Security Target

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

NOS e-Passport (BAC) v.1.01-I

Version 1.0

Universal Information Technologies LLC

BSI-DSZ-CC-0987

Foreword

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

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

Universal Information Technologies LLC, Kiev, Ukraine

Contents

List of Tables

1 ST Introduction

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

1.1 ST reference

Title:	Security Target ‘Machine Readable e-Document with „ICAO Application”, Basic Access Control based on National Operating System (NOS), NOS e-Passport (BAC) v.1.01-I’
Origin:	Universal Information Technologies LLC
CC Version:	3.1 (Revision 4)
Assurance Level:	EAL4-augmented with assurance component ALC_DVS.2
General Status:	Under review
Version Number:	1.0
Registration:	BSI-DSZ-CC-0987
Keywords:	ICAO, machine readable travel document, basic access control, ePassport, e-Document, SAC, National Operating System

1.2 TOE Reference

The TOE is Machine Readable e-Document with „ICAO Application”, Basic Access Control based on National Operating System (NOS), NOS e-Passport (BAC) v.1.01-I, running on the security microcontrollers listed in sec. 1.3 and hosting the ePassport application as required by [6].

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

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

that corresponds to ASCII notation:

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

where:

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

`b0.33` - embedded software build number;

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

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

1.3 TOE Overview

This Security Target defines the security objectives and requirements for the contactless chip of machine readable electronic documents (e-Document) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the 'ICAO Doc 9303' [9].

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

Explanatory note 1: In the current ST the term „Machine Readable Electronic Document" in the sense of Common Criteria is equal to „Machine Readable Travel Document" term, defined in PP [7] and 'ICAO Doc 9303' [9]. The term „Machine Readable Electronic Document" is used for the demonstration of the TOE application area extension and universalization in comparison with MRTD only.

The ePassport application is hosted on the National Operating System (NOS) running on the following certified [21] security microcontroller, compliant with to the Protection Profile BSI-PP-0035:

- Infineon Security Controller M7892 B11 (BSI-DSZ-CC-0782-V3-2017).

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

The current evaluation is a composite evaluation in the sense of CCDB-2012-04-001 [5].

The compatibility of Embedded Software and Hardware Platform according to ASE_COMP.1.1D,C of [5] is shown into corresponding "Statement of Compatibility" document.

1.3.1 TOE definition

The Target of Evaluation (TOE) is the contactless[1] integrated circuit chip of machine readable electronic documents (e-Document's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303' [9].

[1] These microcontrollers possess both contact based and contactless interfaces. For the ePassport application, only the contactless interface is used.

The TOE comprises:

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

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

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

(iv) the e-Document application and

(v) the associated guidance documentation.

1.3.2 TOE usage and security features for operational use

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

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

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

  (1) the biographical data on the biographical data page of the passport book,

  (2) the printed data in the Machine-Readable Zone (MRZ) and

  (3) the printed portrait.

(b) the **logical e-Document** as data of the e-Document holder stored according to the Logical Data Structure [9] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the e-Document holder

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

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

  (3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[2]

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

[2] These additional biometric reference data are optional.

(5) the Document security object.

The issuing State or Organization implements security features of the e-Document to maintain the authenticity and integrity of the e-Document and their data (see [11]). The e-Document as the passport book and the e-Document's chip is uniquely identified by the Document Number.

The physical e-Document is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the e-Document's chip) and organizational security measures (e.g. control of materials, personalization procedures) [9]. These security measures include the binding of the e-Document's chip to the passport book.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical e-Document, Active Authentication of the e-Document's chip, Extended Access Control and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [9]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This security target addresses the protection of the logical e-Document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism. This security target addresses the Active Authentication and the Extended Access Control as optional security mechanisms.

The TOE supports the Active Autentication procedure, defined in [9]. Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the e-Document's chip, the Active Autentication procedure is out of scope of the current ST.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the e-Document, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the e-Document's chip provides read access to the logical e-Document by means of private communication (secure messaging) with this inspection system [9], normative appendix 5.

1.3.3 TOE life-cycle

The TOE life cycle is described in terms of the three life cycle phases. With respect to the [8], the TOE 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 Embedded software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the ePassport application and the guidance documentation associated with these TOE components.

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

Explanatory Note 2: According to [21] the Personalisation Agent downloads the software into the SOLID FLASH™ flash memory of Infineon M7892 B11 chip.

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

Phase 2 "Manufacturing and Personalization of the e-Document"

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

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

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

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

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

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

Explanatory Note 3: Creation of the application implies:

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

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

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

The signing of the Document security object by the Document signer [9] finalizes the personalization of the genuine e-Document for the e-Document holder. The personalized e-Document (together with appropriate guidance for TOE use if necessary) is handed over to the e-Document holder for operational use.

Explanatory Note 4: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [1]) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Chip Authentication Private Key.

Explanatory Note 5: This security target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [9]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

Phase 3 "Operational Use"

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

Explanatory Note 6: The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the ePassport application (DG 17 and subsequent data groups) in the Phase 3 "Operational Use". Data groups DG 1 - DG 16 remain unchanged and the SOD is not overwritten.

Explanatory Note 7: The intention of the ST is to consider the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase 2. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. The national body of the issuing State or Organization is responsible for these specific production steps.

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

1.3.4 TOE type

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

1.3.5 Non-TOE hardware/software/firmware

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

In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless communication according to [19].

From the logical point of view, the TOE shall be able to distinguish between the following terminal type, which, hence, shall be available (see [13]):

– *Inspection System*[3]: an official terminal that is always operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier).

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

Explanatory note 8: The specification [13], sec. 2.4 knows the following types of inspection systems (i.e. for ePassport):
– BIS-PACE: Basic Inspection System[4] with PACE[5],
– BIS-BAC: Basic Inspection System with BAC[6],
– EIS-AIP-PACE: Extended Inspection System using Advanced Inspection Procedure with PACE[7],
– EIS-AIP-BAC: Extended Inspection System using Advanced Inspection Procedure with BAC[8],

The current ST - due to compliance with [6] - defines security policy for the usage of only BIS-BAC type of inspection systems.

The BIS-BAC inspection system allows to read all data groups excepting DG3 and DG4 from e-Document.

Using other types of inspection systems is out of the scope of the current ST. They may *functionally* be supported by the current e-Document product, but are not part of the TOE in the context of the current ST.

[3] see the *Explanatory note 8* below for further details

[4] a Basic Inspection Systems (BIS) always uses Standard Inspection Procedure (SIP).

[5] SIP with PACE means: PACE and passive authentication with SO_D according to [13], sec. 2.4.

[6] SIP with BAC means: BAC and passive authentication with SO_D according to [13]. It is commensurate with BIS in [6] and [7]; i.e. the terminal has proven the possession of MRZ optically read out from the physical carrier of the MRTD.

