Federal Office
for Information Security

Common Criteria Protection Profile
for
Inspection Systems (IS)

Common Criteria

BSI-CC-PP-0064

Version 1.01 (15th April 2010)

Federal Office for Information Security
Postfach 20 03 63
53133 Bonn
Phone: +49 228 99 9582-0
e-Mail: zertifizierung@bsi.bund.de
internet: http://www.bsi.bund.de

Table of Content

List of Figures

List of Tables

1. PP-Introduction

1.1. PP reference

1	Title:	Protection Profile — Inspection Systems (IS)
	Sponsor:	Federal Office for Information Security
	CC Version:	3.1 (Revision 3)
	Assurance Level:	The minimum assurance level for this PP is EAL3
	General Status:	Final
	Version Number:	1.01
	Registration:	BSI-CC-PP-0064
	Keywords:	ICAO, inspection system, machine readable travel document, extended access control

1.2. TOE overview

2 The Target of Evaluation (TOE) addressed by this Protection Profile (PP) is an application, and its interfaces, which defines the main item of an Inspection System (IS). The TOE is used to read, and where applicable update, the electronic data of an electronic identity document[1] and verify its integrity and authenticity. In the following this application is called "document application".

3 Therefore in order to get access to the chip data the TOE must be able to perform several cryptographic operations. An overview of protocols which may be used is given in section 1.2.4.

4 The inspection systems regarded in this PP are operated by government or enforcement organisations e.g. police or government or other state approved agencies.

5 Inspection Systems can have different configurations. The TOE is the main item of an Inspection System, but there are several additional components necessary to get a fully functional IS. For this reason a description of the required and optional non-TOE hardware/software is given in section 1.2.2 before usage and major security features are described in section 1.2.3.

6 A general overview of the TOE and its related components is given in Figure 1 in the following section.

1 In most cases this will be an eMRTD (electronic Machine Readable Travel Document) compliant to [ICAO Doc9303], but can also be some other kind of official electronic identity document which supports the protocols needed to prove authenticity and integrity of the document. *Please note:* The eMRTD is abbreviated further in this PP as MRTD.

1.2.1 General overview of the TOE and the related components

7 The following figure shows the components necessary for an IS as regarded in this PP. The document application shall be the Target of Evaluation (TOE) and is therefore marked green. The connections of the document application (e.g. to the logfile, key and certificate/CRL storages, Input/Output interfaces) are also subject of the evaluation since they constitute the external interfaces of the TOE.

8 The operating system as base of the document application, the input and output devices, the key and certificate/CRL storages, the logfile storage and the PCD (Proximity Coupling Device, see also chap. 1.2.2) are marked orange as being not part of the TOE but necessary for the functionality of the IS.

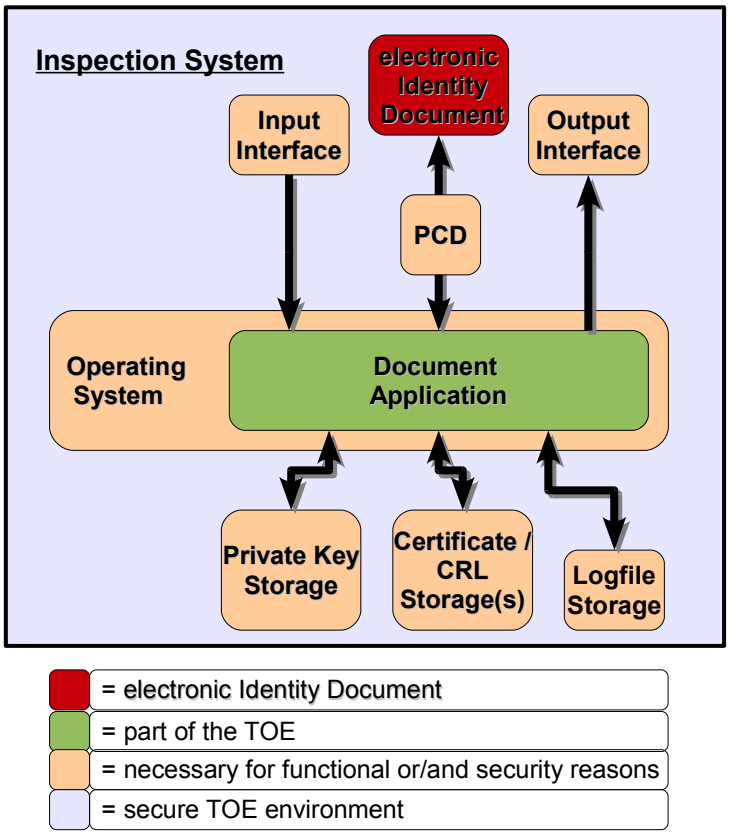


Figure 1: general overview of the TOE and the related components

1.2.2 Required non-TOE hardware/software

9 In order to read out the personal data from the chip and to verify its authenticity and integrity the following components are necessary additionally to the document application:

1. The document application is running on an o**perating system**.

2. The **PCD (Proximity Coupling Device)** is featured with a RF (Radio Frequency) reading module and an antenna. It is used for the wireless communication with the electronic identity document chip in order to establish a connection based on the [ISO/IEC14443] and [ISO/IEC7816] protocols.

3. Most types of electronic identity documents demand some kind of password to get basic access to the electronic identity document's chip. Therefore an II **(Input Interface)** is necessary. It is conditional which type of II device should be used. In case of an ICAO compliant eMRTD this "password" is one part of the MRZ (Machine Readable Zone) and it can be read with an OCR-Reader (Optical Character Recognition). With consideration of the electronic identity documents where the password is not meant to be read optically or cases in which the MRZ, etc. is difficult to be read due to a damaged or polluted document, an II device should be usable to type in a password. Furthermore a kind of keyboard etc. is needed when personal chip data (e.g. the address) shall be updated. The II device may provide also capturing features for biometric attributes like fingerprint or images of the MRTD holder's face. Advanced matching mechanisms between the biometric information captured from the MRTD holders and the respective information stored at the electronic identity document are not addressed by this document.

4. In order to communicate information about the authenticity and integrity of the electronic identity document and the chip data to the IS user[2] an OI **(Output Interface)** is needed which delegates the information to an output device.

5. The **private key storage** contains the private key of the Inspection System used for Terminal Authentication in the context of EAC.

6. The **certificate and CRL (Certificate Revocation List) storages** contain the CSCA-Certificates and the corresponding CRLs needed for Passive Authentication and may also contain the corresponding DS-Certificates. The certificate chain needed for Terminal Authentication may be stored in the same storage or in a different one.

7. The **logfile storage** contains the logfile written by the TOE for revision purposes. There shall be a logfile to retrace the changes in the TOE's configuration made by the administrator.

Application note 1: *This Protection Profile addresses in its formal sections only the security mechanisms Basic Access Control (BAC), Password Authenticated Connection Establishment (PACE), Chip Authentication and Passive Authentication. A manufacturer producing a complete Inspection System – which is more than the TOE - shall implement in either case also the advanced security mechanism Terminal Authentication.*

2 this could be the border control officer or any other person who is authorised to operate the IS

1.2.3 Usage and major security features

10 The TOE is always used as part of an inspection system. An IS can be used for border control as a stationary or as a mobile device, it can be used as a Kiosk for an information service in a government location or for an updating service in a registry office.

1.2.3.1 Inspection procedure

11 For the user of an IS the procedure is the same in most cases:

1.First the password of the document to be read (if one is needed) is given to the IS. For this there are two possibilities:

1.1. the password (this can also be the MRZ) is typed in via keyboard etc. (other input devices) or

1.2. if possible it is read via an OCR-Reader.

