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

OE.Personalisation Personalisation of travel document

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enrol the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [6][36], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [6] (in the role of a DS).

Terminal operator: Terminal's receiving branch

OE.Terminal Terminal operating

The terminal operators must operate their terminals as follows:

1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [6].

2.) The related terminals implement the terminal parts of the PACE protocol [4], of the Passive Authentication [4] (by verification of the signature of the Document Security Object) and use them in this order[37]. The PACE terminal uses randomly and (almost)

[36] see also [6], sec. 10

[37] This order is commensurate with [4].

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 travel document (determination of the authenticity of data groups stored in the travel document, [6]).

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

Application note 24: OE.Terminal completely covers and extends “OE.Exam_MRTD”, “OE.Passive_Auth_Verif“ and “OE.Prot_Logical_MRTD” from BAC PP [9].

Travel document holder Obligations

OE.Travel_Document_Holder **Travel document holder Obligations**

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

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for *sufficiency* and *necessity* of the objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

	OT.Identification	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.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.Travel_Document_Holder	OE.Legislative_Compliance
T.Skimming			x	x	x									x	

	OT.Identification	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance
T.Eavesdropping					x										
T.Tracing						x								x	
T.Forgery		x	x	x			x		x		x	x	x		
T.Abuse-Func							x								
T.Information_Leakage								x							
T.Phys-Tamper									x						
T.Malfunction										x					
P.Manufact	x														
P.Pre-Operational	x	x									x				x
P.Terminal													x		
P.Card_PKI												x			
P.Trustworthy_PKI												x			
A.Passive_Auth												x			

Table 4: Security Objective Rationale

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

The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact 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.Travel_Document_Holder ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

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.

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

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 terminal. The security objective OT.AC_Pers requires the TOE to limit the write access for the travel document 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 terminal operator 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.

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.

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.

The OSP **P.Manufact** “Manufacturing of the travel document’s chip” requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalisation Data as being fulfilled by **OT.Identification**.

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.AC_Pers 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’.

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

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).

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

680 The Assumption **A.Passive_Auth** "PKI for Passive Authentication" is directly addressed by OE.Passive_Auth_Sign requiring the travel document issuer to establish a PKI for Passive Authentication, generating Document Signing private keys only for rightful organisations and requiring the Document Signer to sign exclusively correct Document Security Objects to be stored on travel document.

5 Extended Components Definition

This protection profile uses components defined as extensions to CC part 2. Most of them are drawn from [11].

5.1 Definition of the Family FAU_SAS

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.

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

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.

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 FMT_LIM

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.

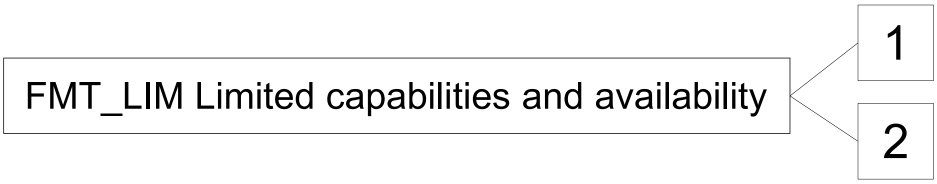
The family 'Limited capabilities and availability (FMT_LIM)' is specified as follows:

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*].

Application note 25: 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.

5.4 Definition of the Family FPT_EMS

The family FPT_EMS (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].

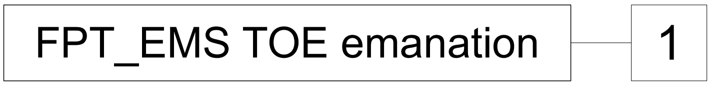
The family 'TOE Emanation (FPT_EMS)' is specified as follows:

FPT_EMS TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies

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

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

6 Security Requirements

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.

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.

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

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the 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*.

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*.