[7] Advanced Inspection Procedure (AIP) with PACE means: PACE, chip authentication (version 1), passive authentication with SO_D and terminal authentication (version 1) according to [13], sec. 2.4.

[8] AIP with BAC means: BAC, chip authentication (version 1), passive authentication with SO_D and terminal authentication (version 1) according to [13]. It is commensurate with EIS in [6] and [7]; please note that this EIS also covers the General Inspection Systems (GIS) in the sense of [6].

1.3.6 TOE Description

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

The logical scope of the TOE has already been described in sec. 1.3.2.

2 Conformance Claims

2.1 CC Conformance Claim

This security target claims conformance to

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

as follows

- Part 2 extended,
- Part 3 conformant.

The

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

has to be taken into account.

The current TOE is a composite product in the sense of [5]. The TOE platform (e-Documents chip and corresponding Infineon cryptographic libraries) was certified in accordance with Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4 (see CC report [21] for details).

The compatibility of Embedded Software and Hardware Platform according to ASE_COMP.1.1D,C of [5] is shown into corresponding "Statement of Compatibility" document.

2.2 PP Claim

This ST claims *strict* conformance to the ICAO-BAC PP [6].

Explanatory Note 9: The NOS implementation of Extended Access Control according to EAC-PP [7] is subject to a dedicated certification procedure.

2.3 Package Claim

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

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

2.4 Conformance Claim Rationale

The current ST claims *strict* conformance to the ICAO-BAC PP [6].

TOE Type

The PP [6] does not explicitly state any TOE type, but it can be inferred from the TOE definition in sec. 1.1 there: '... TOE ... is is the contactless integrated circuit chip of machine readable e-Document (e-Document's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303''.

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

SPD Statement

The security problem definition (SPD) of the current ST contains the security problem definition of the PP [6]. The current SPD includes the same threats, organisational security policies and assumptions as for the TOE in [6], see chap. 3 below.

Security Objectives Statement

The security objectives statement for the TOE in the current ST includes all the security objectives for the TOE of the PP [6], see chap. 4.1 below.

The security objectives statement for the TOE's operational environment in the current ST includes all security objectives for the operational environment of the PP [6], see chap. 4.2 below.

Security Requirements Statement

The PP [6] conforms to CC v3.1, revision 3, the current ST – to CC v3.1, revision 4. In respect to this, it is to rely on the statement of CCMB that respective assurance levels achieved by applying different CC revisions are equivalent to each other.

The SFR statement for the TOE in the current ST includes all the SFRs for the TOE of the PP [6], see chap. 6.1 below.

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

Explanatory note 10: Strict conformance allows that the security requirements for the TOE of the current ST may be hierarchically stronger than those items of each PP to which the conformance is being claimed.

3 Security Problem Definition

3.1 Introduction

3.1.1 Assets

The assets to be protected by the TOE include the User Data on the e-Document's chip.

Logical e-Document sensitive User Data

The logical e-Document data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [9]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the e-Document holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical e-Document.

Due to interoperability reasons as the 'ICAO Doc 9303' [9] the TOE described in this protection profile specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to:

- Logical e-Document standard User Data (i.e. Personal Data) of the e-Document holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data:

- Sensitive biometric reference data (EF.DG3, EF.DG4).

A sensitive asset is the following more general one.

Authenticity of the e-Document's chip The authenticity of the e-Document's chip personalized by the issuing State or Organization for the e-Document holder isused by the e-Document holder to prove his possession of a genuine e-Document.

3.1.2 Subjects

This Security Target considers the following subjects:

Manufacturer

Generic term for the IC Manufacturer producing integrated circuit and the e-Document Manufacturer completing the IC to the e-Document`s chip. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase[9]. The TOE itself does not distinguish between the IC Manufacturer and e-Document Manufacturer using this role Manufacturer.

This entity is commensurate with 'Manufacturer' in [6].

Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the e-Document for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the e-Document, (ii) enrolling the biometric reference data of the e-Document holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical e-Document for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [9].

Terminal

A terminal is any technical system communicating with the TOE through the contactless interface.

The role 'Terminal' is the default role for any terminal being recognised by the TOE as not PCT ('Terminal' is used by the ePass presenter).

This entity is commensurate with 'Terminal' in [6].

Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an e-Document presented by the e-Document presenter and verifying its authenticity and (ii) verifying the document`s presenter as e-Document holder. The **Basic Inspection System** (BIS) (i) contains a terminal for the contactless communication with the e-Document's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical e-Document under the Basic Access Control by optical reading the e-Document or other parts of the passport book providing this information. Optionally, the BIS may support Active Authentication. The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

Explanatory Note 11: This security target does not distinguish between the BIS, GIS and EIS because the Active Authentication and the Extended Access Control is outside the scope, see also sec. 1.3.5 above.

e-Document Holder

The rightful holder of the e-Document for whom the issuing State or Organization personalized the e-Document.

[9] cf. also sec. 1.3.3 above

This entity is commensurate with 'MRTD Holder' in [6].

Please note that an e-Document holder can also be an attacker (s. below).

e-Document Presenter

Person presenting the e-Document to the inspection system and claiming the identity of the e-Document holder.

This external entity is commensurate with 'Traveller' in [6].

Please note that an e-Document presenter can also be an attacker (s. below).

Attacker

A threat agent trying (i) to manipulate the logical e-Document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or (iii) to forge a genuine e-Document.

Please note that the attacker might 'capture' any subject role recognised by the TOE.

This external entity is commensurate with 'Attacker' in [6].

Explanatory Note 12: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged e-Document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

Document Signer (DS)

An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the e-Document for passive authentication.

A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [13] and [9].

This role is usually delegated to a *Personalisation Agent*.

Service Provider (SP)

An official organisation (inspection authority) providing inspection service which can be used by the ePass holder. Service Provider uses terminals (only BIS-BAC in the context of this ST) managed by a DV.

Document Verifier (DV)

An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Inspection System (Terminal) Certificates. A Document Verifier is therefore a CertA, authorised by at least the national CVCA to issue certificates for national terminals, see [13].

Please note that while using Standard Inspection Procedure, the TOE cannot recognise a DV as a subject, because the SIP does not imply any certificate-based terminal authentication; in this case DV merely represents an organisational entity within this ST.

There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the ePass Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement[10] between the ePass Issuer und a foreign CVCA ensuring enforcing the ePass Issuer's privacy policy[11]).

This external entity is commensurate with 'Document Verifier' in [6].

