Athena IDProtect Duo v5
ICAO BAC optional AA

-

Athena IDProtect Duo v5 Java Card
on Inside Secure AT90SC28880RCFV Microcontroller
embedding ICAO applet

-

Public Security Target

Version 2.2

January 6, 2014

athena
Smartcard

Contents

List of Tables

List of Figures

1. ST Introduction

1.1. ST Identification

ST title	**Athena IDProtect Duo v5 – ICAO BAC optional AA on Inside Secure AT90SC28880RCFV**
Authors	Athena Smartcard, Inc.
General Status	Final version
ST reference	FV-IDDS-03
ST Version Number	2.2
Date of production	6 January 2014
TOE Reference	ROM Mask Reference: “Aries_AT90SC28880RCFV_002” EEPROM Mask Reference: “Aries_AT90SC28880RCFV_002_P4_F2” IASECC Applet Athena Smartcard Solutions, Inc. AID A0000002471001 Version 0004 Build 0010 ROM Code reference: “v0004 b0010” EEPROM Code Reference: “vF204 b0010” IDProtect Athena Smartcard Solutions, Inc. Release Date 1245 Release Level 0002 ROM Code reference: “Aries_AT90SC28880RCFV_002” EEPROM Code Reference: “Aries_AT90SC28880RCFV_002_P4” AT90SC28880RCFV Inside Secure Revision J Identification Number AT59U05 Certificate ANSSI – 2012/22-M01 Ad-X Inside Secure Version 00.03.12.00 Certified with the microcontroller
Common Criteria	CC version 3.1 Part 1: CCMB 2012-09-001 revision 4 [1] Part 2: CCMB 2012-09-002 revision 4 [2] Part 3: CCMB 2012-09-003 revision 4 [3]
PP Claim	Protection Profile [4] Machine Readable Travel Document with “ICAO Application”, Basic Access Control Version 1.10 Assurance level CC 3.1 (Revision 2) EAL 4 augmented Prepared By BSI, Germany Identification BSI-CC-PP-0055
Updates	Updates to ANSSI-CC-2013/36 : - IDProtect Corrective Patch : P2 ⇨ P4 - AT90SC28880RCFV Revision: Rev I ⇨Rev J

1.2. Composite TOE

In this Security Target, the name of the composite TOE developer (Athena Smartcard Solutions, Inc.) will be referenced as 'Athena'.

IDProtect with associated ICAO applet are embedded on Inside Secure AT90SC28880RCFV IC.

The composition analysis conducted in this section will use the words Platform to designate the Inside Secure AT90SC28880RCFV IC [6, 7], Application to designate the two software components Athena IDProtect Duo and Athena ICAO Applet, and Composite Product to designate the TOE.

According to the Composite product documentation [14], the different roles considered in the composition activities are associated as follows:

Platform Developer	Inside Secure
Platform Evaluator	Leti
Platform Certification Body	ANSSI
Application Developer	Athena
Composite Product Integrator	Inside Secure
Composite Product Evaluator	CEACI Thales
Composite Product Certification Body	ANSSI
Composite Product evaluation Sponsor	Athena

See composition requirements coverage:

[R1] Platform was evaluated to CC EAL 5+ [9] according to BSI-PP-0035-2007 [8] and Composite Product ST relies on this claim.

[R2] Platform Security Target [10] is available.

[R3] Evaluated versions of the Platform and Application are exposed here in section 1.1.

[R4] Integration evidences are provided as part of the process.

[R5] Integration is guided by delivery procedures enforced by Athena and Inside Secure.

[R6] Integration process involves all configuration parameters provided by Athena.

[R7] Integration data and processing are tracked by Athena.

[R8] Application development process incorporates the Platform User Guide as technical input.

[R9] EAL 5+ certification of the Platform provides:

- List of applicable Technical Guides, Application Notes and Errata Sheets
- Certified Platform ETR
- Platform Certification Report [9]

[R10] TOE Test Plan describes validation of the Application on Platform dedicated emulator.

[R11] TOE Test Plan describes validation of the Application on the Platform.

[R12] Platform certification includes testing evaluation.

[R13] Platform samples are delivered by Inside Secure to TOE's evaluator for testing purpose.

[R14] Composite Product samples are delivered by Inside Secure to TOE's evaluator for penetration testing purpose.

[R15] Platform open samples are delivered by Inside Secure to TOE's evaluator for testing purpose.

[R16] EAL 5+ certification of the Platform provides Certified Platform ETR and Certification Report.

1.3. TOE Overview

The protection profile [4] defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). This ST extends this PP to contact, contactless and dual interface smartcard modules. It addresses the advanced security methods Basic Access Control (BAC) and Extended Access Control (EAC) and Chip Authentication similar to the Active Authentication in the Technical reports of 'ICAO Doc 9303' [15].

Athena IDProtect Duo v5 passport application is configurable in BAC or EAC chip authentication modes, with or without Active Authentication [15]. Also, it supports contact and contactless communication.

This ST applies to the BAC configuration with or without Active Authentication.

Note that there is no non-TOE hardware/software/firmware that is required by the TOE.

1.3.1. TOE Definition

The Target of Evaluation (TOE) is the integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [15] and providing the BAC and EAC according to the 'ICAO Doc 9303' [15] and BSI TR-03110 [16], respectively.

