ID&TRUST DOCUMENTS

EMRTD WITH BAC

COMMON CRITERIA EVALUATION

01. SECURITY TARGET ID&TRUST IDENTITY CARD 3.1/BAC

Revision history

Version	Date	Information
v.0.1.	05.06.2013.	First Draft
v.0.2.	24.06.2013	Corrections
v.0.3.	02.09.2013.	First Evaluation version
v.0.4.	25.09.2013.	Composite TOE considerations
v.0.5	14.10.2013.	The ETR fc indicated changes
v.0.6.	18.03.2014	Corrections
v.0.7.	21.03.2014	Further corrections
v.0.8.	25.03.2014	Corrections of formal and conceptual differences
v.0.9.	26.03.2014.	Correcting table headings
v.0.10.	31.03.2014.	OR changes
v.0.11.	13.08.2015	Huntrust->ID&Trust, Certifier review

Table of Contents

1 ST Introduction

1 This section provides document management and overview information that are required a potential user of the TOE to determine, whether the TOE fulfils its requirements.

2 Throughout this document, the term BAC refers to Basic Access Control.

3 The inspection system SHALL use BAC in the session."

1.1 ST reference

4 Title: Security Target ID&Trust Identity Applet Version 3.1. / BAC

TOE: ID&Trust IDentity Card 3.1: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite Version 3.1 / BAC

TOE short name: IDentity v3.1/BAC

Editor(s): Tamás Szabó ID&Trust.

CC Version: 3.1 (Revision 4)

Assurance Level: EAL4 augmented with the following assurance component: ALC_DVS.2.

Version Number: 0.11

Date: 13.08.2015.

TOE Documentation:

- IDentity Applet Initialization and configuration Version 3.1.05
- IDentity Applet Administrator's Guide Version 3.1.06
- IDentity Applet User's Guide Version 3.1.12

1.2 TOE reference

5 The Security Target refers to the product "ID&Trust ID Card 3.1: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Card 3.1" (TOE) for CC evaluation.

6 The TOE comprises:

i. Underlying Platform of the TOE, which is evaluated by Brightsight and certified by TÜV Rheinland Nederland B.V. at assurance level EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 under the certificate number C13-37760 [25]

Platform name: J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65, Secure Smart Card Controller Revision 3

Short name: JCOP 2.4.2 R3

It consists of:

a. Smart card platform (SCP), which consists of:

i. Hardware Abstraction Layer with the Crypto Lybrary,

ii. Hardware Platform

b. Embedded software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager)

c. Native MIFARE application (physically always present but logical availability depends on configuration)

and

ii. the Application Part of the TOE:

ID&Trust IDentity Applet Suite Version 3.1 , configured as eMRTD application,

iii. the associated guidance documentation.

1.3 TOE overview

7 The Security Target defines the security objectives and requirements for the contact based / contactless smart card of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in 'ICAO Doc 9303' [6].

8 The Target of Evaluation (TOE) is the a contactless integrated circuit chip containing components for a machine readable travel document (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to ICAO Doc 9303' [6].

9 The Application part of the TOE, the applet functionalities are distributed according to the following table:

No	Function	Standard
1	European citizen card	CEN/TS 15480-2
2	European card for e-Services and National e-ID applications	IAS-ECC 1.0.1 specification
3	Basic Access Control	ICAO Doc 9303
4	Extended Access Control v1	BSI TR-3110 version 2.10
5	International Driving License	ISO/IEC 18013
6	European Driving License	EC 383/2012

Table 1: Applet functionalities

10 All the functions are supplied by the applet "ID&Trust IDentity Applet Suite Version 3.1", the behaviour of the applet changes according to the environmental behaviour. The scope of the current ST is only concerned with applet behaviour No 3 .

11 For the TOE, beside the eMRTD application other applications may be present on the JCOP 2.4.2 R3. They are not relevant for the current ST and do not infer the Security Functions of the TOE. The TOE utilises the results of the NXP Secure Smart Card Controllers P5Cx128V0v/P5Cx145V0v/V0B(s) certified under the German CC Scheme (BSI-DSZ-CC-0858) and the Crypto Library V2.7/V.2.9 on SmartMX P5Cx128/P5Cx145 V0v/V0B(s) certified under the German CC Scheme (BSI-DSZ-CC-0750).

12 The intended customer of the product the Card Issuer, who is in charge of the issuance of the product to the smartcard holders.

13 **Application note 1 (of the ST author):** Operational mode of the TOE depends on the decided operation of the Inspection Sytem. Identity Applet can work using BAC or EAC with PACE authentication also. If the Inspection System knows the EAC with PACE mode and wants to use it the TOE accepts it and communicates on this way. Nevertheless, this ST addresses the Basic Access Control only. EAC with PACE is out of scope of this ST and is described in an another ST.

1.3.1 Non-TOE hardware/software/firmware

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

1.4 TOE description

15 The Platform part of the Composit ST can be any of the following products:

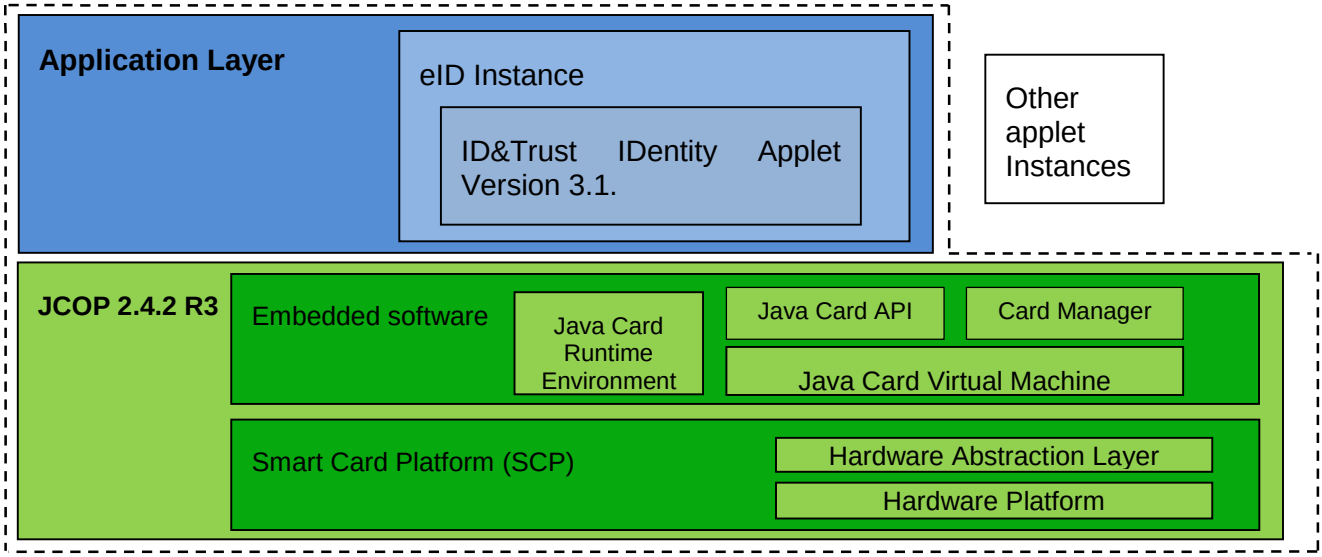
- J3E120_M65
- J2E120_M65
- J3E082_M65
- J2E082_M65

These are all based on:

- the P5Cx128/P5Cx145 V0v/ V0B(s) hardware controller.
- Crypto library version 2.7/2.9 which is built upon the hardware platform
- JCOP 2.4.2 R3 OS which is built upon the hardware platform and the
- Crypto Library platform

16 The composite part always means ID&Trust IDentity Suite 3.1.

17 The logical architecture of the TOE:



1.4.1 TOE usage and security features for operational use

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

19 For this security target the travel document is viewed as unit of

i. the physical part of the travel document in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder
   a) the biographical data on the biographical data page of the travel document surface,
   b) the printed data in the Machine Readable Zone (MRZ) and
   c) the printed portrait.

20 ii. the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [6] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document holder
   a) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   b) the digitized portraits (EF.DG2),
   c) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]
   d) the other data according to LDS (EF.DG5 to EF.DG16) and
   e) the Document Security Object (SOD).

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

22 The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [6]. These security measures can include the binding of the travel document's chip to the travel document.

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

24 The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, 'ICAO Doc 9303' [6].

25 This security target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism. This security target does not address the Active Authentication and the Extended Access Control as optional security mechanisms,

26 The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system according to [6], normative appendix 5.

1.4.2 TOE life cycle

27 The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [18], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

28 Phase 1 "Development"

[1] These additional biometric references are optional, and accessible only during PACE sessions.

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

29 (Step2) NXP uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system). The eMRTD application and the guidance documentation associated with these TOE components are developed by ID&Trust Ltd.[2]

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

31 Phase 2 “Manufacturing”

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

32 If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM). The IC manufacturer in this phase preconfigures the JCOP card and the EEPROM.

33 (Step4 optional) The travel document manufacturer combines the IC with hardware for the contact based/contactless interface in the travel document.