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

6.1 Security Functional Requirements for the TOE

6.1.1 Overview

In order to give an overview of the security functional requirements in the context of the security services offered by the TOE, the author of the 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

Security Functional Groups	Security Functional Requirements concerned
	(PACE authenticated BIS-PACE)
Secure data exchange between the travel document and the terminal connected	– FTP_ITC.1/PACE: trusted channel Supported by: – FCS_COP.1/PACE_ENC: encryption/decryption – FCS_COP.1/PACE_MAC: MAC generation/verification – FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE)
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (PACE authenticated BIS-PACE) – FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE) – FIA_UAU.4/PACE: single-use of authentication data – FIA_UAU.5/PACE: multiple authentication mechanisms – FIA_UAU.6/PACE: 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 (PACE authenticated BIS-PACE) – FCS_CKM.4: session keys destruction (authentication expiration) – FCS_RND.1: random numbers generation – FMT_SMR.1/PACE: security roles definition.
Audit	– FAU_SAS.1: Audit storage Supported by: – FMT_MTD.1/INI_ENA: Writing Initialisation and Pre-personalisation – FMT_MTD.1/INI_DIS: Disabling access to Initialisation and Pre-personalisation Data in the operational phase
Management of and access to TSF and TSF-data	– The entire class FMT. Supported by: – the entire class FIA: user identification /

Security Functional Groups	Security Functional Requirements concerned
	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 5: Security functional groups vs. SFRs

810 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 travel document 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}) to be distributed by strictly secure diplomatic means, see. [6], 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 travel document 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) or 3DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol, see [4].
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

Name	Data
ephem-PK_{PICC}-PACE)	PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 [12], cf. [4].

Table 6: Keys and Certificates

6.1.2 Class FCS Cryptographic Support

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

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.
fulfilled by FCS_CKM.2/DH.

Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

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

FCS_CKM.1.1/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 [12]*][38] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [4][39].

Application note 26: The TOE generates a shared secret value *K* with the terminal during the PACE protocol, see [4]. 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 [12] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [4] and [12] for details). The shared secret value *K* is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [4] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Application note 27: FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [4].

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

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

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*]

Application note 28: 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)

FCS_COP.1/PACE_ENC Cryptographic operation – Encryption / Decryption AES / 3DES

Hierarchical to: No other components.

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

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

FCS_COP.1.1/ PACE_ENC The TSF shall perform secure messaging – encryption and decryption [40] in accordance with a specified cryptographic algorithm[selection: *AES, 3DES*] in CBC mode [41] and cryptographic key sizes [selection: *112, 128, 192, 256*] bit [42] that meet the following: compliant to [4] [43].

Application note 29: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-KEnc).

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

[41] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1/PACE_MAC Cryptographic operation – MAC

Hierarchical to: No other components.

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

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

FCS_COP.1.1/PACE_MAC The TSF shall perform secure messaging – message authentication code [44] in accordance with a specified cryptographic algorithm [selection: *CMAC, Retail-MAC*] [45] and cryptographic key sizes [selection: *112, 128, 192, 256*] bit [46] that meet the following: compliant to [4] [47].

835 *Application note 30*: 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 [4] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

6.1.2.3 Random Number Generation (FCS_RND.1)

840 **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*].

Application note 31: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE.

6.1.3 Class FIA Identification and Authentication

For the sake of better readability, Table 7 provides an overview of the authentication mechanisms used:

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

[45] [assignment: *cryptographic algorithm*]

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

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

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

Table 7: Overview of authentication SFRs

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/PACE The TSF shall detect when *[assignment: positive integer number]*[48] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password[49].

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met[50], the TSF shall [assignment: *list of actions*].

Application Note 32: 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 (PACE passwords, see [4]) or for an arbitrary subset of them or may also separately be defined for each datum in question.

Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy[51], 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[52] 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 PACE passwords*'.

FIA_UID.1/PACE Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

[51] ≥ 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.

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

FIA_UID.1.1/PACE The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE Protocol according to [4]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[53]
4. [assignment: *list of TSF-mediated actions*].

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

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

Application note 33: User identified after a successfully performed PACE protocol is a PACE authenticated BIS-PACE. Please note that neither CAN nor MRZ effectively represent secrets (but other PACE passwords may do so), but are restricted-revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE).

FIA_UAU.1/PACE Timing of authentication

Hierarchical to: No other components.

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

FIA_UAU.1.1/PACE The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE Protocol according to [4][54]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,[55]
4. [assignment: *list of TSF-mediated actions*]

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

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

Application note 34: The user authenticated after a successfully performed PACE protocol is a PACE authenticated BIS-PACE. Please note that neither CAN nor MRZ effectively represent secrets (but other PACE passwords may do so), but are restricted-revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE).