The TOE comprises at least:

- the circuitry of the MRTD's chip (AT90SC28880RCFV IC [6])
- the IC Dedicated Software with the parts IC Dedicated Test and Support Software (Ad-X [7])
- the IC Embedded Software (IDProtect Operating System)
- the MRTD application (ICAO applet)
- the associated guidance documentation

1.3.2. TOE usage and security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this TOE 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 MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [15]. These security measures include the binding of the MRTD's chip to the passport book.

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

The ICAO defines the baseline security methods (Passive Authentication) and the optional advanced security methods (BAC to the logical MRTD, Active Authentication of the MRTD's chip, EAC to the logical MRTD and the Data Encryption of additional sensitive biometrics) as optional security measure in the 'ICAO Doc 9303' [15]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This TOE addresses the protection of the logical MRTD (i) in integrity by write only- once access control and by physical means, and (ii) in confidentiality by the BAC Mechanism. This TOE does not address EAC (Extended Access Control), and this TOE addresses the AA as an optional security mechanism.

1.4. TOE Description

1.4.1. General

The TOE is an MRTD IC where application software is masked in ROM and that can be assembled in a variety of form factors. The main form factor is the electronic passport, a paper book passport embedding a contactless module:

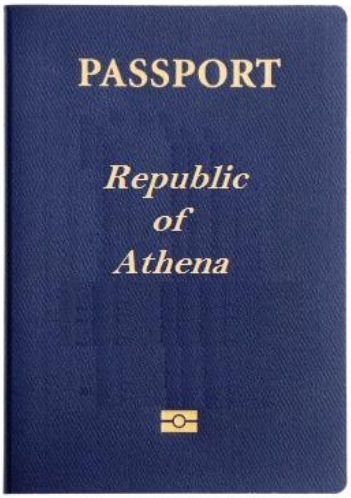


Figure 1 – TOE Main Form Factor *(photo non-contractual)*

The followings are an informal and non-exhaustive list of example graphic representations of possible end products embedding the TOE:

- Contactless interface cards and modules
- Dual interface cards and modules
- Contact only cards and modules
- SOIC8 package
- QFN44 package
- Chip on Board (PCB)

The scope of this TOE is covered in section 1.3.1 above.

The TOE is linked to a MRTD reader via its HW and physical interfaces.

- The contactless type interface of the TOE smartcard is ISO/IEC 14443 compliant.
- The optional contact type interface of the TOE smartcard is ISO/IEC 7816 compliant.
- The optional interfaces of the TOE SOIC-8 are ISO 9141 compliant.
- The optional interfaces of the TOE QNF-44 are JEDEC compliant.

There are no other external interfaces of the TOE except the ones described above.

The antenna and the packaging, including their external interfaces, are out of the scope of this TOE.

The TOE may be applied to a contact reader or to a contactless reader, depending on the external interface type(s) available in its form factor. The readers are connected to a computer and allow application programs (APs) to use the TOE.

1.4.2. MRTD's chip

For this TOE the MRTD is viewed as unit of

(1) The **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
   a. the biographical data on the biographical data page of the passport book,
   b. the printed data in the Machine Readable Zone (MRZ) and
   c. the printed portrait.

(2) The **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [15] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
   a. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   b. the digitized portraits (EF.DG2),
   c. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,
   d. the other data according to LDS (EF.DG5 to EF.DG16) and
   e. the Document security object.

This TOE addresses the protection of the logical MRTD:

- in integrity by write-only-once access control and by physical means, and
- in confidentiality by the Extended Access Control Mechanism.

This TOE addresses the Chip Authentication described in [16] as an alternative to the Active Authentication stated in [15].

1.4.3. Basic Access Control

The confidentiality by Basic Access Control (BAC) is a mandatory security feature that is implemented by the TOE. For BAC, the inspection system

(i) reads optically the MRTD,
(ii) authenticates itself as an 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 [15], normative appendix 5.

In compliance with the ICAO Basic protection profile [4], this ST requires the TOE to implement the Chip Authentication defined in [16]. The Chip Authentication prevents data traces described in [15], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps:

(i) the inspection system communicates by means of secure messaging established by Basic Access Control,
(ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object,
(iii) the inspection system generates an ephemeral key pair,
(iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and
(v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys).

The Chip Authentication requires collaboration of the TOE and the TOE environment.

1.4.4. Active Authentication

This TOE offers an optional mechanism called Active Authentication and specified in [16] section 1.2. This security feature is a digital security feature that prevents cloning by introducing a chip-individual key pair:

(i) The public key is stored in data group DG15 and thus protected by Passive Authentication.

(ii) The corresponding private key is stored in secure memory and may only be used internally by the MRTD chip and cannot be read out.

Thus, the chip can prove knowledge of this private key in a challenge-response protocol, which is called Active Authentication. In this protocol the MRTD chip digitally signs a challenge randomly chosen by the inspection system. The inspection system recognizes that the MRTD chip is genuine if and only if the returned signature is correct. Active Authentication is a straightforward protocol and prevents cloning very effectively, but introduces a privacy threat: Challenge Semantics (see Appendix F for a discussion on Challenge Semantics).