2. the document is laid on the PCD;
3. when the TOE has detected the chip inside the document, it tries to read or write data on the chip;

3.1. therefore the TOE reads first which protocols are supported;

3.2. then the supported protocols are executed (examples how different protocols are applied can be found in [EAC1.11], [EAC2.0] or [ICAO_Doc9303]);

4. the results of this process are delivered over the OI straight to an display or to another application which prepares them for displaying in order to get a simple fast understandable information for the IS user,
5. finally data will be read or written if the protocols were executed successfully.

1.2.3.2 Main security features

12 There are two main security features for the TOE. The first is the protection of sensitive personal data read from or written to the electronic identity document right from the beginning of the reading/writing process as long as the data are in the scope of the TOE.

13 The document chip defines how sensitive the different chip data are. The TOE is not required to protect the data on a higher level than the chip itself does.

14 The other main security feature is the correct procedure of the applied protocols. For this purpose besides the correct implementation and the generation of strong random numbers, the dependability on the certificate storage needed for Passive Authentication and Terminal Authentication is important.

15 In addition the TOE has to be secured against manipulations of the application itself and must generate strong random numbers for the used protocols and protect its ephemeral and static keys.

Application note 2: *If software updates for the TOE are required the ST author has to select secure methods to safely update the TOE's software .*

1.2.4 Protocol overview

protocol name	specified in	keys/certificates/randoms needed by the IS	use case
BAC	[ICAO_Doc 9303]	rnd_{BAC} = random nonce created by the IS K_{BAC} = random key created by the IS	confidentiality of the submitted chip data, authentication & secure channels Is provided by the TOE
Chip Authentication	[EAC1.11] [EAC2.01]	$\widetilde{PK}_{CA}$ = ephemeral public key of the IS $\widetilde{SK}_{CA}$ = ephemeral private key of the IS	originality of the eMRTD chip, secure channels, confidentiality of the submitted chip data Is provided by the TOE
PACE	[EAC2.01]	$\widetilde{PK}_{PACE}$ = ephemeral public key of the IS $\widetilde{SK}_{PACE}$ = ephemeral private key of the IS	confidentiality of the submitted chip data, authentication & secure channels Is provided by the TOE
Passive Authentication	[ICAO_Doc 9303]	CSCA-Certificates and CRLs of the issuing states of the documents to be read	authenticity and integrity of the chip data Is provided by the TOE
Terminal Authentication	[EAC1.11] [EAC2.01]	PK_{PCD} = public key of the IS SK_{PCD} = private key of the IS C_{DV} = Document Verifier Certificate(-s) C_T = Terminal Certificate	authenticity and authorisation of the IS Is provided by the private key storage

1.2.5 TOE type

16 The TOE is a software which is proficient in reading or updating electronic identity documents. The electronic identity documents have protected data and have to prove their

authenticity and integrity by the protocols defined in [ICAO_Doc9303], [EAC2.01] and/or [EAC1.11] to the TOE.

2. Conformance Claim

2.1. Conformance Claim

17 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB- 2009-007-001, Version 3.1, Revision 3, July 2009 [CC_P1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB- 2009-007-002, Version 3.1, Revision 3, July 2009 [CC_P2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB- 2009-007-003, Version 3.1, Revision 3, July 2009 [CC_P3]

as follows

- Part 2 extended,
- Part 3 conformant

18 The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB- 2009-007-004, Version 3.1, Revision 3, July 2009, [CEM]

has to be taken into account.

2.2. PP Claim

19 This PP does not claim conformance to any another Protection Profiles.

2.3. Package Claim

20 This PP is conforming to assurance package EAL3 as defined in CC part 3 [CC_P3].

2.4. Conformance Claim Rationale

21 Because there is no conformance claim to a Protection Profile a rationale is not necessary.

2.5. Conformance Statement

22 This PP calls for "demonstrable" conformance.

23 Note: "Demonstrable" conformance as defined in appendix D.3 of [CC_P1] ensures that a Security Target claiming this PP has to have equivalent (or more restrictive) definitions than defined in this Protection Profile.

3. Security Problem Definition

3.1. TOE security policy

3.1.1 External entities

24 Operator (E1)

The operator is the user of the TOE (e.g. employee of a governmental organization).

25 Administrator (E2)

The administrator is a person who administrates the TOE and who is able to access the TOE on a dedicated service interface to change security attributes of the TOE Security Functionality (TSF).

26 Revisor (E3)

The revisor is a person who is able to access the IS on a dedicated service interface to inspect the log files of the TOE.

27 Attacker (E4)

A person who tries to manipulate the TOE in order to change its behaviour without being authorized or tries to provide the TOE with false information (this may be a forged certificate or a false software update, etc.) is an attacker.

28 Electronic identity document (E5)

An MRTD, ePass or ePA supporting cryptographic mechanisms which allows the Inspection System to check their integrity and authenticity. The electronic identity document is presented to the Inspection System which then communicates with the TOE secured by cryptographic means.

29 Electronic identity document presenter (E6)

Person presenting the electronic identity document to the inspection system and claiming the identity of the electronic identity document holder.

30 Private key storage (E7)

Storage of the Inspection System's key pair. The key pair is used for the Terminal Authentication protocol. The private key storage is protected by further security measures to enforce the protection needs of the Inspection System's key pair.

31 Certificate / CRL storage (E8)

The certificate and CRL storage hold the certificates and CRLs representing the PKI for the Passive Authentication and Terminal Authentication. Furthermore the storage maintains specific certificates and/or specific public keys the Inspection System implicitly trusts in. These specific certificates and/or specific public keys are the root keys of the PKI. The

Certificate and CRL storage is protected by further security measures to enforce the protection needs of the certificates and CRLs.

32 Logfile storage (E9)

The logfile Storage holds the logfile entries generated by the TOE. The logfile Storage is protected by further security measures to enforce the protection needs of the logfile entries.

33 Proximity coupling device (PCD) (E10)

The PCD realizes the interface between the electronic identity document and the TOE. The PCD consists of a contact-less interface and some further electronic components implementing appropriate transmission protocols allowing communication between the PCD and electronic identity documents. Furthermore the PCD provides an interface to the TOE finally allowing the communication between the TOE and electronic identity document.

34 Input interface (II) (E11)

The II shall provide necessary input data from an input device to the TOE. For an Inspection System II devices may be e.g. an OCR reading device to scan the MRZ information, a keyboard to provide the MRZ and further information to the TOE or biometric input devices (e.g. camera, finger print scanner).

35 Output interface (OI) (E12)

The OI delivers results of the inspection process to an output device as well as further information obtained during the process to the user of the TOE (E1 and/or E2). One example for an OI device is a monitor but also a traffic light display indicating the results of the inspection system may be possible.

36 Electronic identity document holder (E13)

The rightful/legitimated holder of the electronic identity document for whom the issuing authority personalised the electronic identity document.

3.1.2 Assets

37 The assets to be protected by the TOE and its environment are as follows:

38 Chip password (O1)

The chip password is used to get basic access to the chip data. In case of an eMRTD according to [ICAO_Doc9303] this would be a part of the MRZ (Machine Readable Zone), for other electronic identity documents this could be e.g. an other password printed on the document (as CAN in [EAC2.01]). Dependent upon the form of the Chip Password it can be read by an OCR Reader or must be typed in on a keyboard, etc.

Required Protection: integrity, confidentiality

39 Personal chip data (O2)

The personal chip data (O2) is the data of a chip of an electronic identity document which is not secured by EAC according to [EAC2.01] and/or [EAC1.11]

Required Protection: integrity, confidentiality

40 Sensitive chip data (O3)

The sensitive chip data (O3) is the data of a chip (DG3, DG4) of an electronic identity document which can be read-out only by processing EAC according to [EAC2.01] and/or [EAC1.11] successfully.

Required Protection: integrity, confidentiality

41 Private key (O4)

The private key (O4) is the private key of the IS used for Terminal Authentication.