3.2 Assumptions

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

A.MRTD_Manufact **e-Document manufacturing on steps 4 to 6**

It is assumed that appropriate functionality testing of the e-Document is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the e-Document and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery **e-Document delivery during steps 4 to 6**

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent **Personalization of the e-Document's chip**

The Personalization Agent ensures the correctness of (i) the logical e-Document with respect to the e-Document holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the e-Document's chip, (iv) the Document Signer Public Key Certificate (if stored on the e-Document's chip), and (v) the Active Authentication Public Key (if stored on the e-Document's chip). The Personalization Agent signs the Document Security Object.

The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys **Inspection Systems for global interoperability**

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

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

The Inspection System is used by the border control officer of the receiving State (i) examining an e-Document presented by the e-Document presenter and verifying its authenticity and (ii) verifying the e-Document holder as e-Document holder. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [9]. The Basic Inspection System reads the logical e-Document under Basic Access Control and performs the Passive Authentication to verify the logical e-Document.

Explanatory Note 13: According to [9] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

A.BAC-Keys **Cryptographic quality of Basic Access Control Keys**

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [9], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

Explanatory Note 14: When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

3.3 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 TOE method of use in the operational environment and the assets stored in or protected by the TOE.

The TOE in collaboration with its IT environment shall avert the threats as specified below.

T. Chip_ID **Identification of e-Document's chip**

Adverse action: An attacker trying to trace the movement of the e-Document by identifying remotely the e-Document's chip by establishing or listening to communications through the contactless communication interface.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: Anonymity of user.

T. Skimming **Skimming the logical e-Document**

Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical e-Document or parts of it via the contactless communication channel of the TOE.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: confidentiality of logical e-Document data.

T.Eavesdropping Eeavesdropping to the communication between TOE and inspection system

Adverse action: An attacker is listening to an existing communication between the e-Document's chip and an inspection system to gain the logical e-Document or parts of it. The inspection system uses the MRZ data printed on the e-Document data page but the attacker does not know these data in advance.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: confidentiality of logical e-Document data.

T.Forgery Forgery of data on e-Document's chip

Adverse action: An attacker alters fraudulently the complete stored logical e-Document or any part of it including its security related data in order to deceive on an inspection system by means of the changed e-Document holder's identity or biometric reference data. This threat comprises several attack scenarios of e-Document forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the e-Document presenter. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical e-Documents to create a new forged e-Document, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical e-Document of a e-Document presenter into another e-Document's chip leaving their digital MRZ unchanged to claim the identity of the holder this e-Document. The attacker may also copy the complete unchanged logical e-Document to another contactless chip.

Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate e-Documents.

Asset: authenticity of logical e-Document data.

The TOE shall avert the threats as specified below.

T.Abuse-Func Abuse of Functionality

Adverse action: An attacker may use functions of the TOE which shall not be used in "Operational Use" phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to e-Document holder.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate e-Document.

Asset: confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF.

T.Information_Leakage Information Leakage from e-Document's chip

Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

Threat agent: having enhanced basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality of logical e-Document and TSF data.

T.Phys-Tamper Physical Tampering

Adverse action: An attacker may perform physical probing of the e-Document's chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the e-Document's chip Embedded Software. An attacker may physically modify the e-Document's chip in order to (i) modify security features or functions of the e-Document's chip, (ii) modify security functions of the e-Document's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the e-Document's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering

	requires direct interaction with the e-Document's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.
Threat agent:	having enhanced basic attack potential, being in possession of a legitimate e-Document
Asset:	confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF

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

Adverse action:	An attacker may cause a malfunction of TSF or of the e-Document's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the e-Document's chip Embedded Software. This may be achieved e.g. by operating the e-Document's chip outside the normal operating conditions, exploiting errors in the e-Document's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.
Threat agent:	having enhanced basic attack potential, being in possession of a legitimate e-Document.
Asset:	confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF.

3.4 Organisational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1 [1]).

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

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

P.Personalization **Personalization of the e-Document by issuing State or Organization only**

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

P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the e-Document's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) 4 and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the e-Document's chip are personal data of the e-Document holder. These data groups are intended to be used only with agreement of the e-Document holder by inspection systems to which the e-Document is presented. The e-Document's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [9].

Explanatory Note 15: The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [9]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

4 Security Objectives

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

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

OT.AC_Pers Access Control for Personalization of logical e-Document

The TOE must ensure that the logical e-Document data in EF.DG1 to EF.DG16, the Document security object according to LDS [9] and the TSF data can be written by authorized Personalization Agents only. The logical e-Document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

Explanatory Note 16: The OT.AC_Pers implies that

(1) the data of the LDS groups written during personalization for e-Document holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,

(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

OT.Data_Int Integrity of personal data

The TOE must ensure the integrity of the logical e-Document stored on the e-Document's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical e-Document data.

OT.Data_Conf Confidentiality of sensitive biometric reference data

The TOE must ensure the confidentiality of the logical e-Document data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical e-Document data during their transmission to the Basic Inspection System.

Explanatory Note 17: The e-Document presenter grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the Inspection System by presenting the e-Document. The e-Document's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. This Security Objective requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [9] that the Inspection System derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this Security Target, but that of BSI-DSZ-CC-0894. Thus the read access must be prevented even in case of a successful BAC Authentication.

OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the e-Document". The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s). In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

Explanatory Note 18: The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the e-Document". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or e-Document identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

The following TOE security objectives address the protection provided by the e-Document's chip independent of the TOE environment.

OT.Prot_Abuse-Func Protection against Abuse of Functionality

After delivery of the TOE to the e-Document Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate

critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.Prot_Inf_Leak Protection against Information Leakage

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the e-Document's chip

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

Explanatory Note 19: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper Protection against Physical Tampering

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the e-Document's chip Embedded Software. This includes protection against attacks with enhanced basic attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips 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 charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data) with a prior
- reverse-engineering to understand the design and its properties and functions.

OT.Prot_Malfunction Protection against Malfunctions

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Explanatory Note 20: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer

to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

4.2 Security Objectives for Operational Environment

Issuing State or Organization

The issuing State or Organization will implement the following security objectives of the TOE environment.

OE.MRTD_Manufact Protection of the e-Document Manufacturing

Appropriate functionality testing of the TOE shall be used in step 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.MRTD_ Delivery Protection of the e-Document delivery

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,

- identification of the element under delivery,

- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),

- physical protection to prevent external damage,

- secure storage and handling procedures (including rejected TOE's),

- traceability of TOE during delivery including the following parameters:

  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

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

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

OE.Personalization Personalization of logical e-Document

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the e-Document, (ii) enroll the biometric reference data of the e-Document holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the e-Document for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign Authentication of logical e-Document by Signature

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine e-Document in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [9].

OE.BAC-Keys Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [9] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

Receiving State or Organization

The receiving State or Organization will implement the following security objectives ofthe TOE environment.