1.5. TOE Limits

The TOE boundaries are the following:

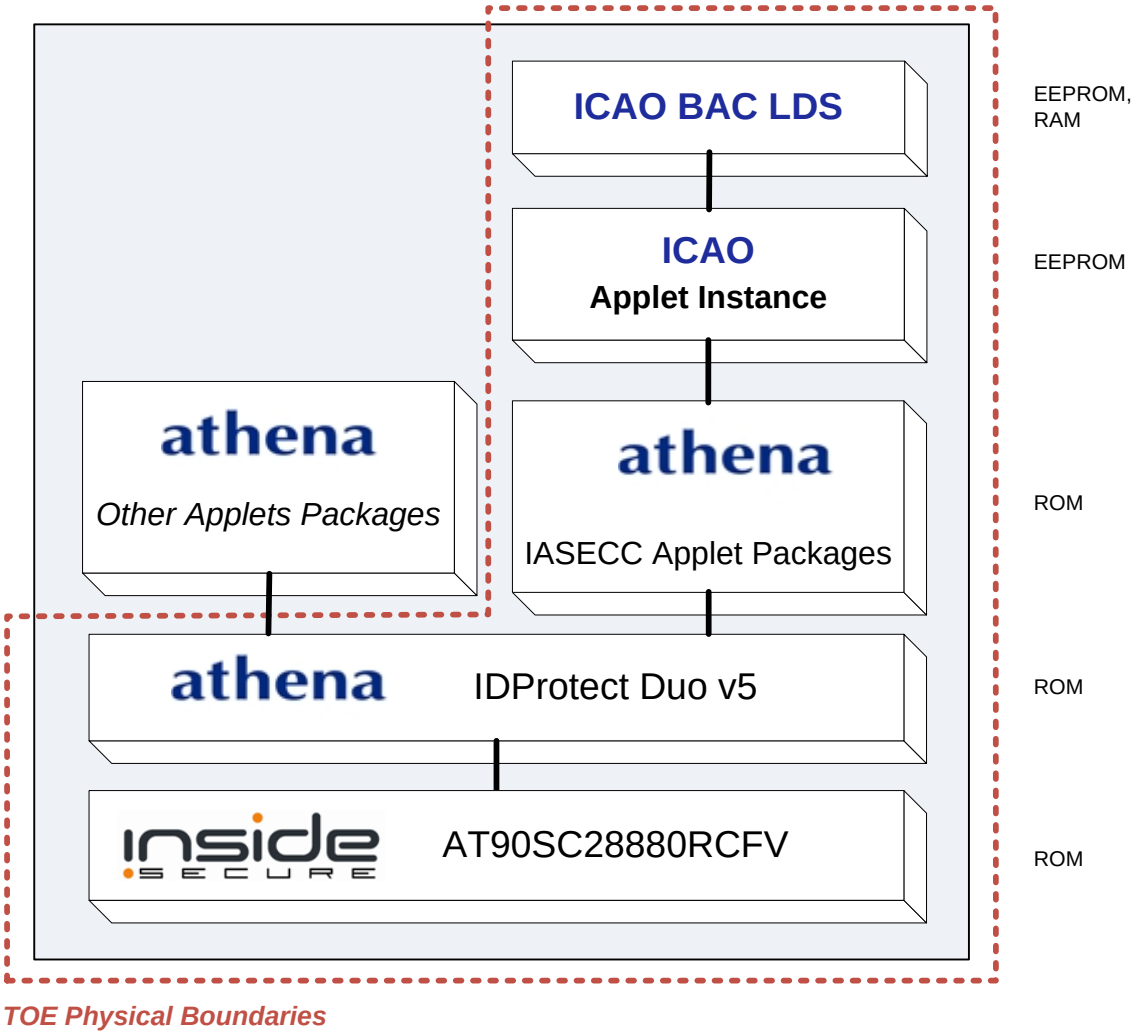


Figure 2 – TOE Description

Three Athena applet packages are present on the chip: IASECC applet, LASER applet and MiniDriver applet. No other Java Card applet package is present in the chip. Athena LASER and MiniDriver applet packages are not in the scope of this TOE.

The IASECC package could be instantiated into an ICAO applet instance or an IAS-ECC applet instance. Only the ICAO applet instance is part of the TOE, and no other instance should be installed.

IDProtect Operating System enforces separation of the data between the applets and associated packages imposing logical separation of data using the Java Card Firewall [11-JCRE].

Athena IDProtect is a GlobalPlatform 2.1.1 and Java Card 2.2.2 compliant Operating System that provides applets with standard services as defined in the related GlobalPlatform [13] and Java Card specifications [12].

The hardware platform on which the Operating System is implemented is the Inside Secure AT90SC28880RCFV IC. This IC is certified according to CC EAL 5+ [9] with the Security Target [10] compliant with BSI-PP-0002-2001 [8].

1.6. TOE Guidance

The TOE guidance comprises the following documentation:

Title	Date	Version
IDProtect Duo v5 – ICAO Manufacturer Manual	*Consult certification report for applicable dates and versions*	
IDProtect Duo v5 – ICAO BAC Preparation Manual		
IDProtect Duo v5 – ICAO BAC Operation Manual		

1.7. TOE lifecycle

The TOE lifecycle is shown in Figure 3.

The integration phase is added to the PP generic lifecycle as this particular TOE requires that card production phase is refined.