34 (Step5) The travel document manufacturer (i) adds the IC Embedded Software or part of it in the non-volatile programmable memories (for instance EEPROM or FLASH) if necessary (this is the so-called Pre-personalization), (ii) creates the eMRTD application, and (iii) equips travel document’s chips with preloaded-personalisation Data.

35 **Application note 2 (redefined for the goals of this ST by the ST author, originally from [22]):** Creation of the application implies the Applet ROM-coding NXP burns the ROM of the integrated circuits putting the IDentity on it. This procedure is called ROM coding. Once it is done, the card or integrated circuit cannot be programmed or reprogrammed again The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation to the Personalisation Agent.

[2] In the case of the Current Security Target, the Common Criteria Certified JCOP v2.4.2 R3 Platforms also the IC Embedded Software (Operating System) and the IC Dedicated Softwarec (cryptographic library) and becasue of ROM coding the eMRTD application, thus the Software Developers are two separated entities, NXP and ID&Trust, the latter only responsible for the development of the IDentity Applet. The development of the Platform and the cryptolibrary is at one developer, NXP, the development of the Applet and related documentation is at an another site in Hungary, by ID&Trust Ltd. For more information on this, see Statement of Compatibility concerning Composite Security Target chapter.

The Personalization Agent Authentication Keys are the preinstalled keys for the Applet, which are preinstalled by the Travel Document Manufacturer, and which are needed and used in the Personalization process.

36 Phase 3 “Personalisation of the travel document”

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

37 **Application Note 3 (of the ST author):** The referred Personalization Agent can be the card issuer, or a different contributor, depending on the business case, but the intended customer of the TOE is the Card Issuer, who will participate in the process before (until) the *Operational Phase* of the Applet. The Applet Life cycle has the following phases, which differ from the whole TOE Lifecycle:

- IDentity applet

  LOADED (Creation phase)

- IDentity instance

  Personalization Phase

  SELECTABLE (Configuration Phase)

  CONFIGURED (Initialization Phase)

  Operational Phase

  PERSONALIZED

  LOCKED

  BLOCKED

These phases are detailed in the IDentity Applet Administrator’s Guide.[23] These states and phases are presented here because of informational reasons, to serve better understanding.
The Phase of Personalization of the TOE Paltform and Application Parts are the same. At the end of the phase the developer issues the Finish Configuration command. Part of this command is the verification of the authentic profile.
The Personalization Agent Authentication Keys which are loaded at the end of Phase 2 can be changed during this phase by the Personalization Agent

38 The signing of the Document security object by the Document signer [6] finalizes the personalisation of the genuine travel document for the travel document holder. The personalised travel document (together with appropriate guidance for TOE use if

necessary) is handed over to the travel document holder for operational use. This is the end of the Personalization phase.

39 **Application note 3 (taken from [22]):** The Personalization Agent Authentication Keys which are loaded at the end of Phase 2 can be changed here by the Personalization Agent. The Personalization has 2 parts accordingly.

40 **Application note 4 (taken from [22]):** This security target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [6]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives.

The TOE uses symmetric authentication keys for the personalization process. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

41 **Phase 4 “Operational Use”**

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

42 **Application note 5 (taken from [22]):** The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.

43 **Application note 6 (taken from [22]):** The intention of the ST is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

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

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

1.4.3 TOE security functions

46 The following TOEensured security functions are the most significant for its operational use:

47 Only entities (e.g. terminals) possessing authorisation can get access to the user data stored on the TOE and use security functionality of the travel document under control of the travel document holder,

48 Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the entity connected,

49 Averting of inconspicuous tracing of the travel document,

50 Self-protection of the TOE security functionality and the data stored inside.

51 These are described below informally, and in detail in section 7.1.

1.4.4 Features of the Applet

52 This section is informational and intended to provide a general detail about the IDentity applet which is the essential part of this ST. Information in this section does not extend the TOE description or claims of this ST.

53 IDentity applet may be considered as a highly secure and configurable multi-application cryptographic smart card framework for PKI and e-ID purposes.

54 IDentity applet complies with the standards referenced in TOE Overview.

55 The API exposed by IDentity allows fast development of cryptographic supported applications for National ID, ePassport, Enterprise ID, Healthcare, Transportation, and Payment applications.

56 IDentity is designed for the Java Card family of smart card platforms and specifically for the NXP JCOP IC which is certified according to the CC EAL 5+ both the microprocessor and the JCOP OS as well. JCOP 2.4.2 R3 is protected against state of the art attacks.

57 The OS:

- supports ISO 14443-4 Type A, ISO/IEC 7816-4, 8 and 9 standards
- supports PC/SC applications
- provides fast cryptography
- enforces smart memory management
- provides strong security and data integrity mechanisms

1.4.4.1 File System

58 The applet file system is based on the following basic file types:

- directory files, denoted as Dedicated Files (DF)
- application containers, denoted as Application Dedicated Files (ADF)
- generic data files, denoted as Elementary Files (EF)

59 A Dedicated File (DF) represents a directory and may include other objects (except ADFs). A DF contains a set of information dedicated to control the access to this DF and to its included objects. The supported operations on DFs are: creation, selection and deletion.

60 An Application Dedicated File (ADF) is a special kind of Dedicated File having an ISO/IEC 7816-4 Application Identifier (AID) which represents an application and may include other objects. This ST uses the “smart card application” terminology for ADFs

and “applet” terminology for Java Card applets. An ADF contains a set of information dedicated to control the access to this ADF and to its included objects. The supported operations on ADFs are: creation, selection and deletion.

61 Elementary File (EF) is used for data storage. For this reason EFs are also referred to as data files. File access is similar to traditional file systems controlled by access control rules. The IDenity applet supports ISO/IEC 7816-4 transparent EFs only. Transparent files are seen as a single continuous sequence of data units with granularity of one byte. The supported data unit size is one byte. Any data can be accessed by providing an offset and a length. The supported operations on EFs are: read binary, update binary, file selection and deletion. The card is able to import, store and export data in the file system.

62 The Master File (MF) is the root of the file system and is always the initial entry point to the file system. It is implicitly selected after a reset of the card. The MF can be considered to be a special ADF that contains all the files and security data objects.

1.4.4.2 Data Objects

63 A DataObject (DO) represents a byte string available from everywhere in the directory architecture. For example, the serial number is retrieved with this method.

1.4.4.3 Security Environments

64 A Security Environment is involved in the card security context setting (clarifying algorithm or Security Data Object to use) when needed dynamically, or to determine the access control rules of an object / file.

65 The TOE is resistant to physical tampering on the TSF. The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

1.4.4.4 Secure Messaging

66 All commands can be secured.

67 Secure Messaging is managed by the Platform, and can be achieved by two different ways during Perso phase:

- Secure Messaging (GP) - GlobalPlatform Secure Messaging
- Secure Messaging (ISO) – ISO Secure Messaging –, established with standard MUTUAL AUTHENTICATE command using the SK.PERS key.

Supports command chaining and extended length APDUs with data length up to 32K bytes More about the Secure Messaging and the key can be read in the Administrator’s Guide document [23]. Additionally Secure Messaging can be achieved by BAC during the Operational phase.

1.4.4.5 Memory Management

68 All internal file system structures are stored in highly reliable non-volatile memory with guaranteed data integrity. All memory updates are updated using “atomic operations”. This provides safe operations even when power is interrupted.

69 Content of deleted files and objects are cleared (wiped) and returned to the “free memory pool” for reuse.

1.4.4.6 Access Control

70 The TOE provides access control mechanisms that allow the maintenance of different users (Manufacturer, Personalisation Agent, Terminal, Country Verifying Certification Authority,Document Verifier, Domestic Extended Inspection System, Foreign Extended Inspection System).

71 The TOE administers the user roles enabling and restricting capabilities and accesses. The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

72 Before applet instantiation only the role of the Manufacturer exist, who is responsible for the pre-personalization. After that, the applet instantiation requires the Card Issuer or a dedicated Application Provider Role. After the instantiation, during Personalization, the card is prepared to handle the Personalization Agent and the Application Profile Provider Roles. After Personalization, when the card usage started, the applet does not contain predefined roles for the operational phase, because those are contained by the Application Profile.

More about the Management of roles can be read in the Administrator’s Guide document.[23]

73 The access control is administered through authentication mechanisms.

74 Proving the identity of the TOE is supported by the following means:

- Basic Access Control Authentication Protocol
- Passive Authentication Mechanism

75 The TOE prevents reuse of authentication data related to:

- Basic Access Control Authentication Protocol
- Symmetric Authentication Mechanism based on Triple DES

In these the functions the methods are divided between the Platform and the Applet as follows.

Symmetric Authentication Mechanism: Applet: symmetric key permission verification, session counter initialization. Platform: symmetric key cryptography, hashing for session key computation

76 After completion of the BAC Protocol, the TOE accepts commands with correct message authentication code only. These commands must be send via secure messaging using the key previously agreed with the terminal during the last authentication. More about these functions can be read in section 7.1.