OE.Exam_MRTD Examination of the e-Document passport book

The inspection system of the receiving State or Organization must examine the e-Document presented by the e-Document presenter to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical e-Document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [9].

OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the receiving State uses the inspection system to verify the e-Document presenter as e-Document holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical e-Document before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

OE.Prot_Logical_MRTD Protection of data from the logical e-Document

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical e-Document. The receiving State examining the logical e-Document being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				X									X			
T.Skimming			X										X			
T.Eavesdropping			X													
T.Forgery	X	X					X					X		X	X	
T.Abuse-Func					X						X					
T.Information_Leakage						X										
T.Phys-Tamper							X									
T.Malfunction								X								
P.Manufact				X												
P.Personalization	X			X							X					

P.Personal_Data		X	X												
A.MRTD_Manufact									X						
A.MRTD_Delivery										X					
A.Pers_Agent											X				
A.Insp_Sys													X		X
A.BAC-Keys												X			

Table 1: Security Objective Rationale

The OSP **P.Manufact** "Manufacturing of the e-Document's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre- personalization Data as being fulfilled by **OT.Identification**.

The OSP **P.Personalization** "Personalization of the e-Document by issuing State or Organization only" addresses the (i) the enrolment of the logical e-Document by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of logical e-Document", and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalization of logical e-Document". Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

The OSP **P.Personal_Data** "Personal data protection policy" requires the TOE (i) to support the protection of the confidentiality of the logical e-Document by means of the Basic Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives **OT.Data_Int** "Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT.Data_Conf** "Confidentiality of personal data" describes the protection of the confidentiality.

The threat **T. Chip_ID** "Identification of e-Document's chip" addresses the trace of the e-Document movement by identifying remotely the e-Document's chip through the contactless communication interface. This threat is countered as described by the security objective **OT.Identification** by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T. Skimming** "Skimming digital MRZ data or the digital portrait" and T.Eavesdropping "Eavesdropping to the communication between TOE and inspection system" address the reading of the logical e-Document trough the contactless interface or listening the communication between the e-Document's chip and a terminal. This threat is countered by the security objective **OT.Data_Conf** "Confidentiality of personal data" through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Forgery** "Forgery of data on e-Document's chip" addresses the fraudulent alteration of the complete stored logical e-Document or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical e-Document" requires the TOE to limit the write access for the logical e-Document to the trustworthy Personalization Agent (cf. **OE.Personalization**). The TOE will protect the integrity of the stored logical e-Document according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering".

The examination of the presented e-Document passport book according to **OE.Exam_MRTD** "Examination of the e-Document passport book" shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical e-Document. The TOE environment will detect partly forged logical e-Document data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** "Authentication of logical e-Document by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif** "Verification by Passive Authentication".

The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks using the e-Document's chip as production material for the e-Document and misuse of the functions for personalization in the operational state after delivery to e-Document holder to disclose or to manipulate the logical e-Document. This threat is countered by **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality". Additionally this objective is supported by the security objective for the TOE environment: **OE.Personalization** "Personalization of logical e-Document" ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to e-Document holder are enabled according to the intended use of the TOE.

The threats **T.Information_Leakage**" Information Leakage from e-Document's chip", T.Phys-Tamper "**Physical Tampering**" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak** "Protection against Information Leakage", **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot_Malfunction** "Protection against Malfunctions".

The assumption **A.MRTD_Manufact** "e-Document manufacturing on step 4 to 6" is covered by the security objective for the TOE environment **OE.MRTD_Manufact** "Protection of the e-Document Manufacturing" that requires to use security procedures during all manufacturing steps.

The assumption **A.MRTD_Delivery** "e-Document delivery during step 4 to 6" is covered by the security objective for the TOE environment **OE.MRTD_Delivery** "Protection of the e-Document delivery" that requires to use security procedures during delivery steps of the e-Document.

The assumption **A.Pers_Agent** "Personalization of the e-Document's chip" is covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical e-Document" including the enrolment, the protection with digital signature and the storage of the e-Document holder personal data.

The examination of the e-Document passport book addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the e-Document passport book". The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data from the logical e-Document" will require the Basic Inspection System to implement the Basic Access Control and to protect the logical e-Document data during the transmission and the internal handling.

The assumption **A.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" is directly covered by the security objective for the TOE environment **OE.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization.

5 Extended Components Definition

This ST includes all Extended Component Definitions from the ICAO-BAC PP [6] chap. 5, namely FAU_SAS.1, FCS_RND.1, FMT_LIM.1, FMT_LIM.2, FPT_EMSEC.1. These definitions are taken over as described in [7], therefore they are not repeated here.

6 Security Requirements

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

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

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

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

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the ST author are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment has to be made [assignment:], and are *italicised*.

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

6.1 Security Functional Requirements for the TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

6.1.1 Overview

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

Security Functional Groups	Security Functional Requirements concerned
Access control to User Data stored in the TOE	– {FDP_ACC.1, FDP_ACF.1}

Security Functional Groups	Security Functional Requirements concerned
	- FMT_MTD.1/KEY_READ - FMT_MTD.1/INI_DIS - FMT_MTD.1/KEY_WRITE - FMT_MTD.1/INI_ENA - FAU_SAS.1 Supported by: – FIA_UAU.1: Authentication - FMT_SMF.1 - FMT_SMR.1 - FCS_CKM.4
Secure data exchange between the ePass and the service provider (inspecting authority) connected	– FDP_UIT.1: data exchange integrity – FDP_UCT.1: data exchange confidentiality Supported by: – FCS_COP.1/ENC: encryption/decryption – FCS_COP.1/MAC: MAC generation / verification – FCS_CKM.1: Session keys generation – FIA_UAU.4, FIA_UAU.5: BAC Authentication
Identification and authentication of users and components	– FIA_UAU.4: single-use of authentication data (BAC and Personalisation Agent) – FIA_UAU.5: multiple authentication mechanisms (BAC and Personalisation Agent) – FIA_UAU.6: re-authentication of Terminal (BAC) – FIA_AFL.1: authentication failure handling (BAC) Supported by: – FIA_UID.1, FIA_UAU.1: life pases authentication – FCS_CKM.1: Generation of Document Basic Access Keys

Security Functional Groups	Security Functional Requirements concerned
	– FCS_CKM.4: Cryptographic keys destruction - FCS_COP.1/Auth: FIA_UAU.4 for Personalisation Agent - FCS_COP:1/SHA: for FIA_UAU.4 – FCS_RND.1: random numbers generation – FMT_SMR.1: security roles definition.
Management of and access to TSF and TSF-data	– The entire class FMT. Supported by: – the entire class FIA: user identification / authentication
Accuracy of the TOE security functionality / Self-protection	– The entire class FPT Supported by: – the entire class FMT.