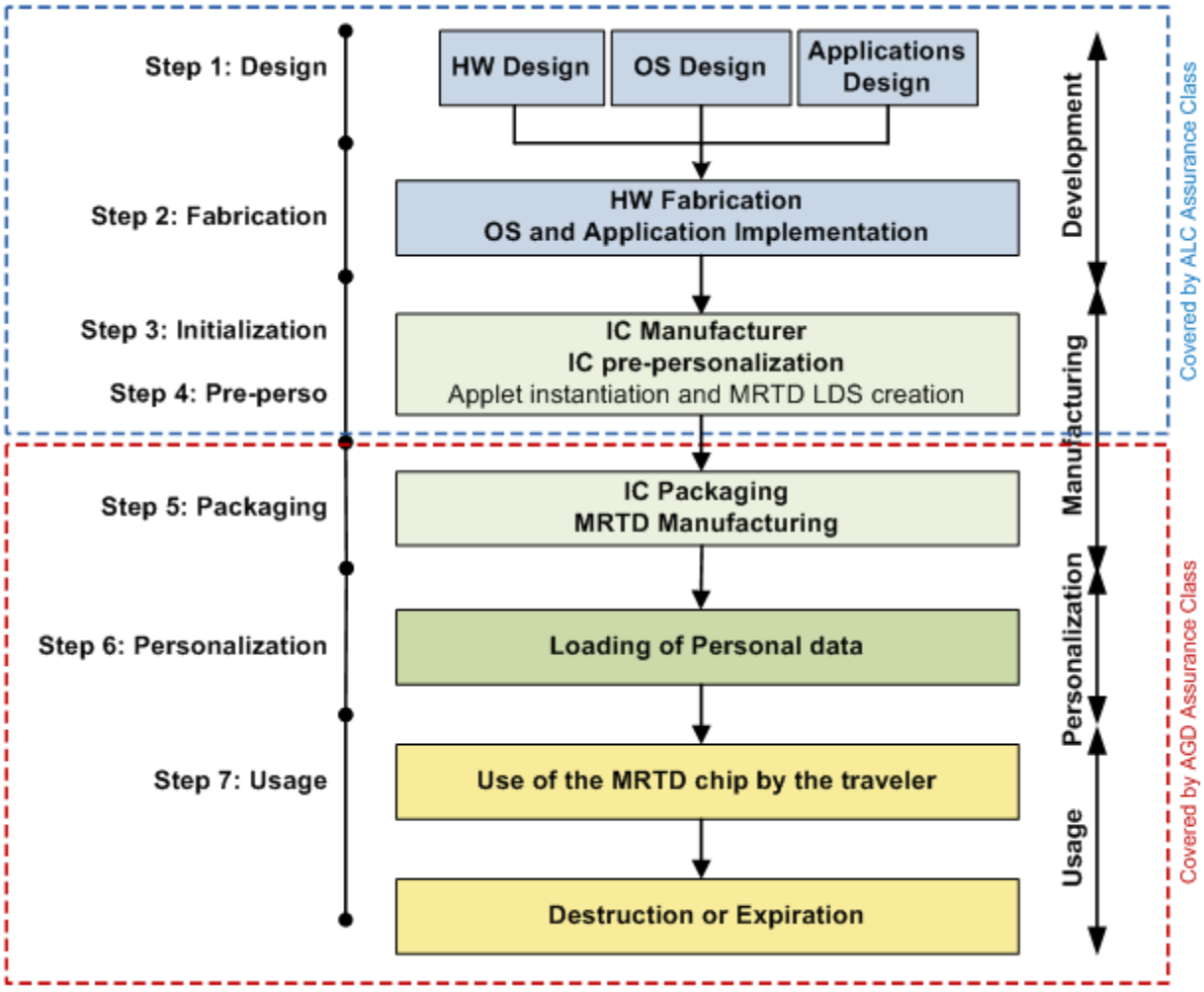


Figure 3 – TOE lifecycle

1.7.1. Phase 1 "Development"

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

HW Design – Inside Secure

(Step 2)
The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

OS Design – Athena Development departments – Cupertino then Los Gatos, US
– Edinburgh then Livingston, Scotland

Application Design – Athena Development departments – Cupertino then Los Gatos, US

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

1.7.2. Phase 2 "Manufacturing"

(Step 3)
In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.
The IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM). Patch mechanism is terminated in this phase.

HW Fabrication and OS & Application implementation – Inside Secure

IC Manufacturing – Inside Secure

The Operating System and applicative parts of the TOE which are developed by Athena are sent in a secure way to Inside Secure for masking in NVM. In addition to the TOE, the mask contains confidential data, knowledge of which is required in order to initialize and personalize the chip. Additional Java Card applets developed by Athena are included in the mask and the corresponding converted files (.cap or.jca) are also provided to Inside Secure.

(Step 4)
During the step Pre-Perso, the MRTD manufacturer

(i) creates the MRTD application and
(ii) equips MRTD's chips with pre-personalization Data.

IC Pre-Personalization – Inside Secure

Creation of the application implies applet instantiation and the creation of MF and ICAO.DF. Card Content Loading and Installing mechanism is terminated in this phase.
The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. Athena or the MRTD Manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

(Step 5)
The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

IC Packaging – Inside Secure

MRTD Manufacturing – Inside Secure

This step corresponds to the integration of the hardware and firmware components into the final product body. The TOE is protected during transfer between various parties. IC Packaging and MRTD Manufacturing are not part of the scope of this TOE.