1.4.4.7 Cryptography

77 Counter measures are in operation against state of the art attacks such as SPA/DPA.

78 The TOE supports onboard generation of cryptographic keys based on the DH and ECDH compliant as well as generation of RSA and ECDSA key pairs

79 The TOE contains a deterministic random number generator rated K4 (high) according to AIS20 [24] that provides random numbers used authentication. The seed for the deterministic random number generator is provided by the P2 (high) true random number generator of the underlying Platform.

80 The algorithms allowed for the different functions are the following, as is stated in the Users Guide [23]

81 IAS-ECC algorithms:

- PKCS#1 v1.5 SHA-1 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v1.5 SHA-256 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v1.5 SHA-384 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v1.5 SHA-512 (All by the Platform: padding, hashing, digital signature)
- ISO/IEC 9796-2 SHA-1 (All by the Platform: padding, hashing, digital signature)
- ISO/IEC 9796-2 SHA-256 (All by the Platform: padding, hashing, digital signature)
- ISO/IEC 9796-2 SHA-384 (All by the Platform: padding, hashing, digital signature)
- ISO/IEC 9796-2 SHA-512 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v2.1 PSS SHA-1 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v2.1 PSS SHA-256 (Applet padding)
- ECDSA SHA-1 (All by the Platform: padding, hashing, digital signature)
- ECDSA SHA-224 (All by the Platform: padding, hashing, digital signature)
- ECDSA SHA-256 (All by the Platform: padding, hashing, digital signature)
- ECDSA SHA-384 (All by the Platform: padding, hashing, digital signature)
- ECDSA SHA-512 (All by the Platform: padding, hashing, digital signature)

1.4.4.8 Signed Parameters

82 During the Applet life cycle phases after LOADED state the applet becomes the default Application and reaches SELECTABLE state. This is called the Initialization phase. During this phase the following steps are carryed out:

- Applet configuration
- File creation (all control parameters)

Object creation (all control parameters and some usage parameters)

83 Certain configuration and control parameters are signed, and this signature is verified before closing the Initialization phase. Only the unsigned parameters can be changed by the Initializer. This way only those Application Profiles can be applied which are validated by the Developer, and conform to the requirements. The Initialization state can not be finished by reaching the INITIALIZED state, and the Personalization phase can not be started without successful signature verification.

The Administrators Guide [23] 5.2.2. contains more about this topic.

1.4.4.9 Write once behaviour

84 The personalization of certain Data Object Usage Parameters is restricted to write once during the Personalization Phase. This way the value of certain Data Object Usage Parameters can be enforced by the Application Profile (e.g. 'Algorithm to compulsory use'). Note that after personalization – i.e. the applet is in Operational Phase – write once behaviour is not affective any more.

1.4.4.10 Performance

85 IDentity applet supports T=0 and T=1 protocol in contact mode, with speed of up to 223200 bit/s, and T=CL protocol in contactless mode, with speed up to 848 kbit/s.

1.4.4.11 Secure management of the Applet run

86 The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets of the TOE as well as temporarily stored hash values for data to be signed.

87 The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information.

1.4.4.12 Platform-ensured security functions

88 There are security functions which are ensured fully by the Platform, these are covered by TSF_Platform.

2 Conformance Claims

2.1 CC Conformance Claim

89
- This security target claims conformance to
- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012, [3]

as follows

- Part 2 extended, (see Chapter 5 Extended components definition)
- Part 3 conformant.

90 The

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

has to be taken into account.

2.2 PP Claim

91 This ST claims strict conformance to the following Protection Profile:

Title: Protection Profile — Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP)

Sponsor: Bundesamt für Sicherheit in der Informationstechnik

CC Version: 3.1 (Revision 2)

Assurance Level: The minimum assurance level for this PP is EAL4 augmented.

General Status: Final

Version Number: 1.10

Registration: BSI-CC-PP-0055

Keywords: ICAO, machine readable travel document, basic access control

2.3 Package Claim

92 This ST is conforming to assurance package EAL4 augmented with ALC_DVS.2 defined in CC part 3 [3].

2.4 Conformance rationale

92 The security target claims **strict conformance** to one PP. ([22])

93 The Target of Evaluation (TOE) is contactless/contact smart card with ePassport application as programmed according to ICAO Technical Report [6]. The Security Target refers to the eMRTD compliant configurations of the IDentity applet. The IDentity applet is a Java Card Application used exclusively on the NXP JCOP 2.4.2. R3 Platform, which is a CC EAL5+ certified product.

So the TOE is **consistent** with the **TOE type** in the PP.

94 The **security problem definition** of this security target is **consistent** with the statement of the security problem definition in the PP, as the security target claims strict conformance to the PP and no other assumptions, threats, organizational security policies are added.

95 The **security objectives** of this security target are **consistent** with the statement of the security objectives in the PP as the security target claims strict conformance to the PP. There is no added security objectives.

96 The **security requirements** of this security target are **consistent** with the statement of the security requirements in the PP as the security target claims strict conformance to the PP. No further security functional requirement is added in this security target. All assignments and selections of the security functional requirements are defined in the PP section 6.1 and in this security target section 6.1.

2.5 Statement of compatibility

2.5.1 Security Functionalities

97 The following table contains the security functionalities of the Platform ST and of this ST, showing which Functionality correspond to the platform ST and which has no corresspondence. This statement is compliant to the requirements of [16].

98 A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for this ST

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant	Not relevant	Remarks
SF.AccessControl	TSF_AccessControl	X		enforces the access control
SF.Audit	TSF_Platform	X		Audit functionality
SF.CryptoKey	TSF_CryptoKey_MRTD	X		Cryptographic key management
SF.CryptoOperation	TSF_Platform, TSF_AppletParameters_Sign	X		Cryptographic operation Used by calling Platform Security Functionalities
SF.I&A	TSF_Authenticate	X		Identification and authentication
SF.SecureManagement	SF_SecureManagement_MRTD	X		Secure management of TOE resources
SF.PIN	TSF_AccessControl	X		PIN management Used by calling Access Control TSF
SF.LoadIntegrity	TSF_Platform, TSF_AppletParameters_Sign		X	Package integrity check
SF.Transaction			X	Transaction management
SF.Hardware:	TSF_Platform	X		TSF of the underlying Platform Used by calling Platform Security Functionalities
SF.CryptoLib:	TSF_Platform	X		TSF of the certified crypto library Used by calling

				Platform Security Functionalities

Table 2 Classification of Platform-TSFs

99 All listed TSFs of the Platform-ST are relevant for this ST.

100 **Application note 5 (by the ST author)** The TSF_Platform Security functionality in the above list represents functionalities which are not directly used in the IDentity Applet, they are implicitly invoked by calls to the platform, respectively the JCOP operating system. These functions are called altogether as TSF_Platform.

2.5.1.1 Threats

101 The following threats of this ST are directly related to JCOP Platform functionality:

- T.Phys-Tamper
- T.Malfunction
- T.Abuse-Func
- T.Information_Leakage
- T.Forgery

102 These threats will be mapped to the following Platform-ST threats:

- T.PHYSICAL
- T.RND
- T.CONFID-APPLI-DATA
- T.INTEG-APPLI-DATA
- T.RESOURCES

103 The following table shows the mapping of the threats.

This ST		T.Phys-Tamper	T.Malfunction	T.Information_Leakage	T.Forgery
Platform ST	T.PHYSICAL	X			
	T.CONFID-APPLI-DATA			X	
	T.INTEG-APPLI-DATA				X
	T.RND		X		
	T.RESOURCES		X		

Table 3 Mapping of Threats

104 The T.Phys-Tamper matches to T.PHYSICAL, as physical TOE interfaces like emanations, probing, environmental stress and tampering are used to exploit vulnerabilities.

105 The T.Malfunction matches T.RND and T.RESOURCES because these are the threats which may lead to a malfunction of the hardware or the Embedded Software by applying environmental stress in order to deactivate or modify security features or functionality of the TOE hardware or to circumvent, deactivate or modify security functions of the TOE's Embedded Software.

106 T.Information_Leakage matches T.CONFID-APPLI-DATA as physical TOE interfaces like emanations, probing, environmental stress and tampering could be used to exploit exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data.

107 T.Forgery matches T.INTEG-APPLI-DATA because if an attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the inspection system then the listed threats of the Platform-ST could be relevant.

108 The following threats:

- T.CONFID-JCS-CODE
- T.CONFID-JCS-DATA
- T.DELETION
- T.EXE-CODE.1
- T.EXE-CODE.2
- T.EXE-CODE-REMOTE
- T.INTEG-APPLI-CODE
- T.INTEG-APPLI-CODE.LOAD
- T.INTEG-APPLI-DATA.LOAD
- T.INTEG-JCS-CODE
- T.INTEG-JCS-DATA

- T.NATIVE
- T.OBJ-DELETION
- T.SID.1
- T.SID.2
- T.SEC_BOX_ORDER
- T.OS_OPERATET.INSTALL

have no corresponde to the treaths of this ST. They are assessed, and found that there is also no contradiction related to this ST.

2.5.2 OSPs

109 None of the OSPs of this ST are applicable to the JCOP Platform and therefore not mappable for the Platform-ST.

110 The OSP-s from the Platform ST OSP.VERIFICATION and OSP.PROCESS-TOE does not deal with any additional security components.