Table 2: Security functional groups vs. SFRs.

Definition of security attributes: **security attribute**	**values**	**meaning**
terminal authentication status	none (a Terminal)	default role (i.e. non-authenticated terminal communicating with e-Document)
	BIS (BIS-BAC)	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2. SIP (Standard Inspection Procedure) with BAC means: BAC and passive authentication with SO_D according to [13]. It is commensurate with BIS in [6] and [7]; i.e. the terminal has proven the possession of MRZ optically read out from the physical carrier of the e-Document. A Basic Inspection Systems (BIS) always uses Standard Inspection Procedure (SIP). Since SIP does not comprise any Terminal Authentication as required Advanced Inspection Procedure (AIP), the TOE considered in the current ST cannot determine any role may be stored in the related

		terminal certificate like CVCA, DV and any therminal type using AIP. For this reason, any terminal authorisation, which may be achieved by a BIS, is not sufficient for reading DG3 and DG4, cf. [13].
	Personalisation Agent	Terminal is authenticated as Personalisation Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2, see also FCS_COP.1/AUTH.

Table 3: Summary of terminal authentication statuses

6.1.2 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer with the capability to store the **Initialisation Data (i.e.** IC Identification Data[12]**) and Pre-Personalisation Data** in the audit records.

Explanatory Note 21: The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the e-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 e-Document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.1.3 Class Cryptographic Support (FCS)

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

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

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

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [9], normative appendix 5.

Explanatory Note 22: The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [9], produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [9]. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2).

FCS_CKM.4 Cryptographic key destruction - MRTD

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion of key value[13] that meets the following: FIPS 140-2 [16][14].

Explanatory Note 23: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

6.1.3.1 Cryptographic operation (FCS_COP.1)

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA Cryptographic operation – Hash for key derivation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

[13] [assignment: *cryptographic key destruction method*]
[14] [assignment: *list of standards*]

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SHA The TSF shall perform hashing in accordance with a specified cryptographic algorithm SHA-1[15] and cryptographic key sizes none that meet the following: FIPS 180-2[16].

Explanatory Note 24: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive to derive the Basic Access Control Authentication Mechanism (see also FAU_UAU.4) according to [9].

FCS_COP.1/ENC Cryptographic operation – Symmetric Encryption / Decryption Triple DES

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ENC The TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC_mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [17] and [9]; normative appendix 5, A5.3.

Explanatory Note 25: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

FCS_COP.1/AUTH Cryptographic operation – Authentication

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

[15] [selection: *SHA-1 or other approved algorithms*]
[16] [selection: *FIPS 180-2 or other approved standards*]

FCS_COP.1.1/AUTH The TSF shall perform symmetric authentication – encryption and decryption in accordance with a specified cryptographic algorithm AES[17] and cryptographic key sizes 128[18] bit that meet the following: FIPS197 [15][19].

Explanatory Note 26: This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

FCS_COP.1/MAC Cryptographic operation – Retail MAC

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

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

Explanatory Note 27: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

6.1.3.2 Random Number Generation (FCS_RND.1)

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

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 i) Test procedure A, as defined in [18] does not distinguish the internal random numbers from output sequences of an ideal RNG, ii) The average Shannon entropy per internal random bit exceeds 0.997[20]

[17] [selection: *Triple-DES, AES*]
[18] [selection: *112, 128, 168, 192, 256*]
[19] [selection: *FIPS 46-3 [17], FIPS 197 [15]*]
[20] [assignment: *a defined quality metric*]

Explanatory Note 28: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

6.1.4 Class FIA Identification and Authentication

Explanatory Note 29: The Table 4 provides an overview of the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [9], normative appendix 5, and [12]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail- MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	AES with 128 bit keys (cf. FCS_COP.1/AUTH)

Table 4: Overview on authentication SFRs.

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2).

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 "Manufacturing",

2. to read random identifier in Phase 3 "Personalization of the ~~MRTD~~ **e-Document**",

3. to read the random identifier in Phase 4 "Operational Use"

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

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

Explanatory Note 30: The IC manufacturer and the e-Document manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the

Phase 2 "Manufacturing". The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The e-Document manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the e-Document". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

Explanatory Note 31: The In the "Operational Use" phase the e-Document must not allow anybody to read the ICCSN, the e-Document identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the e-Document's chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2).

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 "Manufacturing",

2. to read the random identifier in Phase 3 "Personalization of the ~~MRTD~~ **e-Document**",

3. to read the random identifier in Phase 4 "Operational Use"

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

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

Explanatory Note 32: The Basic Inspection System and the Personalization Agent authenticate themselves.

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4 Single-use authentication mechanisms – Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Basic Access Control Authentication Mechanism,

2. Authentication Mechanism based on AES[21]

Explanatory Note 33: The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. The authentication of a terminal as Personalization Agent uses the cryptographic primitives as required by FCS_COP.1/AUTH (AES), see also FIA_UAU.5.1 – rule 2.

Explanatory Note 34: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [9]. In the first step the terminal authenticates itself to the e-Document's chip and the e-Document's chip authenticates to the terminal in the second step. In this second step the e-Document's chip provides the terminal with a challenge-response-pair which allows a unique identification of the e-Document's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfil the security objective OT.Identification and to prevent T.Chip_ID.

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2).

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism,

2. Symmetric Authentication Mechanism based on AES[22]

to support user authentication.

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

1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s)

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

the Symmetric Authentication Mechanism with the Personalization Agent Key[23].

2. the TOE accepts the authentication attempt as Basic Inspection System only by means of Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

Explanatory Note 35: In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [7] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or other symmetric authentication mechanism based on the two-key Triple-DES. The Personalization Agent is authenticated by using the AES-based Symmetric Authentication Mechanism with the Personalization Agent Key, cf. [7] FIA_UAU.5.2.

Explanatory Note 36: The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

Explanatory Note 37: The Basic Access Control Mechanism specified in [9] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

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

Explanatory Note 38: Note that in case the TOE should also fulfil [7], the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process. The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1)" as specified below (Common Criteria Part 2).

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1)" as specified below (Common Criteria Part 2).

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1 The TSF shall detect when **at most** 15[24] unsuccessful authentication attempts occur related to BAC authentication[25].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[26], the TSF shall consecutively increase the reaction time of the TOE to the next authentication attempt[27].

Explanatory Note 39: These assignments are assigned to ensure especially the strength of authentication function as terminal part of the Basic Access Control Authentication Protocol to resist enhanced basic attack potential. The terminal challenge e_{IFD} and the TSF response e_{ICC} are described in [12], Appendix C. The refinement by inclusion of the word "consecutive" allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the "consecutive unsuccessful authentication attempts" are count independent on power-on sessions but reset to zero after successful authentication only.