Required Protection: integrity, confidentiality

42 Session and Ephemeral Keys (O5)

The session and ephemeral keys (O5) are those non-static keys needed by the TOE to perform the protocols in section 1.2.4.

Required Protection: integrity, confidentiality

43 Random numbers (O6)

The random numbers (O6) are those random numbers needed by the TOE to perform the protocols in section 1.2.4.

Required Protection: integrity

44 Certificates (O7)

The certificates(O7) are needed for Passive Authentication and Terminal Authentication.

Required Protection: integrity

45 CRLs (O8)

CRLs(O8) are needed for Passive Authentication.

Required Protection: integrity including protection against unauthorised deletion

46 Configuration Data (O9)

TSF data to configure the TOE. These data include security attributes of the TSF (e.g. address of update server for revocation lists).

Required Protection: integrity

47 Log data (O10)

A document reading application can write log data to a permanent log file. These data can be used for revision purposes.

Required Protection: integrity

48 Sensitive input data (O11)

All further input data besides the chip password (O1) received from a II are considered as sensitive input data (O11).

Required Protection: integrity, confidentiality

49 Protocol results (O12)

Protocol results are the information about the processed protocols. This includes which protocols have been executed and if applicable what are the results of the process, e.g. the integrity of the chip data has been proved by successful Passive Authentication.

Required Protection: integrity

3.2. Threats

50 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.

51 T.ForgeMRTD – Acceptance of forged MRTD

Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD 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 traveller. 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 MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveller into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder of this MRTD.

Threat agent: An attacker (E4) having basic attack potential, being in possession of one or more legitimate MRTDs

Asset: Protocol Results (O12)

52 T.DataCompromise – Compromise of sensitive MRTD data

Adverse action: An attacker (E4) could pretend to be an operator (E1) using the IS and the TOE to read sensitive data (O2 and O3) from electronic identity documents.

Threat agent: An attacker (E4) having basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance nor having access to the MRTDs accessed

Asset: Personal chip data (O2), sensitive chip data (O3)

53 T.FakedLogfileEntries Spoofing of logfile information

Adverse action: An attacker (E4) could try to manipulate the logfiles (O10) to cover information about the TOE installation which might be changed maliciously.

Threat agent: An attacker (E4) having basic attack potential, having physical access to the Inspection System.

Asset: Log file entries (O10)

54 T.Eavesdropping Eavesdropping of sensitive chip data

Adverse action: An attacker (E4) could eavesdrop sensitive and personal chip data (O2 and O3) transmitted between MRTD Chip and document reading application.

Threat agent: An attacker (E4) having basic attack potential, having physical access to the Inspection System.

Asset: Personal chip data (O2), Sensitive chip data (O3)

3.3. Assumptions

55 A.SecureBoot

It is assumed that the environment provides mechanisms to boot the operating system containing the document application and the device drivers in a secure way so that an initial secure state without protection compromise is guaranteed. Furthermore it is assumed the secure boot process provides an integrity check of the TSF.

56 A.PhysicalTamper

It is assumed that the Inspection System is protected against physical tamper by placing additional devices on the Inspection System as e.g. key loggers or removing the whole terminal or parts of it concerning low level attacks.

57 A.SecureAdministration

It is assumed that the administration of the Inspection System as well as of the TOE installed at the Inspection System is maintained securely. This includes that only authorised personnel is allowed to administer the Inspection System respectively the TOE and that no malware will be installed at the Inspection System.

58 A.TrainedUser

It is assumed that the authorised users of the TOE, operator (E1) and administrator (E2), are well trained. This includes that no user will intentionally compromise the TOE installation as well as the assets secured by the TOE and the TOE environment.

59 A.SecureEnvironment

It is assumed that the TOE environment at the Inspection System is secure. This assumption includes that no other application - or also parts of the operating system - installed at the inspection system compromise sensitive data, manipulate sensitive data or the results of the MRTD authentication, or even try to penetrate the TOE itself with the intention to affect the TOE's security functionality maliciously. Furthermore this includes also that components of the Inspection System the TOE relies on work properly as intended (e.g. the Output of the Inspection System prints the MRTD data as handed over by the TOE, the identification and authentication mechanism of Inspection System – provided by the operating environment – is effective, the security measures of the certificate/ CRL, private key and logfile storage are in place, etc.).

60 A.DisplayShield

It is assumed that the Inspection System is installed in such a way that the sensitive data printed at the output device are visible only to authorised persons.

61 A.ValidKeyAndCertificateData

It is assumed that all further data stored in TOE related components are securely maintained. This includes that they are generated and imported according to their protection requirements as defined in section 3.1.2.

62 A.PKI

It is assumed that the environment provides a public key infrastructure for EAC and Passive Authentication.

3.4. OSP

63 P.CheckTerminal

The integrity of the entire IS hardware shall be checked regularly by the operator (E1) .

The case of the IS should be sealed in a manner that the operator can verify at the beginning of his duty that the terminal is authentic. Therefore a unique label is necessary so that an exchange of the whole IS or manipulation on cable connections can be detected.

The stored log data shall be revised regularly to discover malfunctions or attacks. This shall be done by a revisor (E3) who is not the same person as the administrator (E2).

64 P.Date

The operator (E1) must perform a daily check of the system date and time. Therefore he has to use a reliable reference (e.g. DCF-77 Clock, GPS Clock, etc.). Especially in the context of certificate validation it must be assured that the system date and time is correct.

65 P.ChipPassword

The operator (E1) must ensure during a reading or updating operation that any person who is not authorised to know the chip password (O1) is not able to skim it. Therefore a special distance between the IS and waiting customers shall be enforced.

Application note 3: *This distance is to be defined in the Security Target of the individual TOE depending on its operation purpose.*

66 P.CertifiedPrivateKeyStore

It has to be assured that the private key Storage is a device certified according to minimum EAL4.

67 P.PrivateKeyStore

The private key storage has to authenticate with the electronic identity document (E5) via the Terminal Authentication protocol.

4. Security Objectives

4.1. Security Objectives for the TOE

68 O.AdminAuthorisation

The TOE must provide an administration interface. The TOE shall use the result of an identification and authentication mechanism to enforce that only authorised administrators are allowed to make use of the administration interface to change the TOE's configuration (including update of the TOE's current version). The TOE may use those identification and authentication mechanisms provided by the operating system.

Application note 4: *The identification and authentication (I&A) mechanism has to be provided by the environment according to OE.SecureEnvironment. The ST Author may decide to implement the I&A mechanism in the TOE. In this case the objective for the environment to provide an I&A mechanism may be replaced by an objective for the TOE.*

69 O.OperatorAuthorisation

If personal chip data (O2) and/or sensitive chip data (O3) shall be read the TOE must enforce the authentication of the operator (E1) as an authorised person. The TOE shall use the result of an identification and authentication mechanism to enforce the operator's authorisation. The TOE may use those identification and authentication mechanisms provided by the operating system.

Application note 5: *If sensitive chip data shall be read on a self-service terminal this could be made possible by giving the document holder the authorisation only for reading his/her own data and this would be proved by a secret password known by the holder and the document's chip.*

Application note 6: *The identification and authentication (I&A) mechanism has to be provided by the environment according to OE.SecureEnvironment. The ST Author may decide to implement the I&A mechanism in the TOE. In this case the objective for the environment to provide an I&A mechanism may be replaced by an objective for the TOE.*

70 O.DisplayVersion

The TSF must be able to maintain version information about the TOE itself and must be able to present this evidence to external entities allowing those entities to verify the version of the TSF itself.

71 O.Logdata

The TOE shall write log data at least about every change in configuration or software updates.

72 O.DeletionEphemeralData

The TOE shall delete ephemeral data after every completed or aborted reading/updating process in a secure way (data shall be overwritten). This includes all data read from the chip (O1, O2, O3), every generated random number (O6), ephemeral key and session key (O5) and sensitive input data (O11).