2.5.3 Assumptions

111 The Assumptions of the Platform ST are categorized according to the [25], as IrPA, CfPA and SgPA. There is also a comment column with respective remarks.

Assumption	Classification of assumptions	Comment
A.APPLET	CfPA	The Java Card specification explicitly "does not include support for native methods" ([28], §3.3) outside the API.
A.VERIFICATION	CfPA	The first place to fulfil the assumption is connected to the Life-cycle of the TOE, the Applet is loaded on the ROM by the manufacturer. There is also OT.Data_Int, OT_Data_conf and OT.Prot_Malfunction to fulfil the Assumption.
A.USE_DIAG	CfPA	A.Insp_Sys, and the related OE.Exam_MRTD and OE.Prot_Logical_MRTD provide the necessary ensurance.
A.USE_KEYS	CfPA	The Assumption A.BAC-Keys and the related objectives OE.BAC-Keys covers this assumption.
A.PROCESS-SEC-IC	CfPA	The objectives OT.Data_Int OT.Data_Conf and OT.Prot_Inf_Leak provide the necessary fulfillment.

Table 4 Mapping of assumptions

2.5.4 Security objectives

112 These Platform-ST objectives can be mapped to this STs objectives as shown in the following table.

Objective from the Platform ST	Objective from this ST
OT.IDENTIFICATION	OT.Identification
OT.OPERATE	OT.Prot_Malfunction
OT.CIPHER	OT.Sens_Data_Conf

OT.SCP.IC	OT.Prot_Phys-Tamper
OT.RND	OT.Prot_Malfunction, OT.Prot_Inf_Leak
OT.KEY-MNGT	OT.Data_Int, OT_Data_Conf, OT.Prot_Inf_Leak, OT.Identification
OT.PIN-MNGT	OT.Data_Int, OT_Data_Conf, OT.Prot_Inf_Leak

Table 5 Mapping of security objectives for the TOE

113 The following Platform-ST objectives are not relevant for or cannot be mapped to the TOE of this ST:

- OT.NATIVE
- OT.REMOTE
- OT.OBJ-DELETION
- OT.DELETION
- OT.SEC_BOX_FW
- OT.GLOBAL_ARRAYS_INTEG
- OT.GLOBAL_ARRAYS_CONFID
- OT.REALLOCATION
- OT.RESOURCES
- OT.ALARM
- OT.MF_FW
- OT.LOAD
- OT.SCP.SUPPORT
- OT.INSTALL
- OT.CARD-MANAGEMENT
- OT.SCP-RECOVERY
- OT.EXT-MEM
- OT.TRANSACTION
- OT.SID
- OT.FIREWALL

cannot be mapped because these are out of scope.

114 The objectives for the operational environment can be mapped as follows:

Objective from the Platform ST	Objective from this ST
OE.USE_DIAG	OE.Passive_Auth_Sign OE.Pass_Auth_Sign , OE.BAC_Keys
OE.USE_KEYS	OE.Passive_Auth_Sign OE.Pass_Auth_Sign , OE.BAC_Keys
OE.PROCESS_SEC_IC	OE.Personalisation
OE.APPLET	OE.Prot_Logical_MRTD, OT.Data_Int, OT.Prot_Abuse-Func OT.Prot_Malfunction
OE.VERIFICATION	OT.Data_Int, OT_Data_Conf and OT.Prot_Malfunction

Table 6 Mapping of security objectives of the environment

115 There is no conflict between security objectives of this ST and the Platform-ST.

2.5.5 Security requirements

116 The Security Requirements of the Platform ST can be mapped as follows:

Platform SFR	Corresponding TOE SFR	Remarks
FDP_ACC.2/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFC.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFF.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/OBJECTS	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/JCRE	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.2/FIREWALL_JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.1	FCS_CKM.1	The FCS_CKM.1 corresponds to the FCS_CKM.1 requirement of the Platform since they contain overlapping requirements.
FCS_CKM.2	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.3	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.4	FCS_CKM.4	The requirements are equivalent (physically overwriting the keys with zeros).
FCS_COP.1	FCS_COP.1/SHA, FCS_COP.1/ENC ,	FCS_COP.1 pf the Platform matches the equivalent SFRs of the Platform.

	FCS_COP.1/AUTH, FCS_COP.1/MAC,	
FDP_RIP.1/ABORT	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/APDU	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/bArray	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/KEYS	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/TRANSIENT	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ROL.1/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FAU_ARP.1	FPT_PHP.3	The Security Alarms requirement FAU_ARP.1 of the Platform corresponds to the FPT_PHP.3 of this ST about physical resistance.
FDP_SDI.2	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPR_UNO.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1	FPT_FLS.1	FPT_FLS.1 matches to the equivalent SFR of the Platform-ST.
FPT_TDC.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_ATD.1/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_UID.2/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_USB.1/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MTD.1/JCRE	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
MT_MTD.3/JCRE	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ITC.2/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_RCV.3/Installer	No Correspondence	Out of scope (Platform functionality)

		No contradiction to this ST
FDP_ACC.2/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.2/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.2.2/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/ODEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/ODEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCO_NRO.2/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFC.2/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFF.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_UIT.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_UID.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/CM	No Correspondence	Out of scope (Platform functionality)

		No contradiction to this ST
FMT_SMR.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FTP_ITC.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FRU_FLT.2/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_PHP.3/SCP	FPT_PHP.3	The FPT_PHP.3 of this ST matches the FPT_PHP.3/SCP of the Platform ST.
FDP_ACC.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_AFL.1/PIN	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FTP_ITC.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FAU_SAS.1/SCP	FAU_SAS.1	FAU_SAS.1 of this ST matches to the equivalent SFR of the Platform-ST.

FCS_RNG.1	FCS_RND.1	FCS_RND.1 of the ST matches FCS_RNG.1 of the Platform-ST when the hardware random number generator is used by the TOE.
FCS_RNG.1/RNG2	FCS_RND.1	FCS_RND.1 of the ST matches FCS_RNG.1/RNG2 of the Platform-ST when the hardware random number generator is used by the TOE.
FPT_EMSEC.1	FPT_EMSEC.1	FPT_EMSEC.1 matches the FPT_EMSEC.1 of the Platform-ST
FDP_ACC.2/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST

Table 7 Mapping of Security requirements

2.5.6 Assurance requirements

117 This ST requires EAL 4 according to Common Criteria V3.1 R4 augmented by ALC_DVS.2.

118 The Platform-ST requires EAL 5 according to Common Criteria V3.1 R4 augmented by: ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2.

119 As EAL 5 covers all assurance requirements of EAL 4 all non augmented parts of this ST will match to the Platform-ST assurance requirements.

2.6 Analysis

120 Overall there is no conflict between security requirements of this ST and the Platform-ST.

3 Security Problem Definition

3.1 Introduction

Assets

121 The assets to be protected by the TOE include the User Data on the MRTD's chip.

122 **Logical MRTD Data**

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [6]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

123 Due to interoperability reasons as the 'ICAO Doc 9303' [6] the TOE described in this security target specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

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

124 The TOE prevents read access to sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG4)[3].

125 A sensitive asset is the following more general one.

126 **Authenticity of the MRTD's chip**

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD.

Subjects

127 This security target considers the following subjects:

128 **Manufacturer**

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

[3] Cf. [1] for details how to access these User data under EAC protection

129 The Manufacturer of the smart card is the NXP company. The ID&Trust IDentity Applet is located on the card.

130 **Personalization Agent**

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (iv) signing the Document Security Object defined in [6].

131 Currently Application Profile Provider is ID&Trust.

132 **Terminal**

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

133 **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. The **Basic Inspection System** (BIS) (i) contains a terminal for the contactless communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

134 **Application note 8:** This security target does not distinguish between the BIS, GIS and EIS because the Active Authentication and the Extended Access Control is outside the scope.

135 **MRTD Holder**

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

136 **Traveler**

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

137 **Attacker**

A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

138 **Application note 9:** An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the

impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

3.2 Assumptions

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

140 **A.MRTD_Manufact MRTD manufacturing on steps 4 to 6**

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

141 **A.MRTD_Delivery MRTD delivery during steps 4 to 6**

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

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

142 **Application note 10 (of the ST Author): The developer shall use the delivery procedures.**

The delivery procedures look like the following:

1. The developers build up a new version of the java card application.
2. They make several backups.
3. After the new version is widely tested, they send it to the NXP Company.
4. The NXP Company makes a hash code from the object code.
5. After the developers accept that the right hash code is sent back, the NXP Company sends an integrated circuit with the java card application on it. This procedure is called ROM coding.
6. The developing procedure starts again until the application meets the requirements.
7. The costumers receive the card and the application included. The card is ready to use.

143 **A.Pers_Agent Personalization of the MRTD's chip**

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

144 PERSONALIZED life cycle state indicates that the applet is in the Operational Phase following the corresponding standard and documented behaviour. During this phase access control for eID functions and data objects are activated and managed according to the pre-defined security attributes and security environments.