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

[54] travel document identifies itself within the PACE protocol by selection of the authentication key ephem-PK_{PICC}-PACE

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

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. PACE Protocol according to [4]
2. Authentication Mechanism based on [selection: *Triple-DES, AES or other approved algorithms*][56].
3. [assignment: *identified authentication mechanism(s)*].

Application note 35: For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits length being (almost) uniformly distributed.

FIA_UAU.5/PACE Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE The TSF shall provide

1. PACE Protocol according to [4],
2. Passive Authentication according to [6]
3. Secure messaging in MAC-ENC mode according to [4]
4. Symmetric Authentication Mechanism based on [selection: *Triple-DES, AES or other approved algorithms*][57]
5. [assignment: *list of multiple authentication mechanisms*]

to support user authentication.

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

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalisation Agent by [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*].[58]
3. [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

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

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

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

Application note 36: Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of *ePassport* application.

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/PACE	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.[59]

Application note 37: The PACE protocol specified in [4] 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 or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

6.1.4 Class FDP User Data Protection

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/TRM	The TSF shall enforce the Access Control SFP[60] on terminals gaining access to the User Data stored in the travel document [61] and [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*] .

Application note 38: The assignment in FDP_ACC.1.1/TRM may be used in order to extend the subjects and objects needed for additional security functionalities as e.g by Extende Access Control. This can be done by the ST writer or in a PP claiming conformance to PACE PP.

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

Hierarchical to:	No other components.

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

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

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

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM

FMT_MSA.3 Static attribute initialisation: not fulfilled, but **justified**

The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalisation and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

FDP_ACF.1.1/TRM The TSF shall enforce the Access Control SFP[62] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. BIS-PACE;
2. Objects:
   a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 , EF.SOD and EF.COM of the logical travel document
   b. data in EF.DG3 of the logical travel document,
   c. data in EF.DG4 of the logical travel document ,
3. Security attributes:
   a. Authentication status of terminals[63]
4. [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*].

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

1. A BIS-PACE is allowed to read data objects from FDP_ACF.1/TRM according to [4] after a successful PACE authentication as required by FIA_UAU.1/PACE.[64]

FDP_ACF.1.3/TRM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[65].

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

[63] [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*]

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

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

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

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document
3. [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Application note 39: The assignment in FDP_ACF.1.1/TRM may be used in order to extend the subjects and objects and corresponding security attributes for documents with more types of security levels as e.g. some data groups additionally secured by Extended Access Control. The assignment in FDP_ACF.1.4/TRM may be used in order to deny access to DG3 and DG4 as it is recommended [6] or to further regulate the access to the objects of FDP_ACF.1.1/TRM. This can be done by the ST writer or in a PP claiming conformance to PACE PP.

Application note 40: Please note that the Document Security Object ($\mathrm{SO_D}$) stored in EF.SOD (see [6]) does not belong to the user data, but to the TSF-data. The Document Security Object can be read out by the PACE authenticated BIS-PACE, see [6].

Application note 41: Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects:

1. Session Keys (immediately after closing related communication session),
2. the ephemeral private key ephem-$\mathrm{SK_{PICC}}$-PACE (by having generated a DH shared secret *K*[66]),[67]
3. [assignment: *list of objects*].

Application note 42: 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

[66] according to [4]

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

similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD

Hierarchical to: No other components.

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

FDP_UCT.1.1/TRM The TSF shall enforce the Access Control SFP[68] to be able to transmit and receive[69] user data in a manner protected from unauthorised disclosure.

The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2).

FDP_UIT.1/TRM Data exchange integrity

Hierarchical to: No other components.

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

FDP_UIT.1.1/TRM The TSF shall enforce the Access Control SFP[70] to be able to transmit and receive[71] user data in a manner protected from modification, deletion, insertion and replay[72] errors.

FDP_UIT.1.2/TRM The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[73] has occurred.