6.1.5 Class FDP User Data Protection

6.1.5.1 Subset access control (FDP_ACC.1)

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2).

---

[24] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[25] [assignment: *list of authentication events*]
[26] [assignment: *met or surpassed*]
[27] [assignment*: list of actions*]

FDP_ACC.1 Subset access control – Basic Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical ~~MRTD~~ **e-Document**.

6.1.5.2 Security attribute based access control (FDP_ACF.1)

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2).

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the Basic Access Control SFP to objects based on the following:

1. Subjects:
   a. Personalisation Agent,
   b. Basic Inspection System **(BIS-BAC)**,
   c. Terminal,
2. Objects:
   a. data EF.DG1 to EF.DG16 of the logical ~~MRTD~~ **e-Document**,
   b. data in EF.COM,
   c. data in EF.SOD,
3. Security attributes:
   a. authentication status of terminals.

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

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical ~~MRTD~~ **e-Document**,
2. the successfully authenticated Basic Inspection System (BIS-BAC) is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical ~~MRTD~~ **e-Document**

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

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

1. Any terminal is not allowed to modify any of EF.DG1 to EF.DG16 of the logical ~~MRTD~~ **e-Document**.
2. Any terminal is not allowed to read any of EF.DG1 to EF.DG16 of the logical ~~MRTD~~ **e-Document**.
3. The Basic Inspection System **(BIS-BAC Terminal)** is not allowed to read the data in EF.DG3 and EF.DG4.

Explanatory Note 40: An inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this ST (cf. [7] for details).

6.1.5.3 Inter-TSF-Transfer

Explanatory Note 41: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

FDP_UCT.1 Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

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

FDP_UIT.1 Data exchange integrity - MRTD

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay[28] errors.

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

6.1.6 Class FMT Security Management

Explanatory Note 42: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements on the management of the TSF data.

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Initialization,
2. Pre-personalization,
3. Personalization.

The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2).

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles:

1. Manufacturer,
2. Personalization Agent,
3. Basic Inspection System **(BIS-BAC)**.

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

Explanatory Note 43: 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.

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

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

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

Deploying test features after TOE delivery do not allow

1. User Data to be disclosure or manipulated,

2. TSF data to be disclosed or manipulated,

3. software to be reconstructed and

4. substantial information about construction of TSF to be gathered which may enable other attacks

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

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

Deploying test features after TOE delivery do not allow

1. User Data to be disclosure or manipulated,

2. TSF data to be disclosed or manipulated,

3. software to be reconstructed and

4. substantial information about construction of TSF to be gathered which may enable other attacks.

Explanatory Note 44: The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term "software" in item 3 of

FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Explanatory Note 45: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data – Writing Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

Explanatory Note 46: The Pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization and Pre-personalization Data

Hierarchical to: No other components.

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

FMT_MTD.1.1 The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.

Explanatory Note 47: According to P.Manufact the IC Manufacturer and the e-Document Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE restricts the ability to write the Initialization Data and the Pre-personalization Data by blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer writes the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "Personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The e-Document Manufacturer will write the Pre-personalization Data.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none.

Explanatory Note 48: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

6.1.7 Class FPT Protection of the Security Functions

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

The TOE shall meet the requirement "TOE Emanation (FPT_EMSEC.1)" as specified below (Common Criteria Part 2 extended)

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1 The TOE shall not emit information about IC power consumption and command execution time[29] in excess of non useful information[30] enabling access to Personalization Agent Key(s) and logical e-Document data[31].

FPT_EMSEC.1.2 The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and logical e-Document data[32].

[29] [assignment: *types of emissions*]
[30] [assignment: *specified limits*]
[31] [assignment: *list of types of user data*]

Explanatory Note 49: 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 e-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 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.

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,

2. failure detected by TSF according to FPT_TST.1.

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the condition 'reset of the TOE'[33] to demonstrate the correct operation of the TSF.

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

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

[33] [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]*]

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

Explanatory Note 50: The e-Document's chip uses state of the art smart card technology and runs some self tests at the request of the authorized 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 is executed during initial start-up by the "authorized user" Manufacturer in the Phase 2 "Manufacturing". Other self tests are executed automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 "Operational Use", e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks.

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

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 to the TSF by responding automatically such that the SFRs are always enforced.

Explanatory Note 51: 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.

Explanatory Note 52: The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

6.2 Security Assurance Requirements for the TOE

The for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by the following components:

ALC_DVS.2.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					
FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_RND.1	x	x	x					
FIA_UID.1			x	x				
FIA_AFL.1			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4	x	x	x					
FIA_UAU.5	x	x	x					
FIA_UAU.6	x	x	x					
FDP_ACC.1	x	x	x					
FDP_ACF.1	x	x	x					
FDP_UCT.1	x	x	x					
FDP_UIT.1	x	x	x					
FMT_SMF.1	x	x	x					
FMT_SMR.1	x	x	x					
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA				x				
FMT_MTD.1/INI_DIS				x				
FMT_MTD.1/KEY_WRITE	x	x	x					
FMT_MTD.1/KEY_READ	x	x	x					
FPT_EMSEC.1	x				x			
FPT_TST.1					x		x	
FPT_FLS.1	x				x		x	
FPT_PHP.3	x				x	x		

Table 5: Coverage of Security Objectives for the TOE by SFR

The security objective **OT.AC_Pers** "Access Control for Personalization of logical e-Document" addresses the access control of the writing the logical e-Document. The write access to the logical e-Document data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical e-Document only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated (for reasons of interoperability with [7]) by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to protect the integrity of the logical e-Document stored on the e-Document's chip against physical manipulation and unauthorized writing. The write access to the logical e-Document data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical e-Document (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical e-Document (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5 using FCS_COP.1/AUTH.

The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical e-Document data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

The security objective **OT.Data_Conf** "Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical e-Document data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical e-Document data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical e-Document (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical e-Document (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR

FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1 for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

The security objective **OT.Identification** "Identification and Authentication of the TOE" address the storage of the IC Identification Data uniquely identifying the e-Document's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the e-Document's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application note 30). In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

The security objective **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality" is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

The security objective OT.Prot_Inf_Leak "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the e-Document's chip against disclosure

- 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 which is addressed by the SFR FPT_EMSEC.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

The security objective **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" is covered by the SFR FPT_PHP.3.

The security objective **OT.Prot_Malfunction** "Protection against Malfunctions" is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

6.3.2 Dependency Rationale

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 Table 6 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/ENC, and FCS_COP.1/MAC, Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	justification 1 for non-satisfied dependencies Fulfilled by FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1 Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	justification 2 for non-satisfied dependencies justification 2 for non-satisfied dependencies

	FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1 Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 3 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1

FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 6: Dependencies between the SFR for the TOE.