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

The Inspection System is 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. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [6]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

146 **Application note 11:** According to [6] the support of the Passive Authentication mechanism is mandatory whereas the the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

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

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [6], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

148 **Application note 12:** When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

149 The ST contains another Assumptions, not defined in the PP, justified by the fact that the TOE is divided to two parts. The TOE Part I according to 1.4.1 is developed by NXP at the NXP sites, which are already certified at the EAL5+ assurance level.

3.3 Threats

150 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.

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

152 **T.Chip_ID Identification of MRTD's chip**

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

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

Asset: Anonymity of user,

153 **T.Skimming Skimming the logical MRTD**

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

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

Asset: confidentiality of logical MRTD data

154 **T.Eavesdropping Eavesdropping to the communication between TOE and inspection system**

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

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

Asset: confidentiality of logical MRTD data

155 **T.Forgery Forgery of data on MRTD's chip**

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 on 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 traveler. 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 traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate MRTDs

Asset: authenticity of logical MRTD data

156 The TOE shall avert the threats as specified below.

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

Adverse action: An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

158 **T.Information_Leakage Information Leakage from MRTD's chip**

Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

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

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality of logical MRTD and TSF data

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

Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data.

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

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

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

Adverse action: An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software. This may be achieved e.g. by

operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

3.4 Organizational Security Policies

161 The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2).

162 **P.Manufact Manufacturing of the MRTD's chip**

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

163 **P.Personalization Personalization of the MRTD by issuing State or Organization only**

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

164 During Personalization Phase special built-in security policy – so called Security Policy (perso) – is applied for all objects created and updated.

Security Policy (perso) is defined as the following:

1. If Protocol configuration byte is '00', Secure Messaging (perso) is not needed.
2. If Protocol configuration byte is other than '00', Secure Messaging (perso) is needed for commands.

165 **P.Personal_Data Personal data protection policy**

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)[4] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [6].

[4] Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by this security target.

166 **Application note 13:** The organizational security policy P.Personal_Data is drawn from the ICAO ‘ICAO Doc 9303’ [6]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

169 **OT.AC_Pers Access Control for Personalization of logical MRTD**

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [6] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

170 **Application note 14:**The OT.AC_Pers implies that

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

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

171 **OT.Data_Int Integrity of personal data**
The TOE must ensure the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

172 **OT.Data_Conf Confidentiality of personal data**

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

173 **Application note 15:** The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the MRTD.The MRTD’s chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys.

The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded

into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [6] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this security target. Thus the read access must be prevented even in case of a successful BAC Authentication.

174 **OT.Identification Identification and Authentication of the TOE**

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

175 **Application note 16:** The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the MRTD". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

176 The following TOE security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

177 **OT.Prot_Abuse-Func Protection against Abuse of Functionality**

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded ICEmbedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE. Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

178 **OT.Prot_Inf_Leak Protection against Information Leakage**

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

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

179 **Application note 17:** This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

180 **OT.Prot_Phys-Tamper Protection against Physical Tampering**
The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with enhanced-basic attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data) with a prior
- reverse-engineering to understand the design and its properties and functions.

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

182 **Application note 18:** A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

4.2 Security Objectives for the Operational Environment

Issuing State or Organization

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

184 **OE.MRTD_Manufact Protection of the MRTD Manufacturing**

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

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

185 **OE.MRTD_ Delivery Protection of the MRTD delivery**

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

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
- origin and shipment details,
- reception, reception acknowledgement,
- location material/information.

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

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

186 **OE.Personalization Personalization of logical MRTD**

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

187 **OE.Pass_Auth_Sign Authentication of logical MRTD by Signature**

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [6].

188 **OE.BAC-Keys Cryptographic quality of Basic Access Control Keys**
The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the ‘ICAO Doc 9303’ [6] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

Receiving State or Organization

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

190 **OE.Exam_MRTD Examination of the MRTD passport book**
The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [6].

191 **OE.Passive_Auth_Verif Verification by Passive Authentication**

The border control officer of the receiving State uses the inspection system to verify the traveller as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the

Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

192 **OE.Prot_Logical_MRTD Protection of data from the logical MRTD**

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

4.3 Security Objective Rationale

193 The following table provides an overview for security objectives coverage.

	OT.AC Pers	OT.Data Int	OT.Data Conf	OT.Identification	OT.Prot Abuse-Func	OT.Prot Inf Leak	OT.Prot Phys-Tamper	OT.Prot Malfunction	OE.MRTD Manufact	OE.MRTD Delivery	OE.Personalization	OE.Pass Auth Sign	OE.BAC- Keys	OE.Exam MRTD	OE.Passive Auth Verif	OE.Prot Logical MRTD
T.Chip-ID				x									x			
T.Skimming			x										x			
T.Eavesdropping			x													
T.Forgery	x	x					x					x		x	x	
T.Abuse-Func					x						x					
T.Information_Leakage						x										
T.Phys-Tamper							x									
T.Malfunction								x								
P.Manufact				x												
P.Personalization	x			x							x					
P.Personal_Data		x	x													
A.MRTD_Manufact									x							
A.MRTD_Delivery										x						
A.Pers_Agent											x					
A.Insp_Sys														x		x
A.BAC-Keys													x			

Table 8 Security Objective Rationale

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

195 The OSP **P.Personalization** “Personalization of the MRTD by issuing State or Organization only” addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD”, and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers**

"Access Control for Personalization of logical MRTD". Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and management of TSF to the Personalization Agent.

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

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

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

199 The threat **T.Forgery** "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRTD passport book according to **OE.Exam_MRTD** "Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** "Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif** "Verification by Passive Authentication".

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

201 The threats **T.Information_Leakage** "Information Leakage from MRTD's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to

Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak** "Protection against Information Leakage", **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot_Malfunction** "Protection against Malfunctions".

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

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

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

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

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

5 Extended Components Definition

207 This security target uses components defined as extensions to CC part 2. Some of these components are defined in [16], other components are defined in the relevant PP0055 [22] protection profile.

5.1 Definition of the Family FAU_SAS

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

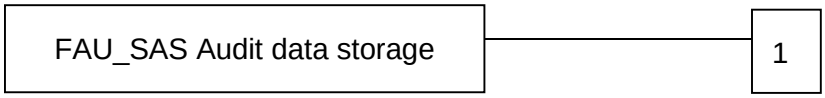
209 The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behavior

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

Component levelling



FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1 There are no management activities foreseen.
Audit:	FAU_SAS.1 There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FAU_SAS.1.1	The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2 Definition of the Family FCS_RND

210 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.

The similar component FIA_SOS.2 is intended for non-cryptographic use.

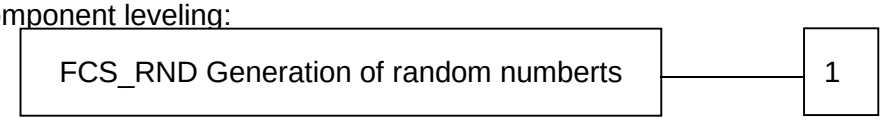
211 The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.
FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

5.3 Definition of the Family FMT_LIM

212 The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to

address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

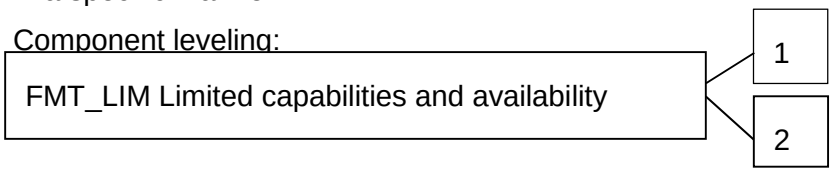
213 The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behavior

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

Component leveling:



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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

214 To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

215 The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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

216 The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: Limited capability and availability policy].

217 **Application note 19:** The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

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

or conversely

(ii) the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

5.4 Definition of the Family FPT_EMSEC

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

219 The family “TOE Emanation (FPT_EMSEC)” is specified as follows.

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMSEC.1	TOE emanation has two constituents:
FPT_EMSEC.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2	Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
Management:	FPT_EMSEC.1 There are no management activities foreseen.
Audit:	FPT_EMSEC.1 There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 Security Requirements

220 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 [1] of the CC. Each of these operations is used in this ST

221 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.

222 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*. Selections filled in by the ST author are denoted as double underlined text and a foot note where the selection choices from the PP are listed.

223 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*. Assignments filled in by the ST author are denoted as double underlined text.

224 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.

225 The definition of the subjects “Manufacturer”, “Personalization Agent”, “Basic Inspection System” and “Terminal” used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined in section 7. The operations “write”, “read”, “modify”, and “disable read access” are used in accordance with the general linguistic usage. The operations “transmit”, “receive” and “authenticate” are originally taken from [2].

226 Definition of security attributes:

security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalisation Agent	Terminal is authenticated as Personalisation uAgent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

6.1 Security Functional Requirements for the TOE

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

6.1.1 Class FAU Security Audit

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

229 **FAU_SAS.1 Audit storage**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer[5] with the capability to store the IC Identification Data [6] in the audit records.

230 **Application note 20:** The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-

[5] [assignment: *authorised users*]
[6] [assignment: *list of audit information*]

personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.1.2 Class Cryptographic Support (FCS)

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

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm [7] and specified cryptographic key sizes 112 bit[8] that meet the following: [6], normative appendix 5[9].