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

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

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

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

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

6.1.5 Class FTP Trusted Path/Channels

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal. [74]

Application note 43: The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word "initiate" is changed to 'enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

Application note 44: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}): this secure messaging enforces preventing tracing while Passive Authentication and the required properties of *operational* trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.
The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

Application note 45: Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

6.1.6 Class FAU Security Audit

FAU_SAS.1 **Audit storage**

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

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

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

FAU_SAS.1.1 The TSF shall provide the Manufacturer[75] with the capability to store the Initialisation and Pre-Personalisation Data [76] in the audit records.

Application note 46: The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see
935 FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.1.7 Class FMT Security Management

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

FMT_SMF.1 **Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Initialization,
2. Pre-personalisation,
3. Personalisation
4. Configuration.[77]

940 **FMT_SMR.1/PACE** **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 47 below.

FMT_SMR.1.1/PACE The TSF shall maintain the roles

1. Manufacturer,
2. Personalisation Agent,
3. Terminal,

[75] [assignment: *authorised users*]

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

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

4. PACE authenticated BIS-PACE.[78]
5. [assignment: *the authorised identified roles*]

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

Application note 47: For explanation on the role Manufacturer and Personalisation Agent please refer to the glossary. The role Terminal is the default role for any terminal being recognised by the TOE as not PACE authenticated BIS-PACE ('Terminal' is used by the travel document presenter).

945 The TOE recognises the travel document holder or an authorised other person or device (BIS-PACE) by using PACE authenticated BIS-PACE (FIA_UAU.1/PACE).

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

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

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

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks.[79] and
5. [assignment: *Limited capability and availability policy*]

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

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

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,

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

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

3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks[80] and
5. [assignment: *Limited capability and availability policy*]

Application note 48:Note that the term “software” in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

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/PACE

FMT_MTD.1.1/ INI_ENA The TSF shall restrict the ability to write[81] the Initialisation Data and Pre-personalisation Data[82] to the Manufacturer.[83]

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ INI_DIS The TSF shall restrict the ability to read out[84] the Initialisation Data and the Pre-personalisation Data[85] to the Personalisation Agent.[86]

Application note 49: The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases ‘manufacturing’ and ‘issuing’, but being not needed and may be misused in the ‘operational use’. Therefore, read and use access to the

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

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

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

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

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

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

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

Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/ KEY_READ The TSF shall restrict the ability to read[87] the

1. PACE passwords,
2. Personalisation Agent Keys[88]
3. [assignment: *list of TSF data*]

to none[89].

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/PA The TSF shall restrict the ability to write[90] the Document Security Object (SO_D)[91] to the Personalisation Agent.[92]

Application note 50: By writing SO_D into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF- data.

6.1.8 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for the User Data and TSF-data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional

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

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

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

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

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

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

requirements 'Failure with preservation of secure state (FPT_FLS.1)' and 'TSF testing (FPT_TST.1)' on the one hand and 'Resistance to physical attack (FPT_PHP.3)' on the other. The SFRs 'Limited capabilities (FMT_LIM.1)', 'Limited availability (FMT_LIM.2)' and 'Resistance to physical attack (FPT_PHP.3)' together with the design measures to be described within the SAR 'Security architecture description' (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of the TOE security functionality.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),
2. the ephemeral private key ephem-SK_{PICC}-PACE,[93]
3. [assignment: *list of types of TSF data*]

and

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

FPT_EMS.1.2 The TSF shall ensure any users[94] are unable to use the following interface travel document's contactless/contact interface and circuit contacts[95] to gain access to

1. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),
2. the ephemeral private key ephem-SK_{PICC}-PACE,[96]
3. [assignment: *list of types of TSF data*]

and

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

Application note 51: 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 travel document's chip has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the

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

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

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

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

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

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

FPT_FLS.1 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,[97]
3. [assignment: *list of types of failures in the TSF*].

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[98].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[99].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[100].

Application note 52: If the travel document's 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 cycle 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

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

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

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

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

private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

FPT_PHP.3 Resistance to physical attack

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[101] to the TSF[102] by responding automatically such that the SFRs are always enforced.