73 O.ProtocolMRTD

The TOE shall implement the protocol according to the specifications [EAC2.01] and/or [EAC1.11] in realisation of an inspection system. This includes the security mechanisms Basic Authentication (BAC), Password Authenticated Connection Establishment (PACE), Chip Authentication and Passive Authentication.

The TOE shall enforce the establishment of secure messaging between the electronic identity document's chip and document application in dependency on the protocols (section 1.2.4) supported by the chip.

4.2. Security Objectives for the Operational Environment

74 OE.SecureBoot

The environment must provide mechanisms to boot the Inspection System OS and the device drivers in a secure way so that an initial secure state without protection compromise is guaranteed.

75 OE.SignedCertsAndCRLs

The environment shall make sure that only certificates, certificate-lists and CRLs (O7, O8) from the certificate storage are provided to the TOE which are signed by the CSCA or a key signed by the CSCA of the operating state.

76 OE.PKI

The environment must provide public key infrastructures for EAC and Passive Authentication according to the specifications in [ICAO_Doc9303], [EAC2.01] and/or [EAC1.11] depending on the used protocols.

Each PKI environment must provide a certificate policy.

77 OE.TA

The environment of the TOE shall implement the cryptographic mechanism Terminal Authentication as part of EAC. This includes maintaining of the terminal's private key and the implementation of the security protocol Terminal Authentication.

78 OE.SecureAdministration

The administration of the Inspection System as well as the TOE itself shall be maintained securely. Only authorised personnel shall be allowed to administer the Inspection System and the TOE. The administration personnel will not install any malicious soft- or hardware at the inspection system.

79 OE.TrainedUser

The Users – operators and administrators – of the Inspection System shall be well trained in a sense not to intentionally compromise neither the TOE installation itself nor the assets secured by the TOE and the TOE environment.

80 OE.SecureEnvironment

The TOE environment shall be secure. Other applications installed at the Inspection System as well as the operating system itself shall not compromise and/or manipulate sensitive data

and shall not penetrate the TOE. The secure environment shall ensure that the results of the MRTD authentication are displayed to the operator unaltered. Further components of the Inspection System the TOE relies on, the certificate and CRL store respectively, the private key Storage and the identification/authentication mechanism of the operating environment shall work properly as intended:

- An effective identification/authentication mechanism shall be implemented by the environment of the TOE. This identification/authentication mechanism shall provide information to the TOE which allows the TOE to assign roles to identities. Such an identification/authentication mechanism may be provided by the operating system.
- The security measures of the certificate and CRL storage respectively and the private key storage shall be in place.
- The operational environment shall provide a secure storage for logfiles which enforces access control and provides secure messaging.

The private key store shall be certified according to the Common Criteria at least with the assurance level EAL4.

81 OE.ComponentCommunication

The communication between the TOE and the logfile storage, the private key storage and the certificate / CRL storage shall be secured for the assets transferred according to the the required protection as defined in chapter 3.1.2.

E.g. the communication between TOE and the private key Store shall be secured against attacks on the confidentiality, authenticity and integrity of the exchanged messages. The communication between the TOE and the log file storage shall be secured against attacks on authenticity and integrity.

82 OE.DisplayShield

The Display of the Inspection System shall be installed in a manner that the output of sensitive data can't be observed by unauthorised persons.

83 OE.CheckTerminalIntegrity

The integrity of the entire IS hardware shall be checked regularly by operator (E1) .

The housing of the IS should be sealed in a manner that the operator can verify at the beginning of his duty that the terminal is authentic. Therefore a unique label is necessary so that an exchange of the whole IS or manipulation on cable connections can be detected.

The stored log data shall be revised regularly to discover malfunctions or attacks. This shall be done by a revisor (E3) who is not the same person as the administrator (E2).

84 OE.Date

The operator (E1) shall check the correctness of the current date and time of the TOE at the beginning of his duty. For this the operator has to use a reliable reference (e.g. DCF-77 Clock, GPS Clock).

85 OE.ChipPassword

The environment must enable the operator (E1) to ensure during a reading or updating operation that any person who is not authorised to know the chip password (O1) is not able to skim it. Therefore a special distance between the IS and waiting customers shall be enforced.

86 OE.ValidKeyAndCertificateData

The TOE environment shall provide adequate measures to ensure the security of the further key and certificate data – including the CRLs – during the generation and the import of such data. In more detail the authenticity and integrity of the private key and the Certificates as well as Certificate Revocation Lists shall be ensured. Furthermore for the private key the confidentiality has to be ensured.

4.3. Security Objective Rationale

87 The following table provides an overview of the security objectives' coverage:

	O.AdminAuthorisation	O.OperatorAuthorisation	O.DisplayVersion	O.Logdata	O.DeletionEphemeralData	O.ProtocolMRTD	OE.SignedCertsAndCRLs	OE.ComponentCommunication	OE.SecureBoot	OE.PKI	OE.TA	OE.SecureAdministration	OE.TrainedUser	OE.SecureEnvironment	OE.DisplayShield	OE.CheckTerminalIntegrity	OE.Date	OE.ChipPassword	OE.ValidKeyAndCertificateData
T.ForgeMRTD	X					X	X				X								
T.DataCompromise	X	X	X		X			X					X		X				
T.FakedLogFileEntries				X				X				X		X					
T.Eavesdropping						X													
A.SecureBoot									X										
A.PhysicalTamper																X			
A.SecureAdministration												X							
A.TrainedUser													X						
A.SecureEnvironment								X						X					
A.DisplayShield															X				
A.ValidKeyAndCertificateData																			X
A.PKI										X									
P.CheckTerminal																X			
P.Date																	X		
P.ChipPassword																		X	
P.CertifiedPrivateKeyStore														X					
P.PrivateKeyStore											X								

Table 1: security objective rationale

4.3.1 Considerations about Threats

88 T.ForgeMRTD

This threat is covered by the following combination of objectives:

O.AdminAuthorisation makes sure that only authorised administrators can change the configuration of the TOE. Therefore attackers cannot change the configuration in any way which might bypass the functionality used to authenticate an MRTD.

OE.SignedCertsAndCRLs makes sure that only legitimate public keys are accepted for the verification of signatures or certificates provided by an MRTD and/or used by the TOE.

O.ProtocolMRTD makes sure that the TOE uses the specified cryptographic protocols to verify the authenticity of data provided by an MRTD.

OE.TA makes sure that the environment supports the advanced cryptographic mechanism necessary for Terminal Authentication according to the respective specifications.

Application note 7: *All security objectives for the environment also help to address this threat, because they prevent modification or bypass of the TOE. However, this holds for all threats in general, because a TOE, which could be modified by unauthorised persons cannot guarantee any security function. Therefore this basic support isn't mentioned in the following discussions any more.*

89 T.DataCompromise

This threat is covered by the following combination of objectives:

O.AdminAuthorisation, **O.OperatorAuthorisation** and **OE.TrainedUser** together make sure that only authorised and trained users can operate the TOE. This prevents compromising MRTD data by operators.

OE.ComponentCommunication, OE.DisplayShield and **O.DeletionEphemeralData** make sure that attackers cannot see secret data during transport between components of the terminal, during display of data or by finding old secret data in the storage of the terminal.

O.DisplayVersion again support this by making sure that only legitimate software is used.

90 T.FakedLogFileEntries

This threat is covered as follows:

O.Logdata makes sure that log entries are written, whenever the TOE configuration is changed or updates are installed.

OE.ComponentCommunication prevents manipulation of log file entries during their transport between TOE and storage.

OE.SecureAdministration and OE.SecureEnvironment make sure that the log files are not manipulated during their storage.

91 T.Eavesdropping

O.ProtocolMRTD makes sure that the specified cryptographic protocols are used for communication between TOE and MRTD. In particular this prevents unauthorised reading of secret data on this interface.