233 **Application note 21**: The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [6], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [6], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

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

235 **FCS_CKM.4 Cryptographic key destruction - MRTD**

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically

[7] [assignment: *cryptographic key generation algorithm*]
[8] [assignment: *cryptographic key sizes*]
[9] [assignment: *list of standards*]

overwriting the keys with zeros[10] that meets the following: none[11].

236 **Application note 22**: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

6.1.2.1 Cryptographic operation (FCS_COP.1)

237 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.

238 **FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation**

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or 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[12] in accordance with a specified cryptographic algorithm: SHA-1[13],[14] and cryptographic key sizes none [15] that meet the following: FIPS 180-2 or other approved *standards* [16],[17].

239 **Application note 23**: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [6].

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ ENC	The TSF shall perform secure messaging (BAC) – encryption and decryption [18] in accordance with a specified

[10] [assignment: *cryptographic key destruction method*]
[11] [assignment: *list of standards*]
[12] [assignment: *list of cryptographic operations*]
[13] [assignment: *cryptographic algorithm*]
[14] [selection: *SHA-1 or other approved algorithms*]
[15] [assignment: *cryptographic key sizes*]
[16] [assignment: *list of standards*]
[17] [selection: *FIPS 180-2 or other approved standards*]
[18] [assignment: *list of cryptographic operations*]

cryptographic algorithm Triple-DES in CBC mode[19] and cryptographic key sizes 112 bit [20] that meet the following: FIPS 46-3 [9] and [6]; normative appendix 5, A5.3 [21].

241 **Application note 24**: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

242 **FCS_COP.1/AUTH Cryptographic operation – Authentication**

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication – encryption and decryption[22] in accordance with a specified cryptographic algorithms Triple-DES[23],[24] and cryptographic key sizes Triple-DES 112bits bits[25],[26] that meet the following: *: FIPS 46-3 [9]..*[27],[28].

243 **Application note 25**: This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

244 **FCS_COP.1/MAC Cryptographic operation – Retail MAC**

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ MAC	The TSF shall perform secure messaging – message authentication code[29] in accordance with a specified

[19] [assignment: *cryptographic algorithm*]
[20] [assignment: *cryptographic key sizes*]
[21] [assignment: *list of standards*]
[22] [assignment: *list of cryptographic operations*]
[23] [assignment: *cryptographic algorithm*]
[24] [selection: *Triple-DES, AES*]
[25] [assignment: *cryptographic key sizes*]
[26] [selection: *112, 128, 168, 192, 256*]
[27] [*assignment: list of standards*]
[28]][selection: *FIPS 46-3 [9]*, *FIPS 197 [12]*]
[29] [assignment: *list of cryptographic operations*]

cryptographic algorithm Retail MAC[30] and cryptographic key sizes 112 bit[31] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [32].

245 **Application note 26**: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

6.1.2.2 Random Number Generation (FCS_RND.1)

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

247 **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 K4 (high) according to AIS20 [24][33].

248 **Application note 27**: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

6.1.3 Class FIA Identification and Authentication

249 **Application note 28**: The Table 2 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [6],normative appendix 5, and [20]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf.FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	either Triple-DES with 112 bit keys or AES with 128 up to 256 bit keys (cf. FCS_COP.1/AUTH)

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

251 **FIA_UID.1 Timing of identification**

[30] [assignment: *cryptographic algorithm*]
[31] [assignment: *cryptographic key sizes*]
[32] [assignment: *list of standards*]
[33] [assignment: *a defined quality metric*]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow 1. to read the Initialization Data in Phase 2 “Manufacturing”, 2. to read the random identifier in Phase 3 “Personalization of the MRTD”, 3. to read the random identifier in Phase 4 “Operational Use”[34] 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.

252 **Application note 29**: The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

253 **Application note 30**: In the “Operational Use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’s chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

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

255 **FIA_UAU.1 Timing of authentication**

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.

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

FIA_UAU.1.1 The TSF shall allow

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

2. to read the random identifier in Phase 3 “Personalization of the MRTD”,

3. to read the random identifier in Phase 4 “Operational Use”[35] on behalf of the user to be performed before the user is authenticated.

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

256 **Application note 31**: The Basic Inspection System and the Personalization Agent authenticate themselves.

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Basic Access Control Authentication Mechanism,

2. Authentication Mechanism based on Triple-DES.[36,37].

259 **Application note 32**: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

260 **Application note 33**: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [6]. In the first step the terminal authenticates itself to the MRTD’s chip and the MRTD’s chip authenticates to the terminal in the second step. In this second step the MRTD’s chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD’s chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

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

---

[35] [assignment: *list of TSF-mediated actions*]
[36] [assignment: *identified authentication mechanism(*s)]
[37] [selection*: Triple-DES, AES or other approved algorithms]*

262 **FIA_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism

2. Symmetric Authentication Mechanism based on Triple-DES,[38,39] to support user authentication.

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

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

the Symmetric Authentication Mechanism with the Personalization Agent Key[40],

2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys [41].

263 **Application note 34**: In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [19] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES. The Personalization Agent could be authenticated by using the symmetric AES-based authentication mechanism or other (e.g. the Terminal Authentication Protocol using the Personalization Key, cf. [19] FIA_UAU.5.2).

264 **Application note 35**: The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

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

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

Hierarchical to: No other components.

---

[38] [assignment: *list of multiple authentication mechanisms*]
39 [selection: *Triple-DES, AES*]
40 [selection: *the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]*]
41 [assignment*: rules describing how the multiple authentication mechanisms provideauthentication*]

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism[42].

267 **Application note 36**: The Basic Access Control Mechanism specified in [6] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

268 **Application note 37**: Note that in case the TOE should also fulfill [19] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

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

270 **Authentication failure handling (FIA_AFL.1)**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when fifteen consecutive [43] unsuccessful authentication attempts occur related to BAC authentication protocol [44].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[45], the TSF shall delay each following authentication attempt until the next successful authentication. [46]

271 **Application note 38**: Application note 35 of [22]: Applied.

[42] [assignment: *list of conditions under which re-authentication is required*]
[43] [selection: *[assignment: positive integer number],an administrator configurable positive integer within [assignment: range of acceptable values]*]
[44] [assignment: *list of authentication events*]
[45] [assignment: *met or surpassed*]
[46] [assignment: *list of actions*]

6.1.4 Class FDP User Data Protection

6.1.4.1 Subset access control (FDP_ACC.1)

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

273 **FDP_ACC.1 Subset access control – Basic Access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the Basic Access Control SFP[47] on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD[48].

6.1.4.2 Security attribute based access control (FDP_ACF.1)

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

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the Basic Access Control SFP[49] to objects based on the following:

1. Subjects:

a. Personalization Agent,

b. Basic Inspection System,

c. Terminal,

2. Objects:

a. data EF.DG1 to EF.DG16 of the logical MRTD,

b. data in EF.COM,

c. data in EF.SOD,

3. Security attributes

a. authentication status of terminals[50].

---

[47] [assignment: *access control SFP*]
[48] [assignment: *list of subjects*, *objects, and operations among subjects and objects covered by the SFP*]
[49] [assignment: *access control SFP*]
[50] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFPrelevant security attributes*, *or named groups of SFP-relevant security attributes*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation

among controlled subjects and controlled objects is allowed:

1. the successfully authenticated Personalization Agent is allowed to

write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,

2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD[51].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[52].

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

1. Any terminal is not allowed to modify any of the EF.DG1 to

EF.DG16 of the logical MRTD.

2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.

3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4[53].

276 **Application note 39**: The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this security target (cf. [19] for details).

6.1.4.3 Inter-TSF-Transfer

277 **Application note 40**: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

279 **FDP_UCT.1 Basic data exchange confidentiality - MRTD**

Hierarchical to: No other components.

[51] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[52] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[53] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1	The TSF shall enforce the Basic Access Control SFP[54] to be able to transmit and receive[55] user data in a manner protected from unauthorised disclosure.

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

281 **FDP_UIT.1 Data exchange integrity - MRTD**

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1	The TSF shall enforce the Basic Access Control SFP[56] to be able to transmit and receive[57] user data in a manner protected from modification, deletion, insertion and replay[58] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[59] has occurred.

6.1.5 Class FMT Security Management

282 **Application note 41**: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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

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

Hierarchical to:	No other components.
Dependencies:	No Dependencies

[54] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[55] [selection*: transmit, receive*]
[56] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[57] [selection*: transmit, receive*]
[58] [selection: *modification, deletion, insertion, replay*]
[59] [selection: *modification*, *deletion, insertion, replay*]

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1. Initialization, 2. Pre-personalization, 3. Personalization[60].

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

286 **FMT_SMR.1 Security roles**

Hierarchical to:	No other components
Dependencies:	FIA_UID.1 Timing of identification.
FMT_SMR.1.1	The TSF shall maintain the roles 1. Manufacturer, 2. Personalization Agent, 3. Basic Inspection System[61]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

287 **Application note 42**: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

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

289 **FMT_LIM.1 Limited capabilities**

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated 2. TSF data to be disclosed or manipulated 3. software to be reconstructed and

[60] [assignment: *list of management functions to be provided by the TSF*]
[61] [assignment: *the authorised identified roles*]

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

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

291 **FMT_LIM.2 Limited availability**

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated 3. software to be reconstructed and 4. substantial information about construction of TSF to be gathered which may enable other attacks.