Application note 53: 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

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

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

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

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

	OT.Identification	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
FCS_CKM.1/DH_PACE			x	x	x					
FCS_CKM.4			x	x	x					
FCS_COP.1/PACE_ENC					x					
FCS_COP.1/PACE_MAC			x	x						
FCS_RND.1			x	x	x					
FIA_AFL.1/PACE						x				
FIA_UID.1/PACE			x	x	x					
FIA_UAU.1/PACE			x	x	x					
FIA_UAU.4/PACE			x	x	x					
FIA_UAU.5/PACE			x	x	x					
FIA_UAU.6/PACE			x	x	x					
FDP_ACC.1/TRM			x		x					
FDP_ACF.1/TRM			x		x					
FDP_RIP.1			x	x	x					
FDP_UCT.1/TRM			x		x					
FDP_UIT.1/TRM			x		x					
FTP_ITC.1/PACE			x	x	x	x				
FAU_SAS.1	x	x								
FMT_MTD.1/KEY_READ		x	x	x	x					
FMT_SMF.1	x	x	x	x	x					
FMT_SMR.1/PACE	x	x	x	x	x					
FMT_LIM.1							x			
FMT_LIM.2							x			
FMT_MTD.1/INI_ENA	x	x								
FMT_MTD.1/INI_DIS	x	x								
FMT_MTD.1/PA		x	x	x	x					
FPT_EMS.1								x		
FPT_FLS.1								x		x
FPT_TST.1								x		x
FPT_PHP.3			x					x	x	

Table 8: Coverage of Security Objectives for the TOE by SFR

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

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 cycle phase ‘operational use’.

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.AC_Pers** 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 covers the related property of OT.AC_Pers (writing SO_D and, in generally, personalisation data).

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related. The SFR FMT_MTD.1./KEY_READ restricts the access to the Personalisation Agent Keys.

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/PACE, FIA_UAU.5/PACE 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 FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. 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 possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords.

FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy.

The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

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/PACE_MAC. 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 possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords.

FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy.

FIA_UAU.4/PACE, FIA_UAU.5/PACE 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/PACE support the functions and roles related.

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/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC. 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 possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. FDP_RIP.1 requires erasing the values of session keys (here: for K_{enc}). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords.

FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy .

The SFR FCS_RND.1 represents the general support for cryptographic operations needed.

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without a priori knowledge of the correct values of shared PACE passwords.

This objective is achieved as follows:

(i) while establishing PACE communication with a PACE password (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.

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 cycle phase.

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_EMS.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.

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.

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

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

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

6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the pre-defined assurance package EAL4. 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.

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

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.

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 3, entry ‘Attacker’). This decision represents a part of the conscious security policy for the travel document required by the travel document Issuer and reflected by the current PP.

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

The augmentation of EAL4 chosen comprises the following assurance components:

- ALC_DVS.2,
- ATE_DPT.2 and
- AVA_VAN.5.

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)		
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 9: SAR Dependencies

6.3.4 Security Requirements – Internal Consistency

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

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

The dependency analysis in section 6.3.2 ‘Rationale for SFR’s Dependencies’ for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

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

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

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met: an opportunity shown not to arise in sections 6.3.2 ‘Rationale for SFR’s Dependencies’ and 6.3.3 ‘Security Assurance Requirements Rationale’. Furthermore, as also discussed in section 6.3.3 ‘Security Assurance Requirements Rationale’, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

7 Glossary and Acronyms

Glossary

Term	Definition
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 travel document's chip to store the Initialisation Data and Pre-personalisation Data.
Authenticity	Ability to confirm that the travel document itself and the data elements stored in were issued by the travel document Issuer
Basic Access Control (BAC)	Security mechanism defined in [6] by which means the travel document's chip proves and the basic inspection system (with BAC) protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on travel document's chip according to LDS.
Basic Inspection System with Basic Access Control protocol (BIS-BAC)	A technical system being used by an official organisation[103] and operated by a governmental organisation 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 travel document using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (travel document document details data and biographical data) stored on the travel document. See also par. 1.2.5; also [6].
Basic Inspection System with PACE protocol (BIS-PACE)	A technical system being used by an inspecting authority[104] and verifying the travel document presenter as the travel document holder (for *ePassport*: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. A technical system being used by an inspecting authority 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

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

[104] concretely, by a control officer

Term	Definition
	data (DG2) of the ePass holder). The Basic Inspection System with PACE is a PCT additionally supporting/applying the Passive Authentication protocol.
Biographical data (biodata)	The personalised details of the travel document holder appearing as text in the visual and machine readable zones of and electronically stored in the travel document. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document 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 travel document and displayed by it using e.g. ePaper, OLED or similar technologies), see [4]
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means [6].
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 (CCSCA) having to be distributed by strictly secure diplomatic means, see. [6], 5.5.1.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KBENC) and message authentication (key KBMAC) of data transmitted between the TOE and an inspection system using BAC [6]. 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 [6].
Document Details Data	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SO_D)	A 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 travel document. It may carry the Document Signer Certificate (C_{DS}); see [6], 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.