4.3.2 Consideration of the assumptions and OSPs

4.3.2.1 Assumptions

92 A.SecureBoot

OE.SecureBoot addresses this assumption directly as a requirement for the environment of the TOE.

93 A.PhysicalTamper

OE.CheckTerminalintegrity addresses this assumption directly as a requirement for the environment of the TOE.

94 A.SecureEnvironment

The identically named security objective for the environment **OE.SecureEnvironment** together with the security objective for the environment **OE.ComponentCommunication** address this assumption to ensure the secure environment for the TOE.

95 **A.SecureAdministration, A.TrainedUser, A.DisplayShield, A.PKI and A.ValidKeyAndCertificateData** are also directly addressed by security objectives for the environment of the corresponding names.

4.3.2.2 OSP

96 P.CheckTerminal

OE.CheckTerminalintegrity addresses this organisational security policy directly as a requirement for the environment of the TOE.

97 P.Date

OE.Date addresses this organisational security policy directly as a requirement for the environment of the TOE.

98 P.ChipPassword

OE.ChipPassword addresses this organisational security policy directly as a requirement for the environment of the TOE.

99 P.CertifiedPrivateKeyStore

OE.SecureEnvironment addresses this in one of its paragraphs.

100 P.PrivateKeyStore

OE.TA addresses this organisational security policy as a requirement for implementation of the Terminal Authentication protocol by the environment of the TOE.

5. Extended Components Definition

101 This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [PP0002], other components are defined in this protection profile.

5.1. Definition of the family FCS_RND

102 To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1.

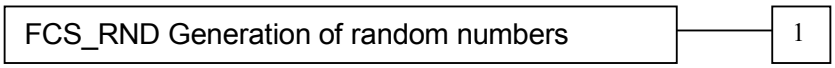
103 The family "generation of random numbers (FCS_RND)" is specified as follows.

104 FCS_RND Generation of random numbers

Family behaviour

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

Component levelling:



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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.2. Definition of the Family FIA_API

105 To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the class FIA (identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

106 The following paragraph defines the family "Authentication Proof of Identity FIA_API".

107 FIA_API Authentication Proof of Identity

Family behavior

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

Component leveling:

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6. Security Requirements

108 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 [CC_P1] of the CC. Each of these operations is used in this PP.

109 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in bold text and the added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

110 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

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

112 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.

113 The definition of the subjects "operator", "administrator", "revisor", "attacker", "electronic identity document", "electronic identity holder", "private key storage", "certificate/CRL storage", "logfile storage", "proximity coupling device", "II" and "OI" used in the following chapter is given in section 3.1.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and "re-authenticate" are originally taken from [CC_P2]. The operation "load" is synonymous to "import" used in [CC_P2].

114 The following table provides an overview of the keys and certificates used:

Name	Data
Country Verifying Certification Authority private key (SK_{CVCA}) and public key (PK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates as well as the corresponding public key (PK_{CVCA}).
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [EAC2.01] and/or [EAC1.11] and Glossary). It contains (i) the Country Verifying Certification Authority public key

Name	Data
	(PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the certificate effective date and the certificate expiration date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier public key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the certificate effective date and the certificate expiration date as security attributes. It is part of the TSF data.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System public key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the certificate effective date and the certificate expiration date as security attributes. It is part of the TSF data.
Terminal Authentication Key Pair	The Terminal Authentication key pair (SK_{PCD}, PK_{PCD}) is used in the context of the Terminal Authentication protocol according to [EAC2.01] and/or [EAC1.11]
Terminal Authentication public key (PK_{PCD})	The Terminal Authentication public key (PK_{PCD}) is stored in the IS and used by the TOE for Terminal Authentication of the TOE.
Terminal Authentication private key (SK_{PCD})	The Terminal Authentication private key (SK_{PCD}) is used by the TOE to authenticate itself as authentic IS. It is part of the TSF data.
CSCA-Certificates	Country Signing CA Certification Authority of the MRTD issuing state or organization signs the Document Signer public key certificate with the Country Signing Certification Authority private key and the signature will be verified by receiving state or organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority public key.
CSCA-Certificate CRLs	The Inspection System stores in the certificate/CRL storage CRLs related to the CSCA certificates. During Passive Authentication the Inspection System checks whether the Document Signer certificate is still valid.
Document basic access	The document basic access key is created by the

Name	Data
keys	Personalization Agent, loaded to the MRTD, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip. This can be either the MRZ used for BAC or PACE, or the CAN (see [EAC2.01]) used for PACE.
Chip Authentication Ephemeral Key Pair	During the Chip Authentication protocol the TOE generates the Chip Authentication ephemeral key pair $\widetilde{SK}_{CA}$, $\widetilde{PK}_{CA}$.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a MRTD in result of the Basic Access Control authentication protocol.
PACE Session Keys	Secure messaging with Triple-DES key and Retail-MAC key or AES and CMAC agreed between the TOE and a MRTD in result of the Password Authenticated Connection Establishment Protocol (PACE).
Chip Session Key	Secure messaging with Triple-DES key and Retail-MAC key or AES and CMAC agreed between the TOE and a MRTD in result of the Chip Authentication Protocol.

Table 2: Keys and Certificates

6.1. Security Functional Requirements for the TOE

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

6.1.1 Class FAU Security Audit

6.1.1.1 Audit data generation (FAU_GEN.1)

116 The TOE shall meet the requirement "Audit data generation (FAU_GEN.1)" as specified below (Common Criteria Part 2).

117 FAU_GEN.1/Audit Audit data generation - Audit

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps.

FAU_GEN.1.1/Audit	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and c) every change of TOE configuration, or software updates and [assignment: *other specifically defined auditable events*].[3]
FAU_GEN.1.2/Audit	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

Refinement: The TOE supports the storage of audit records by the TOE environment (cf. OE.SecureEnvironment) by providing the respective information and by sending that information to the secure audit storage.

Application note 8*: The ST writer shall perform the open operation in the element FAU_GEN.1. The ST writer may add further auditable events to be stored in the logfile storage.*

Application note 9*: The TOE makes use of the time stamps provided by the TOE environment (cf. OE.SecureEnvironment and OE.Date).*

118 FAU_GEN.1/PA Audit data generation – Passive Authentication

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps.

FAU_GEN.1.1/PA	The TSF shall be able to generate **information**[4] of the following auditable events: – announcement of having processed the Passive Authentication protocol including the result of the process – announcement of having processed the Chip Authentication protocol including the result of the process.[5]

3 [assignment: *other specifically defined auditable events*]

4 Refinement: an audit record

5 Refinement:

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and

FAU_GEN.1.2/PA The TSF shall **export**[6] within **the Passive and Chip Authentication result status output**[7] at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, Passive and Chip Authentication carried out and [assignment: *other audit relevant information*].[8]

Refinement: The TSF shall implement the Passive Authentication and Chip Authentication protocol (cf. FCS_COP.1/CER). The TSF shall present the result of the Passive Authentication protocol and the Chip Authentication protocol to the operator.

Application note 10*: The ST writer shall perform the open operation in the element FAU_GEN.1/PA. The ST writer may add further information presented in the context of the Passive Authentication and Chip Authentication protocol result.*

Application note 11*: The TOE makes use of the time stamps provided of the TOE environment (cf. OE.SecureEnvironment and OE.Date).*

6.1.2 Class Cryptographic Support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

119 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 keys to be generated by the TOE.

120 FCS_CKM.1/KDF Cryptographic key generation – Document Basic Access Key

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/KDF The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[9] and specified cryptographic key

- [assignment: other specifically defined auditable events].

6 Refinement: record

7 Refinement: each audit record

8 [assignment: *other audit relevant information*]

sizes 112 bit[10] that meet the following: [assignment:*list of standards*].