1.7.3. Phase 3 "Personalization of the MRTD"

(Step 6)
The personalization of the MRTD includes:

- the survey of the MRTD holder's biographical data,
- the enrolment of the MRTD holder biometric reference data,
- the printing of the visual readable data onto the physical MRTD,
- the writing of the TOE User Data and TSF Data into the logical MRTD and
- configuration of the TSF if necessary.

The step 6 is performed by the Personalization Agent and includes but is not limited to the creation of the digital MRZ data (EF.DG1), the digitized portrait (EF.DG2), and the Document security object. The signing of the Document security object by the Document signer [15] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Personalization – 3rd Party Personalization facility

The TOE is protected during transfer between various parties by the confidential information which resides in the card during mask production.
The Personalization phase is not part of the scope of this TOE.

1.7.4. Phase 4 "Operational Use"

Where upon the card is delivered to the MRTD holder and until MRTD is expired or destroyed.

(Step 7)
The TOE is used as MRTD chip by the traveler 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.
The Operational Use phase is not part of the scope of this TOE.

1.8. Features of IDProtect – Informational

Note:	The features described in this section are provided by the IDProtect product family, they are not necessarily Security Functions of the TOE. Please refer to section 7 of this Security Target to find the TOE summary specification.

Java promises write once, run anywhere capability. Athena IDProtect - Athena Java Card technology and GlobalPlatform Operating System - fulfils that promise for the smart card industry.

Athena's IDProtect is built to give you flexibility in the way you work: a blank canvas on which to create smart card products for all market sectors.

Central to Athena IDProtect is its compliance with the Java Card and GlobalPlatform standards; multiple compliant Java Card applets from any source will run securely on Athena IDProtect enabled silicon. Applets can be securely loaded and deleted post issuance thanks to GlobalPlatform compliant Issuer Security Domain implementation. Athena uses its RapidPort architecture to ease the process of porting the system to different silicon platforms, including contactless, meaning it is already available on various devices from leading manufacturers.

1.8.1. GlobalPlatform

IDProtect provides a Card Manager. This is a generic term for the three card management entities of a GlobalPlatform card; the GlobalPlatform Environment, Issuer Security Domain and Cardholder Verification Method Service Provider.

GlobalPlatform 2.1.1	Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange
Atomic Package and Application Deletion	Memory recovered and is reusable
Global PIN	A PIN that may be checked by all applets on a card, using CVM.verify(). Its value is usually set at personalization time
Secure Channel Protocol 01	SCP01 provides mutual authentication; integrity and data origin authentication; confidentiality
Secure Channel Protocol 02	Support for all SCP02 options
Secure Channel Protocol 03	Support for all SCP03 options
Repeated application install failure	The OPEN may keep track of the number of unsuccessful consecutive attempts of the Card Content load and installation process by a particular Application and the total number of such attempts by all applications. Actions may include such defensive measures as the locking or termination of the card
Applications boundary violations	The OPEN may also enable velocity checking against repeated failed attempts by an Application to allocate additional memory beyond its allowed limit as stored in the Open Platform Registry. The OPEN may choose to lock an Application which exhibits such behavior

1.8.2. Java Card

Athena IDProtect Duo v5 is compatible with the following Java Card standards versions [12]:

- Runtime Environment Specification for the Java Card Platform, Version 2.2.2 March, 2006
- Application Programming Interface, Java Card Platform, Version 2.2.2 March, 2006
- Virtual Machine Specification for the Java Card Platform, Version 2.2.2 March, 2006

Data type *int* is optionally supported in the JCVM and is supported in IDProtect.

1.8.3. Security settings

Keys and PINs are stored encrypted	The OS does not store any Keys or PINs in plain text during computation
On card key generation	RSA keys indicated in the Key Pair list may be generated on the card
FIPS 140-2 Level 3	Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules FIPS PUB 140-2
FIPS approved DRBG	IDProtect supports the secure RNG specified in JC API and is FIPS approved
FIPS 140-2 Self Tests	Self tests are performed to check that the HRNG and the DRBG are not stuck and that RSA Keys that are generated by the TOE are a consistent pair.
FIPS 140-2 KAT	Known Answer Tests performed at power up. The cryptographic function tests consist of computing from pre-recorded input data, and comparing the results with pre-recorded answers
FIPS 140-2 Software Integrity	Checks that no FIPS application present in EEPROM (packages) is corrupted. The error detecting code is FIPS approved

1.8.4. Communication

Athena IDProtect Duo v5 provides the following communication features:

- Physical: ISO/IEC 7816- 1 and 2
- Electrical: ISO/IEC 7816- 3 and 4
- Protocol Support:
  - Protocol T=0 with PPS for speed enhancement
  - Protocol T=1 with PPS for speed enhancement with extended APDU length support
  - Contactless with a full support for ISO/IEC 14443 Type B protocol

1.8.5. Cryptography

Athena IDProtect Duo v5 supports the following cryptographic algorithms:

- AES: AES_128, AES_192, AES_256
- DES [19]: Single DES, 2 Key TDES, 3 Key TDES
- ECC:
  - Finite Prime Field
  - ECC key pair generation
  - Key length: 192 to 521 bits
  - Algorithm: ALG_ECDSA_SHA, ALG_ECDSA_SHA_224, ALG_ECDSA_SHA256
- RSA:
  - Standard and CRT
  - RSA key pair generation
  - Used Key length: RSA_1024 to RSA_2048 bits
  - Algorithm: ALG_RSA_SHA_ISO9796 [17], ALG_RSA_NOPAD, ALG_RSA_SHA_PKCS1, ALG_RSA_SHA256_PKCS1, ALG_RSA_PCKS1, ALG_RSA_SHA_PKCS1_PSS, ALG_RSA_SHA256_PKCS1_PSS
- Hash: SHA-1, SHA-224 [18], SHA-256, SHA-384, SHA-512
- RNG: PSEUDO and SECURE

Note that not all the Cryptographic algorithms, lengths and modes are involved in TOE Security Functions. Please refer to the relevant SFRs for a complete description of what cryptography is used by the TOE (section 6.1.2).

2. Conformance Claims

2.1. CC Conformance Claim

The ST claims compliance with the following references:

- Common Criteria Version 3.1 Part 1 [1]
- Common Criteria Version 3.1 Part 2 [2] extended
- Common Criteria Version 3.1 Part 3 [3] conformant

Extensions are based on the Protection Profiles (PP [4] and PP [5]) presented in the next section:

- FAU_SAS.1 'Audit data storage'
- FCS_RND.1 'Generation of random numbers'
- FIA_API.1 'Authentication Proof of Identity'
- FMT_LIM.1 'Limited capabilities'
- FMT_LIM.2 'Limited availability'
- FPT_EMSEC.1 'TOE emanation'

The assurance level for this ST is EAL 4 augmented with:

- ADV_FSP.5 'Complete semi-formal functional specification with additional error information'
- ADV_INT.2 'Well-structured internals'
- ADV_TDS.4 'Semiformal modular design'
- ALC_CMS.5 'Development tools CM coverage'
- ALC_DVS.2 'Sufficiency of security measures'
- ALC_TAT.2 'Compliance with implementation standards'
- ATE_DPT.3 'Testing: modular design'

2.2. PP Claim

This ST claims strict conformance to the following Protection Profile:

Protection Profile [4] **Machine Readable Travel Document with "ICAO Application", Basic Access Control**	
Version	1.10
Date	25th March 2009
Prepared by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Identification	PP0055
Approved by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Registration	BSI-CC-PP-0055-2009
Assurance Level	Common Criteria 3.1 EAL 4 augmented by ALC_DVS.2

The ICAO BAC and EAC PPs define the security objectives and requirements for the contactless chip 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 and Extended Access Control and Chip Authentication similar to the Active Authentication in the Technical reports of 'ICAO Doc 9303' [15].

This MRTD's IC does not limit the TOE interfaces to contactless: both contact and contactless interfaces are part of this TOE and the PP content has been enhanced for this purpose.

3. Security Problem Definition

3.1. Assets

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

Logical MRTD sensitive User Data

Sensitive biometric reference data:

- **EF.DG3**: Biometric Finger(s)
- **EF.DG4**: Biometric Eye(s) Iris

Logical MRTD data

The 'ICAO Doc 9303' [15] requires that Basic Inspection Systems must have access to:

- **EF.COM**: Common Data Elements, lists the existing EF with the user data
- **EF.SOD**: Document Security Object according to LDS [15] used by the inspection system for Passive Authentication of the logical MRTD
- **EF.DG1**: document's data (Type, Issuing State or Organization, Number, Expiry Date, Optional Data), holder's data (Name, Nationality, Date of Birth, Sex) and Check Digits
- **EF.DG2**: Encoded Face (Global Interchange Feature)
- **EF.DG5**: Biometric Face
- **EF.DG7**: Displayed Signature or Usual Mark
- **EF.DG8**: Displayed Portrait
- **EF.DG9**: Data Feature(s)
- **EF.DG10**: Structure Feature(s)
- **EF.DG11**: Additional Personal Detail(s)
- **EF.DG12**: Additional Document Detail(s)
- **EF.DG13**: optional Detail(s)
- **EF.DG14**: Security Info (Chip Authentication Public Key Info)
- **EF.DG15**: Active Authentication Public Key Info
- **EF.DG16**: Person(s) to Notify

Due to interoperability reasons with 'ICAO Doc 9303' [4], the TOE specifies 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) (DG6 is absent),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data

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

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.

3.2. Subjects

This Security Target considers the following subjects:

S.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.

S.Personalizer *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 of 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 (v) signing the Document Security Object defined in [15].

S.Country *Country Verifying Certification Authority*

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

S.DV *Document Verifier*

The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.

S.Terminal

A terminal is any technical system communicating with the TOE through its physical interfaces.

S.IS *Inspection system*

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 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.

S.Holder *MRTD Holder*

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

S.Traveler

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

3.3. Assumptions

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

A.MRTD_Manufact	*MRTD manufacturing on steps 5 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).

A.MRTD_Delivery	*MRTD delivery during steps 5 to 6*

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

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

The Personalization Agent ensures the correctness of
- the logical MRTD with respect to the MRTD holder,
- the Document Basic Access Keys,
- the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and
- 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.

A.Pers_Agent_AA	*Personalization of the MRTD's chip including Active Authentication*

The Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.
The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys	*Inspection Systems for global interoperability*

The Inspection System is used by the border control officer of the receiving State:
- examining an MRTD presented by the traveler and verifying its authenticity and
- verifying the traveler as MRTD holder.