292 **Application note 43**: The formulation of “Deploying Test Features…” in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy.

Note that the term “software” in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

293 **Application note 44**: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

295 **FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Prepersonalization Data**

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to write [62] the Initialization Data and Prepersonalization Data [63] to the Manufacturer[64].

296 **Application note 45**: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to disable read access for users to[65] the Initialization Data[66] to the Personalization Agent[67].

298 **Application note 46:** According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Prepersonalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to write[68] the Document Basic Access Keys[69] to the Personalization Agent[70].

---

[62] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[63] [assignment: *list of TSF data*]
[64] [assignment: *the authorised identified roles*]
[65] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[66] [assignment: *list of TSF data*]
[67] [assignment: *the authorised identified roles*]
[68] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[69] [assignment: *list of TSF data*]
[70] [assignment: *the authorised identified roles*]

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to read[71] the Document Basic Access Keys and Personalization Agent Keys[72] to none [73].

301 **Application note 47**: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

6.1.6 Class FPT Protection of the Security Functions

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

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

304 **FPT_EMSEC.1 TOE Emanation**

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_EMSEC.1.1	The TOE shall not emit information about IC Power consumption and command execution time [74] in excess of non-useful information[75] enabling access to Personalization Agent Key(s) [76] and none [77]
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users[78] are unable to use the following interface smart card circuit contacts[79]

[71] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[72] [assignment: *list of TSF data*]
[73] [assignment: *the authorised identified roles*]
[74] [assignment: *types of emissions*]
[75] [assignment: *specified limits*]
[76] [assignment: *list of types of TSF data*]
[77] [assignment: *list of types of user data*]
[78] [assignment: *type of users*]
[79] [assignment: *type of connection*]

to gain access to Personalization Agent Key(s)[80] and none[81]

305 **Application note 48:** Application note 45 from [22]: Applied.

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

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

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

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to out-of-range operating conditions where therefore a malfunction could occur, 2. failure detected by TSF according to FPT_TST.1[82]

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

310 **FPT_TST.1 TSF testing**

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up[83] to demonstrate the correct operation of the TSF[84].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[85].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

311 **Application note 49:** Application note 46 of [22]: Applied.

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

---

[80] [assignment: *list of types of TSF data*]
[81] [assignment: *list of types of user data*]
[82] [assignment: *list of types of failures in the TSF*]
[83] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]*
[84] [selection: *[assignment: parts of TSF], the TSF*]
[85] [selection: *[assignment: parts of TSF], TSF data*]

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical intrusions[86] to the IC Hardware[87] by responding automatically such that the TSP is not violated

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

315 **Application note 51**: The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

6.2 Security Assurance Requirements for the TOE

316 The for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following component: ALC_DVS.2.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.AC Pers	OT.Data Int	OT.Data Conf	OT.Identification	OT.Prot Inf Leak	OT.Prot Phys-Tamper	OT.Prot Malfunction	OT.Prot Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					

[86] [assignment: *physical tampering scenarios*]
[87] [assignment: *list of TSF devices/elements*]

FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_RND.1	x	x	x					
FIA_UID.1			x	x				
FIA_AFL.1			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4	x	x	x					
FIA_UAU.5	x	x	x					
FIA_UAU.6	x	x	x					
FDP_ACC.1	x	x	x					
FDP_ACF.1	x	x	x					
FDP_UCT.1	x	x	x					
FDP_UIT.1	x	x	x					
FMT_SMF.1	x	x	x					
FMT_SMR.1	x	x	x					
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA				x				
FMT_MTD.1/INI_DIS				x				
FMT_MTD.1/KEY_WRITE	x	x	x					
FMT_MTD.1/KEY_READ	x	x	x					
FPT_EMSEC.1	x				x			
FPT_TST.1					x		x	
FPT_FLS.1	x				x		x	
FPT_PHP.3	x				x	x		

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

318 The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.
The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [19] by using the symmetric authentication mechanism (FCS_COP.1/ AUTH).
In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions

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

319 The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

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

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

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means

of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/ MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

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

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

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

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

323 The security objective **OT.Prot_Inf_Leak** “Protection against Information Leakage” requires the TOE to protect confidential TSF data stored and/or processed in the MRTD’s chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT_EMSEC.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

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

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

6.3.2 Dependency Rationale

326 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 analyzed, and non-dissolved dependencies are appropriately explained.

327 The Table 10 shows the dependencies between the SFR of the TOE.

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

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

	channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1

	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 10 Dependencies between the SFR for the TOE

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

No. 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material.

Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

No. 2: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

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

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

6.3.3 Security Assurance Requirements Rationale

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

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

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

Dependencies ALC_DVS.2: no dependencies.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

332 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.

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

The dependency analysis in section 6.3.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

334 Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.3.2 Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE summary specification

335 This chapter gives the overview description of the different TOE Security Functions composing the TSF. The mapping in-between the TSFs and SFRs can be found in Table 12.

7.1 TOE Security Functions

7.1.1 TSF_AccessControl

336 The TOE provides access control mechanisms that allow among others the maintenance of different users.

337 The TOE restricts the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. Manufacturer is the only role with the capability to store the IC Identification Data in the audit records. Users of role Manufacturer are assumed default users by the TOE during the Phase 2.

338 Personalisation Agent is the only role with the ability:

- to disable read access for users to the Initialisation Data.
- to write the Document Basic Access Keys.
- to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical travel document after successful authentication.

339 The access control mechanisms ensure that only authenticated Extended Inspection System with the Read access to

- EF.DG3 (Fingerprint) is allowed to read the data in EF.DG3 of the logical travel document.
- EF.DG4 (Iris) is allowed to read the data in EF.DG4 of the logical travel document.

In order to read access to EF.DG3 and EF.DG4 the TOE uses EAC, which is is not covered by this Security Target.

340 The access control mechanisms ensure that nobody is allowed to read the Document Basic Access Keys and the Personalisation Agent Keys.

341 Any terminal is explicitly denied to modify any of the EF.DG1 to EF.DG16 of the logical travel document.

342 The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

343 All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

344 The TSF provides functionality for the following SFRs:

FDP_ACC.1: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF_AccessControl, the authentication control is provided by TSF_Authenticate.

FDP_ACF.1: It is a requirement about access control and authentication. The access control is provided by TSF_AccessControl, the authentication control is provided by TSF_Authenticate.

FDP_UCT.1: It is a requirement about access control, the access control is provided by TSF_AccessControl.

FDP_UIT.1: It is a requirement about access control for details see the SFR), the access control is provided by TSF_AccessControl

FIA_AFL.1: This SFR requires a detection of unsuccessful authentication attempts. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.1: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.4: The requirement is about authentication, and prevention of reuse of authentication data. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.5: The requirement is about multiple authentication mechanisms. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.6: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.6: The requirement is about re-authentication. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UID.1: The requirement is about identification, and what can be accessed before and after it. It is realized by TSF_Authenticate and TSF_AccessControl.

FMT_MTD.1/KEY_READ: This requirement is about restriction of the ability to read out certain passwords and keys. It is realized by TSF.AccessControl.

FMT_MTD.1/KEY_WRITE: This requirement is about restriction of the ability to to write the Document Basic Access Keys to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FMT_MTD.1/INI_ENA: This requirement is about restriction of the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. The control before the operational phase is provided by TSF_Platform.

FMT_MTD.1/INI_DIS: This requirement is about restriction of the ability to read out the Initialisation Data to the Personalization Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. The control before the operational phase is provided by TSF_Platform.

FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

7.1.2 TSF_Authenticate

345 After activation or reset of the TOE no user is authenticated.

346 TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication.

347 The TOE contains a deterministic random number generator rated K4 (high) according to AIS20 [20] that provides random numbers used authentication. The seed for the deterministic random number generator is provided by the P2 (high) true random number generator of the underlying Platform.

348 Proving the identity of the TOE is supported by the following means:

- Basic Access Control Authentication Mechanism
- Passive Authentication Mechanism

349 The TOE prevents reuse of authentication data related to:

- Basic Access Control Authentication Mechanism
- Symmetric Authentication Mechanism based on Triple-DES

350 Personalisation Agent authenticates himself to the TOE by use of the Personalisation Agent Keys with the following cryptographic mechanisms:

- Symmetric Authentication Mechanism

351 After completion of the BAC Protocol, the TOE accepts commands with correct message authentication code only. These commands must have been sent via secure messaging using the key previously agreed with the terminal during the last authentication.

352 The TSF provides functionality for the following SFRs:

FDP_ACC.1: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF_AccessControl, the authentication control is provided by TSF_Authenticate.

FDP_ACF.1: It is a requirement about access control and authentication. The access control is provided by TSF_AccessControl, the authentication control is provided by TSF_Authenticate.