Justification for non-satisfied dependencies between the SFR for TOE:

No. 1: The hash algorithm required by the SFR FCS_COP.1.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

No. 2: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate nor to import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4.

No. 3: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

No. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the e-Document and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

6.3.3 Security Assurance Requirements Rationale

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

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the e-Document's development and manufacturing especially for the secure handling of e-Document's material.

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements

Dependencies ALC_DVS.2:

no dependencies.

6.3.4 Security Requirements – Mutual Support and 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 form a mutually supportive and internally consistent whole.

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

The dependency analysis in section 6.3.2 Dependency Rationale 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 analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and 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 mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.3.2 Dependency Rationale 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 the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specification

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

7.1 TSS_Access_Control

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

In the TOE *operational phase*, only terminals recognised by the TOE as Inspection Systems (BIS-BAC) are allowed to get reading access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM. The authentication as Basic Inspection systems is not sufficient in order to get reading access to EF.DG3 (fingerprint) and EF.DG4 (iris), see (FDP_ACC.1, FDP_ACF.1).

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

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

- to disable read access for users to the Initialization Data (FMT_MTD.1/INI_DIS),
- to write the Document Basic Access Keys (FMT_MTD.1/KEY_WRITE),
- to write the Document Security Object (EF.SOD) as well as the personalisation data (EF.DG1 to EF.DG16, EF.COM) of the logical e-Document after successful authentication (FDP_ACC.1, FDP_ACF.1).

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

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

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

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

In order to prevent access to temporarily stored secrets the TOE destroys the BAC session keys (i) after detection of an error in a received command by verification of the MAC; (ii) The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session (FCS_CKM.4).

7.2 TSS_Trusted_Channel

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

Basic Inspection Procedure

As a result of a successful BAC authentication, the TOE and the Basic Inspection System (BIS-BAC) establish a trusted channel maintaining confidentiality and integrity of all the data exchanged between them (FDP_UIT.1, FDP_UCT.1). The cryptographic properties of this trusted channel are defined in FCS_COP.1/ENC, FCS_COP.1/MAC. The related session keys generation is modelled by FCS_CKM.1.

7.3 TSS_Authentication

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

Authentication Mechanism for Personalisation Agents

The Personalisation Agent authenticates himself to the TOE by using a symmetric challenge-response mechanism. This mechanism uses Personalisation Agent Key shared between the TOE and the Personalisation Agent (FIA_UAU.4, FCS_COP.1/Auth, FIA_UAU.5).

Authentication Mechanism for BAC

The Basic Access System and the e-Document mutually authenticate by means of a Basic Access Control mechanism based on challenge-response protocol (FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5).

In the case of unsuccessful authentication, the TSF consecutively increases the reaction time of the TOE to the next authentication attempt (FIA_AFL.1).

After successful authentication of the terminal with Basic Access Control Authentication Mechanism the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user (FIA_UAU.6).

The challenge is the random number sent from one party to the other (FCS_RND.1). This random number will be enciphered with the secret symmetric key by the receiver and then will be verified by the sender. This security service manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way. These authentication keys are derived by the SHA-1 algorithm (FCS_COP.1/SHA). The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session (FCS_CKM.4).

7.4 TSS_Self-Protection

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

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

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

The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions (FPT_EMSEC.1).

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

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

8 Glossary and Acronyms

Glossary

Term	Definition
Active Authentication	Security mechanism defined in [9] option by which means the e-Document's chip proves and the inspection system verifies the identity and authenticity of the e-Document's chip as part of a genuine e-Document issued by a known State of Organization
Agreement	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Application note	Optional informative part of a PP / ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the ePass's chip to store the Initialisation Data and Pre-personalisation Data.
Authenticity	Ability to confirm that the ePass itself and the data elements stored in were issued by the ePass Issuer
Basic Access Control (BAC)	Security mechanism defined in [9] by which means the e-Document's chip proves and the basic inspection system (with BAC) protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on e-Document's chip according to LDS.
Basic Inspection System with Basic Access Control protocol (BIS-BAC)	A technical system being used by an official organisation[34] and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying correspondence between the stored and printed MRZ. BIS-BAC implements the terminal's part of the Basic Access Control protocol and authenticates itself to the ePass using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (ePass document details data and biographical data) stored on the ePass. See also *Explanatory note 8*, [13]; also [9].
Basic Inspection System with PACE protocol (BIS-PACE)	See [13].
Biographical data	The personalised details of the ePass holder appearing as text in the visual

[34] an inspecting authority

Term	Definition
(biodata)	and machine readable zones of and electronically stored in the ePass. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the ePass holder in the ePass as (i) digital portrait and (ii) optional biometric reference data (e.g. finger and iris).
Card Access Number (CAN)	A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Passport), semi-static (e.g. printed on a label on the Passport) or dynamic (randomly chosen by the electronic ePass and displayed by it using e.g. ePaper, OLED or similar technologies), see [13].
Certificate chain	Hierarchical sequence of Inspection System (Terminal) Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means. [9]
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.
Current date	The most recent certificate effective date contained in a valid CVCA Link Certificate, a DV Certificate or an Accurate Inspection System (Terminal) Certificate known to the TOE, see [13].
CV Certificate	Card Verifiable Certificate according to [13], appendix C.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient; see [20].
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KB_{ENC}) and message authentication (key KB_{MAC}) of data transmitted between the TOE and an inspection system using BAC [9]. 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 [13].
Document Details Data	Data printed on and electronically stored in the ePass representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are

Term	Definition
	less-sensitive data.
Document Security Object (SO_D)	A RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups: A hash for each Data Group in use shall be stored in the Security Data. It is stored in the *ePassport* application (EF.SOD) of the ePass. It may carry the Document Signer Certificate (C_{DS}); see [9].
Eavesdropper	A threat agent reading the communication between the ePass and the Service Provider to gain the data on the ePass.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity; see [9].
ePass (electronic)	The contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*.
ePass Issuer (issuing authority)	Organisation authorised to issue an electronic Passport to the ePass holder
Extended Access Control	Security mechanism identified in [9] by which means the e-Document's chip (i) verifies the authentication of the inspection systems authorised to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.
Extended Inspection System using AIP with BAC (EIS-AIP-BAC)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the RP_Card presenter as the RP_Card holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the RP_Card presenter with the stored biometrical data (DG2 – DG4) of the RP_Card holder). EIS-AIP-BAC is a Basic Inspection System (BIS) in the sense of [6] additionally supporting/applying Chip Authentication (incl. passive authentication) and Terminal Authentication protocols in the context of AIP and is authorised by the RP_Card Issuer through the Document Verifier of receiving state to read a subset of data stored on the RP_Card. EIS-AIP-BAC in the context of [13] is equivalent to the Extended Inspection System (EIS) as defined in [7].
Extended Inspection System using AIP with PACE (EIS-	A technical system being used by an inspecting authority and operated by a governmental organisation[35] (i.e. an Official Domestic or Foreign Document Verifier) and verifying the RP_Card presenter as the RP_Card