Term	Definition
	A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS})(CDS), see [6]. This role is usually delegated to a Personalisation Agent.
Eavesdropper	A threat agent reading the communication between the travel document and the terminal to gain the data on the travel document.
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 [6].
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 [4].
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [6].
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all travel documents; see [6].
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life cycle phases.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person’s document; see [6].
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 [6].
Initialisation Data	Any data defined by the travel document 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 travel document material (IC identification data).
Inspection	The act of an official organisation (inspection authority) examining an

Term	Definition
	travel document presented to it by an travel document presenter and verifying its authenticity as the travel document holder. See also [6].
Inspection system	see BIS-PACE for this PP. see also BIS-BAC for general information
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements stored upon have not been altered from that created by the travel document Issuer.
Issuing Organisation	Organisation authorised to issue an official travel document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [6].
Issuing State	The country issuing the travel document; see [6].
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [6]. The capacity expansion technology used is the travel document's chip.
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods; see [6]. 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 [6].
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life-cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
PACE password	A password needed for PACE authentication, e.g. CAN or MRZ.
PACE Terminal (PCT)	A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ePass using a shared password (CAN or MRZ).
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 [6].
Passport (physical	An optically and electronically readable document in form of a

Term	Definition
and electronic)	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 [4]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document.
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [6], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [6] (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 travel document 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,) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life cycle phase *card issuing*.
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised travel document and/or to secure shipment within or between the life cycle phases *manufacturing* and *card issuing*.

Term	Definition
Pre-personalised travel document*'s chip*	travel document's chip equipped with a unique identifier and a unique Authentication Key Pair of the chip.
Receiving State	The Country to which the travel document holder is applying for entry; see [6].
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [7]
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*).
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [6].
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [8]
Skimming	Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact communication channel of the TOE without knowledge of the printed MRZ and CAN dataPACE password.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [4], namely (i) PACE and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
Supplemental Access Control	A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.
Terminal	A Terminal is any technical system communicating with the TOE through a contactless / contact interface.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document
Travel document	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 [6] (there "Machine readable travel document").
Travel document (electronic)	The contactless/contact smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.

Term	Definition
Travel document holder	A person for whom the ePass Issuer has personalised the travel document.
Travel document Issuer (issuing authority)	Organisation authorised to issue an electronic Passport to the travel document holder
Travel document presenter	A person presenting the travel document to a terminal and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalised travel document	travel document material prepared to produce a personalised travel document containing an initialised and pre-personalised travel document's chip.
User Data	All data (being not authentication data) (i) stored in the context of the *ePassport* application of the travel document as defined in [6]and (ii) being allowed to be *read out* solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [4]). 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.

1175 **Acronyms**

Acronym	Term
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [9])
BIS-PACE	Basic Inspection System with PACE
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
RF	Radio Frequency
SAC	Supplemental Access Control
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure, see [4]
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)

8 Bibliography

[1]: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2006-09-001, Version 3.1, Revision 3, July 2009

[2]: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2007-09-002, Version 3.1, Revision 3, July 2009

[3]: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2007-09-003, Version 3.1, Revision 3, July 2009

[4]: International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

[5]: Security IC Platform Protection Profile; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007, Version 1.0, June 2007

[6]: International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, Version Sixth Edition, 2006 (this includes the latest supplemental for ICAO Doc 9303 which also should be considered)

[7]: ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11

[8]: ISO/IEC 7816: Identification cards — Integrated circuit cards, Version Second Edition, 2008

[9]: 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

[10]: Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2007-09-004 , Version 3.1, Revision 3, July 2009

[11]: 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

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

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