The Basic Inspection System for global interoperability
- includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and
- implements the terminal part of the Basic Access Control [15].

The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.
The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports 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.

A.Insp_Sys_AA	*Inspection Systems for global interoperability with Active Authentication*

The Inspection System may also implement the terminal part of the Active Authentication Protocol.

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' [4], 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.

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

3.4. Threat agent

S.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.

Application note*: 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.*

3.5. Threats

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

T.Chip_ID	*Identification of MRTD's chip*

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 TOE communication interfaces.
The attacker has enhanced basic attack potential and does not know the optically readable MRZ data printed on the MRTD data page in advance.
Threatened asset is the user anonymity.

T.Skimming	*Skimming the logical MRTD*

An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the communication channels of the TOE.
The attacker does not know the optically readable MRZ data printed on the MRTD data page in advance.
Threatened asset is the confidentiality of logical MRTD data.

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

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.
The attacker has enhanced basic attack potential and does not know the optically readable MRZ data printed on the MRTD data page in advance.
Threatened asset is the confidentiality of logical MRTD data.

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

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 chip.
The attacker has enhanced basic attack potential and is in possession of one or more legitimate MRTDs.
Threatened asset is authenticity of logical MRTD data.

T.Counterfeit	*Counterfeit MRTD's chip*

An attacker produces an unauthorised copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveler by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.
The attacker is in possession of one or more legitimate MRTDs.
Threatened asset is authenticity of logical MRTD data.

The TOE shall avert the threats as specified below.

T.Abuse-Func	*Abuse of Functionality*

An attacker may use functions of the TOE which shall not be used in "Operational Use" phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.
The attacker has enhanced basic attack potential and is in possession of a legitimate MRTD.
Threatened assets are confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

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

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 communication interfaces (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).
The attacker has enhanced basic attack potential and is in possession of a legitimate MRTD.
Threatened asset is confidentiality of logical MRTD and TSF data.

T.Phys-Tamper *Physical Tampering*

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.
The attacker has enhanced basic attack potential and is in possession of a legitimate MRTD.
Threatened assets are confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Malfunction *Malfunction due to Environmental Stress*

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.
The attacker has enhanced basic attack potential and is in possession of a legitimate MRTD.
Threatened assets are confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.MOD_SOFT *Unauthorized Software Modification*

An attacker may perform unauthorized modification of Smart Card Embedded Software using the patch mechanism or the Card Content Loading and Installation mechanism.

3.6. Organisational Security Policies

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

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.

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.

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)3 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 [15].

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

4. Security Objectives

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

4.1. SOs for the TOE

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

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

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [15] 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.DG3 to EF.DG16 are added.

Application note: *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) cannot be changed by write access after personalization,

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

OT.Data_Int	*Integrity of personal data*

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

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.

Application note: *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' [15] 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 TOE. Thus the read access must be prevented even in case of a successful BAC Authentication.*

OT.Identification	*Identification and Authentication of the TOE*

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile 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.

Application note: *The TOE security objective OT.Identification addresses security features of the TOE to support the lifecycle 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 physical interfaces before successful authentication as Basic Inspection System or as Personalization Agent.*

OT.AA_Proof	*Proof of MRTD's chip authenticity by Active Authentication*

The TOE may support the Basic Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [15].

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

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 IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.
Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.Prot_Inf_Leak	*Protection against Information Leakage*

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the 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.

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

OT.Prot_Phys-Tamper	*Protection against Physical Tampering*

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

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

with a prior

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

OT.Prot_Malfunction *Protection against Malfunctions*

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested.

This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Application note: *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.*

OT.CCLI_END *Secure termination of Card Content Loading and Installation*

The TOE shall ensure that a mechanism to close the TOE in post issuance is available to the Manufacturer. Terminating Card Content Loading and Installation feature implies that it is not possible for an attacker to load any applet in the card using the GlobalPlatform Card Content Management interfaces.

OT.PATCH_SEC *Secure Patch Mechanism*

The TOE must ensure continued correct operation of the patch mechanism. The TOE shall prevent the alteration of its patch mechanism: mis-routing and load of illegal patches.

OT.PATCH_END *Secure termination of Patching*

The TOE shall ensure that a mechanism to close the TOE patching mechanism is available to the Manufacturer. Terminating patching feature implies that it is not possible for an attacker to load any patch in the card.

4.2. SOs for the Environment

4.2.1. Issuing State or Organization

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

OE.MRTD_Manufact	*Protection of the MRTD Manufacturing*

Appropriate functionality testing of the TOE shall be used in step 5 to 6.
During all manufacturing and test operations, security procedures shall be used through steps 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

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.

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.

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 to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [15].

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' [15] 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.

OE.Active_Auth_Key	*Active Authentication Key*

The issuing State or Organization may establish the necessary public key infrastructure in order to:

- Generate the MRTD's Active Authentication Key Pair,
- Sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and
- Support inspection systems of receiving States or Organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object

4.2.2. Receiving State or Organization

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

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 [15].

OE.Exam_MRTD_AA	*Examination of the MRTD passport book using Active Authentication*

During examination of the MRTD presented by the traveler, the basic inspection system may follow the Active Authentication Protocol to verify the authenticity of the presented MRTD's chip.