Application note 12: *The ST writer shall perform the open operation in the element FCS_CKM.1.1/KDF. The cryptographic key generation algorithm and the cryptographic key sizes depend on the protocol which shall be used by the inspection system. The assigned list of standards shall ensure that the Inspection System derives the same document basic access key as loaded by the personalization agent into the MRTD and used by the TOE for FIA_UAU.4. The [ICAO_Doc9303], Annex A5.1, referenced by [EAC1.11]/[EAC2.01], describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the document basic access keys for Basic Access Control from the second line of the printed MRZ data.*

121 FCS_CKM.1/PACE Cryptographic key generation – Diffie-Hellmann PACE Keys

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/PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm password authenticated Diffie-Hellman key agreement[11] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [EAC2.01], *A.2.3 and A.3*.[12]

Application note 13: *The ST writer shall perform the open operation in the element FCS_CKM.1.1/PACE. The cryptographic key generation algorithm and the cryptographic key sizes depend on the protocol which shall be used by the inspection system for PACE. The [EAC2.01] describes the key agreement protocol for PACE in Annex A.2.3. Annex A.3. of [EAC2.01] lists the standards for symmetric keys agreed by PACE. The shared secret value is used to derive the AES or Triple-DES key for encryption and the Retail-MAC chip session keys according to the Document Basic Access Key Derivation Algorithm [ICAO_Doc9303], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC*

122 FCS_CKM.1/DH Cryptographic key generation – Diffie-Hellmann Chip Authentication Keys

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

9 [assignment: *cryptographic key generation algorithm*]

10 [assignment: *cryptographic key sizes*]

11 [assignment: *cryptographic key generation algorithm*]

12 [assignment: *list of standards*]

FCS_CKM.1.1/DH	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [EAC2.01] and/or [EAC1.11], Annex A.1.[13]

Application note 14: *The TOE generates a shared secret value with the terminal during the Chip Authentication protocol, see [EAC2.01] and/or [EAC1.11], sec. 3.1 and Annex A.1. The shared secret value is used to derive the AES or Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [ICAO_Doc9303], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC.*

6.1.2.2 Cryptographic key destruction (FCS_CKM.4)

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

124 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion by overwriting the memory data with other values or the new key[14] that meets the following: none[15].

Refinement: The TOE shall destroy the BAC session keys and PACE session keys (i) after detection of an error in a received command by verification of the MAC, or (ii) after successful run of the Chip Authentication protocol. The TOE shall destroy the chip session keys as well as the Chip Authentication ephemeral key pair after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys as well as ephemeral keys after ending a session and therefore before starting the communication with the MRTD in a new session.

6.1.2.3 Cryptographic operation (FCS_COP.1)

125 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.

13 [assignment: *list of standards*]

14 [assignment: *cryptographic key destruction method*]

15 [assignment: *list of standards*]

126 FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation and Passive 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
FCS_COP.1.1/ SHA	The TSF shall perform hashing [16] in accordance with a specified cryptographic algorithm SHA-1, SHA-256 and [assignment:*other approved algorithms*][17] and cryptographic key sizes none [18] that meet the following: [selection: *FIPS 180-2 or other approved standards*].[19]

Application note 15: *The ST writer shall perform the missing selection operation. The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control authentication mechanism (cf. [ICAO_Doc9303], annex A5.1, cf. [PP_BAC] also). For the Passive Authentication mechanism the TOE must implement at least SHA-1 and SHA -256. The TOE may implement additionally the SHA-224, the SHA-384 and/or the SHA-512 algorithm. The Chip Authentication protocol and the Password Authenticated Connection Establishment protocol may use SHA-1 for session key derivation (cf. [EAC2.01] and/or [EAC1.11], normative appendix 5, A5.1).*

127 FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ SYM	The TSF shall perform secure messaging – encryption and decryption [20] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: 'TR-03110', [EAC2.01] and/or [EAC1.11]. [21]

16 [assignment: *list of cryptographic operations*]

17 [assignment: *cryptographic algorithm*]

18 [assignment: *cryptographic key sizes*]

19 [assignment: *list of standards*]

20 [assignment: *list of cryptographic operations*]

21 [assignment: *list of standards*]

Application note 16: *This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the MRTD during the execution of the Basic Access Control authentication mechanism, the Password Authenticated Connection Establishment or as part of the Chip Authentication protocol according to the FCS_CKM.1.*

128 FCS_COP.1/MAC Cryptographic operation – MAC

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ MAC: The TSF shall perform secure messaging – message authentication code [22] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: 'TR-03110', [EAC2.01] and/or [EAC1.11]. [23]

Application note 17: *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 during the execution of the Basic Access Control authentication mechanism, the Password Authenticated Connection Establishment or the Chip Authentication protocol according to the FCS_CKM.1.*

129 FCS_COP.1/CER Cryptographic operation – Signature check

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/ CER: The TSF shall perform signature check using CRLs and the whole certificate chain [24] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application note 18: *The TSF shall perform signature check using CRLs and the whole certificate chain in the context of performing the security protocol Passive Authentication as described in [EAC2.01], [EAC1.11] and [ICAO_Doc9303], respectively.*

22 [assignment: *list of cryptographic operations*]

23 [assignment: *list of standards*]

24 [assignment: *list of cryptographic operations*]

Application note 19: *The ST writer shall perform the missing operation for the assignment of the signature algorithm and key sizes as well as the appropriate list of standards supported by the TOE.*

6.1.2.4 Random Number Generation (FCS_RND.1)

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

131 FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet the functionality class K4 as defined in [AIS20] with at least 64 bit entropy for the seed[25].

Application note 20: *This SFR requires the TOE to generate random numbers used for the authentication protocols as requested by the requirements of FCS_CKM.1 and FIA_UAU.5 respectively.*

6.1.3 Class User Data Protection (FDP)

6.1.3.1 Residual information protection (FDP_RIP)

132 The TOE shall meet the requirement "Residual information protection (FDP_RIP.1)" as specified below (Common Criteria Part 2).

133 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from [26] the following objects: Chip Password, personal chip data, sensitive chip data, sensitive input Data.[27]

Refinement: The TSF shall delete the information after every completed or aborted reading/updating process at least by an overwriting mechanism.

25 [assignment: *a defined quality metric*]

26 [selection: a*llocation of the resource to, deallocation of the resource from*]

27 [assignment: *list of objects*]

Application note 21: *The objects requested to be deleted by this requirement have to be deleted by the TSF only if they have been produced during the inspection process.*

6.1.4 Class Identification and Authentication (FIA)

134 The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended).

135 FIA_API.1/BAC Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/BAC	The TSF shall provide a Basic Access Control authentication mechanism according to [EAC2.01] and [EAC1.11][28] to prove the identity of the electronic identity document presenter[29].

Application note 22: *This SFR requires the TOE to implement the Basic Access Control authentication mechanism specified in [EAC2.01] and [EAC1.11].*

136 FIA_API.1/PACE Password Authenticated Connection Establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/PACE	The TSF shall provide a Password Authenticated Connection Establishment according to [EAC2.01][30] to prove the identity of the electronic identity document presenter[31].