FIA_AFL.1: This SFR requires a detection of unsuccessful authentication attempts. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.1: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.4: The requirement is about authentication, and prevention of reuse of authentication data. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.5: The requirement is about multiple authentication mechanisms. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.5: The requirement is about multiple authentication mechanisms. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UAU.6: The requirement is about re-authentication. It is realized by TSF_Authenticate and TSF_AccessControl.

FIA_UID.1: The requirement is about identification, and what can be accessed before and after it. It is realized by TSF_Authenticate and TSF_AccessControl.

FMT_MTD.1/INI_ENA: This requirement is about restriction of the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. The control before the operational phase is provided by TSF_Platform.

FMT_MTD.1/INI_DIS: This requirement is about restriction of the ability to read out the Initialisation Data to the Personalization Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. The control before the operational phase is provided by TSF_Platform.

FMT_MTD.1/KEY_WRITE: This requirement is about restriction of the ability to to write the Document Basic Access Keys to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FMT_MTD.1/KEY_WRITE: This requirement is about restriction of the ability to to write the Document Basic Access Keys to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

7.1.3 TSF_SecureManagement_MRTD

353 The life cycle of TOE is split up in several phases. Phase 4 – „Operational Use" is different from all prior phases, when the TOE is still in the secure environment and Test Features are available. During start-up of the TOE the decision for one of the various operation modes is taken dependent on phase identifiers. The decision of accessing a certain mode is defined as phase entry protection. The phases follow also a defined and protected sequence. The sequence of the phases is protected by means of authentication.

354 Test features of the TOE are not available for the user in Phase 4. Deploying test features after TOE delivery does not allow User Data to be manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks.

355 The TSF provides functionality for the following SFRs:

FMT_LIM.1: The requirement is about restricting capabilities after TOE delivery, which is provided by TSF_SecureManagement_MRTD.

FMT_LIM.2: The requirement is about restricting availibilities after TOE delivery, which is provided by TSF_SecureManagement_MRTD.

FMT_SMF.1: The requirement is about performable management functions, which is provided by TSF_Securemanagement_MRTD.

7.1.4 TSF_CryptoKey_MRTD

356 A successfully authenticated Personalisation Agent is allowed to change the Personalisation Agent Keys.

357 The TOE supports overwriting the cryptographic keys with zero values as follows:

- the BAC Session Keys after detection of an error in a received command by verification of the MAC,
- any session keys before starting the communication with the terminal in a new power-on-session.

358 The TSF provides functionality for the following SFR:

FCS_CKM.1: The SFR requires generation of cryptographic keys. It is realized by TSF_CryptoKey_MRTD, and because it uses Platform functionalities, TSF_Platform.

FCS_CKM.4: Requires the cryptographic key destruction according to a specified cryptographic method. This is realized by TSF_CryptoKey_MRTD.

FCS_COP.1/AUTH: Requires a use of cryptographic operation. It is provided by TSF_CryptoKey_MRTD and TSF_Platform.

FCS_COP.1/ENC: Requires a use of cryptographic operation. It is provided by TSF_CryptoKey_MRTD and TSF_Platform.

7.1.5 TSF_AppletParameters_Sign

359 During the Applet life cycle phases after LOADED state the applet becomes the default Application and reaches SELECTABLE state. This is called the Initialization phase. During this phase the following steps are carryed out:

- Applet configuration
- File creation (all control parameters)
- Object creation (all control parameters and some usage parameters)

360 Certain configuration and control parameters are signed, and this signature is verified before closing the Initialization phase. Only the unsigned parameters can be changed by the Initializer. This way only those Application Profiles can be applied which are validated by the Developer, and conform to the requirements. The Initialization state can not be finished by reaching the INITIALIZED state, and the Personalization phase can not be started without successful signature verification.

361 These signatures can be verified during the whole Applet life-cycle, thus the non-authorized changed become detectable by applying this SF.

362 The TSF provides functionality for the following SFRs:

FPT_FLS.1: The requirement requires the preservation of a secure state when detecting failures. This is provided by TSF_AppletParameters_Sign and TSF_Platform.

FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is provided by TSF_AppletParameters_Sign and TSF_Platform.

7.1.6 TSF_Platform

363 There are security functionalities based on the security functionalities of the certified cryptographic library and the certified IC Platform. This TSF covers those functionalities.

364 The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.

365 The TOE is resistant to physical tampering on the TSF. This is managed by the Platform. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

366 The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF the TOE preserves a secure state. Both the Applet and the Platform manage this.

367 The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets of the TOE as

well as temporarily stored hash values for data to be signed. Both CRC and HASH function are calculated by the Platform

368 The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information.

369 The TSF provides functionality for the following SFRs:

FAU_SAS.1: The SFR requires audit capabilities, which are provided by TSF_Platform.

FCS_CKM.1: The SFR requires generation of cryptographic keys. It is realized by TSF_CryptoKey_MRTD, and because it uses Platform functionalities, TSF_Platform.

FCS_COP.1/ENC: Requires a use of cryptographic operation. It is provided by TSF_CryptoKey_MRTD and TSF_Platform.

FCS_COP.1/AUTH: Requires use of cryptographic operation. It is provided by TSF_CryptoKey_MRTD and TSF_Platform.

FCS_COP.1/MAC: Requires use of operation which is provided by TSF_Platform.

FCS_COP.1/SHA: Requires use of operation which is provided by TSF_Platform.

FMT_MTD.1/INI_ENA: This requirement is about restriction of the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. The control before the operational phase is provided by TSF_Platform.

FMT_MTD.1/INI_DIS: This requirement is about restriction of the ability to read out the Initialisation Data to the Personalization Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. The control before the operational phase is provided by TSF_Platform.

FCS_RND.1: Requires use of operation which is provided by TSF_Platform.

FPT_EMSEC.1: Requires use of operation which is provided by TSF_Platform.

FPT_FLS.1: The requirement requires the preservation of a secure state when detecting failures. This is provided by TSF_AppletParameters_Sign and TSF_Platform.

FPT_PHP.3: Requires resistance to physical manipulation and probing to the Platform. This is realized by the TSF_Platform.

FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is provided by TSF_AppletParameters_Sign and TSF_Platform.

7.2 Assurance Measures

370 This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 6.3.

371 The following table lists the Assurance measures and references the corresponding documents describing the measures.

Assurance measures	Description

AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the Userguide documentation, the AdminGuide document and in the InitandConf documentation.
AM_ALC	The life-cycle support of the TOE during its development and maintenance is described in the life-cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

Table 11 References of Assurance measures

7.3 Fulfilment of the SFRs

372 The following table shows the mapping of the SFRs to security functions of the TOE.

TOE SFR / Security Function	TSF_AccessControl	TSF_Authenticate	TSF_SecureManagement_MRTD	TSF_Cryptokey_MRTD	TSF_Appletparameters_sign	TSF_Platrform
FAU_SAS.1						X
FCS_CKM.1/				X		X
FCS_CKM.4				X		
FCS_COP.1/SHA						X
FCS_COP.1/ENC				X		X
FCS_COP.1/AUTH				X		X
FCS_COP.1/MAC						X
FCS_RND.1						X
FIA_AFL.1	X	X				
FIA_UID.1	X	X				
FIA_UAU.1	X	X				
FIA_UAU.4	X	X				
FIA_UAU.5	X	X				
FIA_UAU.6	X	X				
FDP_ACC.1	X	X				
FDP_ACF.1	X	X				
FDP_UCT.1	X					
FDP_UIT.1	X					
FMT_SMF.1			X			
FMT_SMR.1	X	X				
FMT_LIM.1			X			

FMT_LIM.2			X			
FMT_MTD.1/INI_ENA	X	X				X
FMT_MTD.1/INI_DIS	X	X				X
FMT_MTD.1/KEY_READ	X					
FMT_MTD.1/KEY_WRITE	X	X				
FPT_EMSEC.1						X
FPT_FLS.1					X	X
FPT_PHP.3						X
FPT_TST.1					X	X

Table 12 Mapping of SFRs to mechanisms of TOE

7.3.1 Correspondence of SFR and TOE mechanisms

373 Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 7.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

7.4 Rationale for PP Claims

374 This security target is conformant to the claimed PP [22]. Additionally, the Passive Authentication Mechanism and the key generation of the Active Authentication keys on the TOE are included in the TOE.

8 Bibliography

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

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

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

[5] Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik

[6] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization

[7] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

[8] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[9] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46- 3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[10] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[11] Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

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

[13] Certicom Research: SEC 1: Elliptic Curve Cryptography, September 20, 2000, Version 1.0

[14] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998

[15] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2002

[16] 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

[17] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

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

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

[20] 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)

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

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

[23] ID&Trust IDentity Applet Initialization and configuration Version 3.1.05

ID&Trust IDentity Applet Administrator's Guide Version 3.1.06

ID&Trust IDentity Applet User's Guide Version 3.1.12

[24] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 02.12.1999

[25] NSCIB-CC-13-13-37760-CR NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 Certification Report by TÜV Rheinland Nederland B.V. , 2013 August 12th.

[26] NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 Security Target Rev. 01.02 — 2nd August 2013 NSCIB-CC-13-37760

[27] NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 Security Target Lite, Rev. 00.02 — 2nd August 2013, NSCIB-CC-13-37760