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

Term	Definition
AIP-PACE)	holder (for *ePassport*: by comparing the real biometrical data (face, fingerprint or iris) of the RP_Card presenter with the stored biometrical data (DG2 – DG4) of the RP_Card holder). EIS-AIP-PACE is a PCT additionally supporting/applying Chip Authentication (incl. passive authentication) and Terminal Authentication protocols in the context of AIP and is authorised by the RP_Card Issuer through the Document Verifier of receiving state to read a subset of data stored on the RP_Card. EIS-AIP-PACE in the context of [13] is similar, but not equivalent to the Extended Inspection System (EIS) as defined in [7].
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [9].
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all e-Documents; see [9].
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 [9].
Improperly documented person	(in the MRTD notation) 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 [9].
Initialisation Data	Any data defined by the ePass manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as ePass material (IC identification data).
Inspection	The act of an official organisation (inspection authority) examining an ePass presented to it by an ePass presenter and verifying its authenticity as the ePass holder. See also [9].

Term	Definition
Inspection system	see BIS-PACE and EIS-AIP-PACE for the current ST. see also BIS-BAC and EIS-AIP-BAC for general information
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The ePass's chip is an integrated circuit.
Integrity	Ability to confirm the ePass and its data elements stored upon have not been altered from that created by the ePass Issuer.
Issuing Organisation	Organisation authorised to issue an official e-Document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [9].
Issuing State	The country issuing the e-Document; see [9].
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [9]. The capacity expansion technology used is the e-Document's chip.
Machine readable electronic Document (e-Document)	(in the context of the current ST) Official document issued by a state or organisation which is used by the holder for different applications (international travel, e.g. passport, visa, official document of identity, passport of a citizen etc.) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [9]. In the current ST the term „Machine Readable Electronic Document" in the sense of Common Criteria is equal to „Machine Readable Travel Document" term, defined in PP [7] and 'ICAO Doc 9303' [9].
Machine readable travel document (MRTD)	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [9].
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the e-Document or MRP Data Page or, in the case of the TD1, the back of the e-Document, containing mandatory and optional data for machine reading using OCR methods; see [9]. The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for both PACE and BAC.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a e-Document in a form that can be read and verified by machine; see [9].
Malicious equipment	A technical device being expected, but not possessing a valid, certified key pair for its authentication (if required); validity of its certificate is not

Term	Definition
	verifiable up to the respective root CertA (CVCA for a terminal and CSCA for an ID_Card).
Manufacturer	See sec. 3.1.2.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [14]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date, - Certificate Extensions (optional).
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable electronic document (e-Document). See [13].
PACE password	A password needed for PACE authentication, e.g. CAN or MRZ. Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [10].
PACE Terminal (PCT)	See [13]
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 [13].
Passport (physical and electronic)	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Passport is used in order to verify that identity claimed by the Passport presenter is commensurate with the identity of the Passport holder stored on/in the card.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [13]. 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.

Term	Definition
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the ePass.
Personalisation Agent	See sec. 3.1.2.
Personalisation Data	A set of data incl. (i) individual-related data (biographic and biometric data, signature key pair(s) for the eSign application, if installed) of the ePass holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life cycle phase *card issuing*.
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised ePass and/or to secure shipment within or between the life cycle phases *manufacturing* and *card issuing*.
Pre-personalised ePass's chip	e-Document's chip equipped with a unique identifier and a unique asymmetric Authentication Key Pair of the chip.
Receiving State	The Country to which the ePass holder is applying for entry; see [9].
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443
Rightful equipment (rightful terminal or rightful proximity 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 or EIS-AIP-PACE (see *Inspection System*). A terminal as well as a Card can represent the rightful equipment, whereby the root CertA for a terminal is CVCA and for a Card – CSCA.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [9].
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
sensitive (biometrical) data also called *logical e-Document sensitive User Data*	the content of the DG3 and DG4 acc. to [13].

Term	Definition
Service Provider	See sec. 3.1.2.
Skimming	Imitation of a rightful terminal to read the ePass or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ and CAN data.
Standard Inspection Procedure	A specific order of authentication steps between an ePass and a terminal as required by [13], namely (i) PACE and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
Terminal	Any technical system communicating with the TOE through the contactless interface. See sec. 3.1.2.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Inspection System (Terminal) Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date. It can additionally be restricted at terminal by ePass holder using CHAT.
TOE tracing data	Technical information about the current and previous locations of the ePass gathered by inconspicuous (for the ePass holder) recognising the ePass
Travel document	A passport or other official document of identity issued by a state or organisation which may be used by the rightful holder for international travel; see [9].
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalised ePass	ePass material prepared to produce a personalised ePass containing an initialised and pre-personalised ePass'es chip.
User Data	CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [2]).
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
AIP	Advanced Inspection Procedure, [13]
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [6])
BIS-PACE	Basic Inspection System with PACE (see [13])
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority (the author dispensed with the usual abbreviation 'CA' in order to avoid a collision with 'Chip Authentication')
CHAT	Certificate Holder Authorization Template
EAC	Extended Access Control
EIS-AIP-BAC	Extended Inspection System with BAC (equivalent to EIS as used in [7])
EIS-AIP-PACE	Extended Inspection System with PACE (see [13])
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PCT	PACE-authenticated terminal
ICC	Proximity Integrated Circuit Chip
PP	Protection Profile
RAD	Reference Authentication Data
RF	Radio Frequency
SAR	Security assurance requirements
SFR	Security functional requirement

Acronym	Term
SIP	Standard Inspection Procedure, see [13]
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)
TSS	TOE Security Service
VAD	Verification Authentication Data

9 Bibliography

Common Criteria

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

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

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

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

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

Protection Profiles

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

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

[8] Common Criteria Protection Profile Security IC Platform Protection Profile with Augmentation Packages Version 1.0, BSI-CC-PP-0084-2014

ICAO

[9] ICAO Doc 9303-1, Specifications for electronically enabled passports with biometric identification capabilities. In *Machine Readable Travel Documents – Part 1: Machine Readable Passport*, volume 2, ICAO, 6th edition, 2006

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

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

Technical Guidelines and Directives

[12] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), TR-03110, version 1.11, 21.02.2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[13] TR-03110-1, version 2.10, Technical Guideline: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

Cryptography

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

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

[17] FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), National Institute of Standards and Technology, Reaffirmed October 1999

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

Other Sources

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

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

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