Application note 23: *This SFR requires the TOE to implement the Password Authenticated Connection Establishment specified in [EAC2.01].*

6.1.4.1 Single-use authentication mechanisms (FIA_UAU.4)

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

138 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

28 [assignment: authentication mechanism]

29 [assignment: authorized user or role]

30 [assignment: authentication mechanism]

31 [assignment: authorized user or role]

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

1. Basic Access Control authentication mechanism
2. Password Authenticated Connection Establishment.[32]

Application note 24: *The Basic Access Control authentication mechanism [ICAO_Doc9303] and the Password Authenticated Connection Establishment [EAC2.01] use a challenge RND.IFD freshly and randomly generated by the terminal to prevent reuse of a response generated by an MRTD's chip and of the session keys from a successful run of the authentication protocol.*

6.1.4.2 Multiple authentication mechanisms (FIA_UAU.5)

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

140 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. Password Authenticated Connection Establishment
3. Passive Authentication
4. Chip Authentication protocol[33]

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 MRTD by means of the Basic Access Control authentication mechanism with the document basic access keys or by means of the Password Authenticated Connection Establishment authentication mechanism.
2. After successful authentication as MRTD and until the completion of the Chip Authentication mechanism the TOE accepts only response codes with correct message authentication code sent by means of secure messaging with keys agreed with the authenticated MRTD by means of the Basic Access Control authentication mechanism or by means of the Password Authenticated Connection

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

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

Establishment authentication mechanism.

3. The TOE accepts the authenticity and integrity of the MRTD Data by means of the Passive Authentication mechanism after successful authentication by Basic Access Control or Password Authenticated Connection Establishment authentication mechanism.
4. After run of the Chip Authentication mechanism the TOE accepts only response codes with correct message authentication codes sent by means of secure messaging with keys agreed with the terminal by means of the Chip Authentication mechanism[34]

Application note 25: *Basic Access Control mechanism or the Password Authenticated Connection Establishment authentication mechanism include the secure messaging for all commands and response codes exchanged after successful mutual authentication between the inspection system and the MRTD. The inspection system shall use the Basic Access Control authentication mechanism with the document basic access keys or the Password Authenticated Connection Establishment authentication mechanism drawn from the second, optical readable MRZ line and the secure messaging after the mutual authentication. The Inspection System and the MRTD shall use the secure messaging with the keys generated by the Chip Authentication mechanism after the mutual authentication.*

6.1.4.3 Re-authenticating (FIA_UAU.6)

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

142 FIA_UAU.6/BT Re-authenticating – BAC/PACE

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FIA_UAU.6.1/BT The TOE shall re-authenticate the user under the conditions

1. Each response sent to the TOE after successful authentication of the MRTD with Basic Access Control or Password Authenticated Connection Establishment authentication mechanism and until the completion of the Chip Authentication mechanism shall have a correct MAC created by means of secure messaging keys agreed upon by the Basic Access Control authentication or by the Password Authenticated Connection Establishment mechanism
2. Each response sent to the TOE after successful run of the Chip Authentication protocol shall have a correct MAC created by means of secure messaging keys generated by Chip Authentication protocol.[35]

Application note 26: *The Basic Access Control mechanism, the Password Authenticated Connection Establishment mechanism and the Chip Authentication protocol specified in [EAC2.01] and/or [EAC1.11] include secure messaging for all commands and responses exchanged after successful authentication of the TOE. The TOE checks by secure messaging in MAC_ENC mode each response based on Retail-MAC whether it was sent by the successfully authenticated MRTD (see FCS_COP.1/MAC for further details). The TOE does not accept any response with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those responses received from the authenticated user.*

6.1.4.4 User identification (FIA_UID.1)

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

144 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] 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.

Refinement: The TOE verifies the result of the identification/authentication system of the environment by only respecting the roles supported by the TOE (see OE.SecureEnvironment).

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

Application note 27*: The ST author may specify actions, which are allowed before authentication, however the modification of configuration data of the TOE must not be in this list, since authentication is required for that activity. If the list is empty, FIA_UAU.2 shall be used in the ST instead.*

6.1.5 Class Security management (FMT)

6.1.5.1 Management of TSF data (FMT_MTD.1)

145 The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations are caused by different security roles which have to be implemented by the TOE.

146 **FMT_MTD.1/Admin - Management of TSF data**

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Admin: The TSF shall restrict the ability to modify[36] the
- configuration data of the TOE and
- the further TSF data: [assignment: *list of TSF data*][37]

to the administrator[38].

147 **FMT_MTD.1/Version - Management of TSF data**

Hierarchical to: No other components.

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

FMT_MTD.1.1/Version: The TSF shall restrict the ability to read[39] the TOE version and further TSF data: [assignment: *list of TSF data*][40] to the operator and the administrator[41].

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

37 [assignment: *list of TSF data*]

38 [assignment: *the authorised identified roles*]

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

40 [assignment: *list of TSF data*]

6.1.5.2 Specification of management functions (FMT_SMF.1)

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

149 **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:

- modification of configuration data of the TOE
- read the TOE version
- [assignment: *list of further management functions to be provided by the TSF*] [42]

6.1.5.3 Security management roles (FMT_SMR)

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

151 **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:

- administrator
- operator
- and the further authorised roles [assignment: *the authorised identified roles*][43]

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

Application note 28*: The identification/authentication mechanism is implemented by the TOE environment* (see OE.SecureEnvironment). *The TOE reuses the result of the identification/authentication mechanism by the determination of the user's role.*

41 [assignment: *the authorised identified roles*]

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

43 [assignment: *the authorised identified roles*]

6.2. Security Assurance Requirements for the TOE

152 The security assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 3 (EAL3).

6.3. Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	O.AdminAuthorisation	O.OperatorAuthorisation	O.DisplayVersion	O.Logdata	O.DeletionEphemeralData	O.ProtocolMRTD
FAU_GEN.1/Audit Audit data generation – Audit				X		
FAU_GEN.1/PA Audit data generation – Passive Authentication						X
FCS_CKM.1/KDF Cryptographic key generation – Document Basic Access Key						X
FCS_CKM.1/PACE Cryptographic key generation – Diffie-Hellmann PACE Keys						X
FCS_CKM.1/DH Cryptographic key generation – Diffie-Hellmann Chip Authentication Keys						X
FCS_CKM.4 Cryptographic key destruction					X	X
FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation and Passive Authentication						X
FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption						X
FCS_COP.1/MAC Cryptographic operation – MAC						X
FCS_COP.1/CER Cryptographic operation – Signature check						X
FCS_RND.1 Quality metric for random numbers						X
FDP_RIP.1 Subset residual information protection					X	
FIA_API.1/BAC Authentication Proof of Identity						X
FIA_API.1/PACE Authentication Proof of Identity						X
FIA_UAU.4 Single-use authentication mechanisms						X
FIA_UAU.5 Multiple authentication mechanisms						X
FIA_UAU.6/BT Re-authentication – BAC/PACE						X
FIA_UID.1 Timing of Identification	X	X				
FMT_MTD.1/Admin – Management of TSF data	X					
FMT_MTD.1/Version – Management of TSF data	X	X				
FMT_SMF.1 Specification of management functions	X	X	X			

	O.AdminAuthorisation	O.OperatorAuthorisation	O.DisplayVersion	O.Logdata	O.DeletionEphemeralData	O.ProtocolMRTD
FMT_SMR.1 Security roles	X	X				

Table 3: Coverage of Security Objectives for the TOE by SFRs

154 The Security Objectives for the TOE are covered by the SFRs as follows:

155 **O.AdminAuthorisation** is addressed by FIA_UID.1, because this SFR makes sure that only authorised persons can act as administrators. In addition FMT_SMR.1, FMT_SMF.1, FMT_MTD.1/Version and FMT_MTD.1/Admin specify the actions allowed for the administrator.

156 **O.OperatorAuthorisation** is also addressed by FIA_UID.1, because this SFR makes sure that only authorised persons can act as operators. In addition FMT_SMR.1, FMT_SMF.1 and FMT_MTD.1/Version specify the actions allowed for the operators.

157 **O.DisplayVersion** is addressed by FMT_SMF.1, which specifies a requirement to output the TOE's version number on request of the operator and administrator.

158 **O.LogData** is addressed by FAU_GEN.1/Audit, which requires suitable log data to be generated.

159 **O.DeletionEphemeralData** is addressed by FDP_RIP.1 and FCS_CKM.4, which require deletion of security relevant data after their use.

160 **O.ProtocolMRTD** is realised by several SFRs as follows: The SFRs FCS_CKM.1/*, FCS_CKM.4, FCS_COP.1/* and FCS_RND.1 from class FCS provide the various cryptographic functions and protocols used for the MRTD protocols (including the generation of keys, where applicable). The SFRs FIA_API.1/*, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6/BT from class FIA describe properties of the authentication protocols used between TOE and MRTDs. FAU_GEN.1/PA requires the TOE to present the enforcement and the result of the Passive Authentication to the operator of the Inspection System.

6.3.2 Dependency Rationale

161 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.

162 The following table shows the dependencies between the SFRs of the TOE:

SFR	Dependencies	Support of the Dependencies
FAU_GEN.1/Audit and FAU_GEN.1/PA	FPT_STM.1 Reliable Time Stamps	Not fulfilled: It is assumed that the environment (the hardware/operating system) provides a time stamp. The correctness of the time is verified by the administrator at least once a day, which is considered sufficient here (cf. OE.Date).
FCS_CKM.1/KDF	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SYM and .../MAC (note that FIA_UAU.5 specifies the mutual authentication mechanism, which derives session keys from the BAC key) FCS_CKM.4
FCS_CKM.1/PACE	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SYM and .../MAC FCS_CKM.4
FCS_CKM.1/DH	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SYM and .../MAC FCS_CKM.4
FCS_CKM.4	[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.1/*
FCS_COP.1/SHA	[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	Not fulfilled: SHA doesn't need cryptographic keys and therefore none of the dependencies applies.
FCS_COP.1/SYM and .../MAC	[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	FCS_CKM.1/*

SFR	Dependencies	Support of the Dependencies
	generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4
FCS_COP.1/CER	[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	Not fulfilled formally, but the TOE is obligated by FIA_UAU.5 to provide the Passive Authentication Protocol. This protocol addresses the public key which is subject of this SFR. The application note given subsequently to the SFR definition affirmed this approach. Not fulfilled: For a public key there is no security requirement for key destruction.
FCS_RND.1	None.	n.a.
FDP_RIP.1	None.	n.a.
FIA_API.1/*	None	n.a.
FIA_UAU.4, .5, .6	None	n.a.
FIA_UID.1	None	n.a.
FMT_MTD.1/*	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	None	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1

Table 4: Dependencies between the SFR for the TOE

6.3.3 Security Assurance Requirements Rationale

163 The EAL3 was chosen to permit a developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security and require a thorough investigation of the TOE and its development without substantial re-engineering.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

164 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.

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

166 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 analysed, and non-satisfied dependencies are appropriately explained.

167 The assurance class EAL3 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.

168 Inconsistencies 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. Annex

7.1. Glossary and Acronyms

Glossary

Term	Definition
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Audit entries generated by the TOE and stored in the TOE environment
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control (BAC)	Security mechanism defined in [ICAO_Doc9303] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with document basic access keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminal's part of the Basic Access Control mechanism and authenticates itself to the MRTD's chip using the document basic access keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO_Doc9303]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Inspection System 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).
Complete Inspection System	An complete inspection system is a terminal providing respective services to a human user. E.g. such a terminal can be an attended terminal operated by an border control officer or also an self-service

Term	Definition
	terminal operated by the electronic identity document holder himself. In this sense the TOE described in this protection profile is a major internal part of an complete inspection system.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_Doc9303]
Country Signing CA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority public key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier certificates within this PKI. It enforces the privacy policy of the issuing state or organization with respect to the protection of sensitive biometric reference data stored in the MRTD.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used to validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [ICAO_Doc9303], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the document basic access keys from the second line of the printed MRZ data.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [ICAO_Doc9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer certificate (C_{DS}). [ICAO_Doc9303]
Document Verifier	Certification authority creating the Inspection System certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing states or organizations

Term	Definition
Eavesdropper	A threat agent with enhanced-basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_Doc9303]
ePA	The contactless smart card integrated into the plastic, optical readable cover and providing the following applications: ePassport, eID and eSign (optionally). [PP_eID]
ePass	Look at the term *Machine readable travel document (MRTD)*.
Extended Access Control	Security mechanism identified in [ICAO_Doc9303] by means of which the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The personalization agent may use the same mechanism to authenticate itself with personalization agent private key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication mechanism, (ii) implements the Terminal Authentication protocol and (iii) is authorized by the issuing state or organization through the Document Verifier of the receiving state to read the sensitive biometric reference data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing state or Organization to read the optional biometric reference data and supports the terminal's part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO_Doc9303]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs.

Term	Definition
	[ICAO_Doc9303]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_Doc9303]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_Doc9303]
Inspection or *Inspection Process*	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO_Doc9303]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. Here the "document application" represents the core of the inspection system.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm that the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing state or organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_Doc9303]
Issuing State	The country issuing the MRTD. [ICAO_Doc9303]
Kiosk	An application for the ePA/ePass user to check his/her data on the ePA or ePass.

Term	Definition
Logical Data Structure (LDS)	The collection of groupings of data elements stored in the optional capacity expansion technology [ICAO_Doc9303]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [ICAO_Doc9303] as specified by ICAO on the contact-less integrated circuit. It presents contact-less readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16). (6) EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contact-less integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a state or organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_Doc9303]
Machine readable visa (MRV):	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [ICAO_Doc9303]

Term	Definition
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO_Doc9303]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_Doc9303]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [ICAO_Doc9303], - the definition of the user data, but does not include the user data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing state or organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO, [ICAO_Doc9303].
MRTD's chip Embedded Software	Software embedded in an MRTD's chip and not being developed by the IC designer. The MRTD's chip embedded software is designed in phase 1 and embedded into the MRTD's chip in phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.

Term	Definition
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Receiving State	The country to which the traveller is applying for entry. [ICAO_Doc9303]
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.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO_Doc9303]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contact-less communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the certificate holder authorizations defined by the Inspection System certificate, the Document Verifier certificate and Country Verifying Certification Authority which shall all be valid for the current date.
Travel document	A passport or other official document of identity issued by a state or organization which may be used by the rightful holder for international travel. [ICAO_Doc9303]
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC_P1]).
Unpersonalized MRTD	The MRTD that contains the MRTD chip holding only initialization data and pre-personalization data as delivered to the personalisation agent from the manufacturer.
User data	Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC_P1]).

Term	Definition
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO_Doc9303]
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
BIS	Basic Inspection System
CC	Common Criteria
DIS	Distributed Inspection System
DS	Document Signer
EF	Elementary File
EIS	Extended Inspection System
GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number.
MF	Master File
n.a.	Not applicable
OSP	Organizational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE security functionality

7.2. References

Common Criteria

[CC_P1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB- 2009-007-001, Version 3.1, Revision 3, July 2009

[CC_P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB- 2009-007-002, Version 3.1, Revision 3, July 2009

[CC_P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB- 2009-007-003, Version 3.1, Revision 3, July 2009

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB- 2009-007-004, Version 3.1, Revision 3, July 2009

[AIS20] Anwendungshinweise und Interpretationen zum Schema, AIS20 Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 1, 02.12.1999, Bundesamt für Sicherheit in der Informationstechnik

ICAO

[ICAO_Doc9303] ICAO Doc 9303. 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.

Protection Profiles

[PP0002] PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

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

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

[PP_eID] Common Criteria Protection Profile Electronic Identity Card (ID_Card PP), BSI-CC-PP-0061, Version 1.03, 15th December 2009

Other

[EAC1.11] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[EAC2.01] BSI. Technical Guideline: Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC),Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.01, TR-03110, 2009.

[TR_ECC] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006

[ISO/IEC14443] ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards,2000

[ISO/IEC7816] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004

[ISO/IEC15946-3] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

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