OE.Passive_Auth_Verif	*Verification by Passive Authentication*

The border control officer of the receiving State uses the inspection system to verify the traveler 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.

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 objectives rationale

[Rationale not provided in the Public version of this ST]

5. Extended Components Definition

This ST contains the following extended components defined as extensions to CC part 2 in the claimed PP [4]:

- SFR FAU_SAS 'Audit data storage'
- SFR FCS_RND 'Generation of random numbers'
- SFR FIA_API 'Authentication Proof of Identity'
- SFR FMT_LIM 'Limited capabilities and availability'
- SFR FPT_EMSEC.1 'TOE emanation'

5.1. Audit data storage (FAU_SAS)

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.

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 leveling:

FAU_SAS Audit data storage	1

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. Generation of random numbers (FCS_RND)

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.

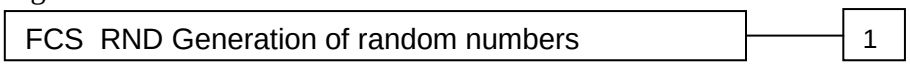
The family "Generation of random numbers (FCS_RND)" is specified as follows.

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. Authentication Proof of Identity (FIA_API)

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

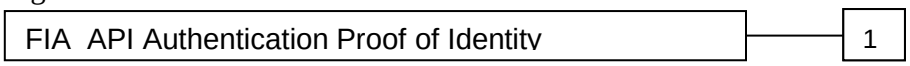
Application note: *The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter "Extended Components definition (ASE_ECD)") from a TOE point of view.*

FIA_API Authentication Proof of Identity

Family behavior

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

Component leveling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.4. Limited capabilities and availability (FMT_LIM)

The family FMT_LIM describes the functional requirements for the Test Features of the TOE.

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

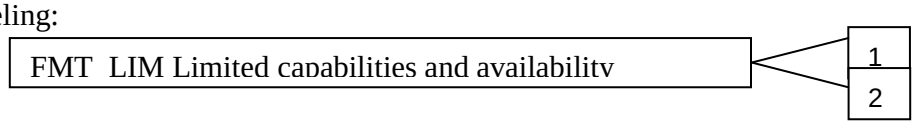
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family 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.

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.

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*].**

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*].**

Application note: *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.

5.5. TOE emanation (FPT_EMSEC.1)

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].

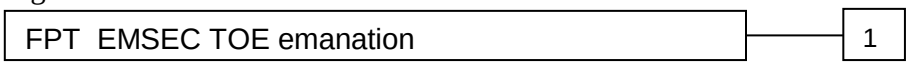
The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

FPT_EMSEC TOE Emanation

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 not to 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

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Some security functional requirements represent extensions to [2].

Operations for assignment, selection and refinement have been made and are designated by an underline (e.g. none), in addition, where operations that were uncompleted in the PP [4] are also identified by *italic underlined* type.

The TOE security assurance requirements statement given in section 0 is drawn from the security assurance components from Common Criteria part 3 [3].

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Basic Inspection System” and “Terminal” used in the following chapter is given in section 3.2. Note, that all these subjects are acting for homonymous external entities. All used objects are defined in section 9. 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].

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 Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

The following table provides an overview of the keys used:

Name	Data
Active Authentication Key Pair	The Active Authentication asymmetric Key Pair (KPr_{AA}, KPu_{AA}) is used for the Active Authentication Protocol: allowing the chip to be authenticated as genuine by the inspection system.
Active Authentication Private Key (KPr_{AA})	The Active Authentication Private Key (KPr_{AA}) is used by the TOE to be authenticated as a genuine MRTD’s chip by the inspection system. It is part of the TSF data.
Active Authentication Public Key (KPu_{AA})	The Active Authentication Public Key (KPu_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE’s logical MRTD and used by the inspection system for Active Authentication of the MRTD’s chip. It is part of the user data provided by the TOE for the IT environment.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD’s chip.
BAC Session Keys	Secure messaging TDES key and Retail-MAC key agreed between the TOE and a Basic Inspection System in result of the Basic Access Control Authentication Protocol.

6.1. TOE Security Functional Requirements

6.1.1. Security Audit (FAU)

6.1.1.1. Audit Storage (FAU_SAS.1)

FAU_SAS.1.1 The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.

Application note: *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-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. Cryptographic support (FCS)

Function		Algorithm	Key Size(s)
Basic Access	Authentication	TDES CBC	112 bits
Active Authentication	Signature generation	RSA signature based on ISO9796-2 scheme 1 [17]	1024, 1280, 1536, 2048
Secure Messaging	ENC/DEC	TDES CBC	112 bits
	MAC	Retail MAC	112 bits

6.1.2.1. Cryptographic key generation (FCS_CKM.1)

→ Generation of Document Basic Access Keys by the TOE

FCS_CKM.1.1/ BAC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [4], normative appendix 5.

Application note: *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 [16], normative appendix 5, A5.2, produces agreed parameters to generate the Triple- DES (TDES) key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [16], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.*

→ Generation of Active Authentication Key Pair by the TOE

FCS_CKM.1.1/ KP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA key pair generation* and specified cryptographic key sizes *RSA 1024-1536-2048 bits* that meet the following: *IEEE 1363 [20]*.

Application note: *The component FMT_MTD.1/AAPK defines an operation "create" that means that the Active Authentication Private Key is generated by the TOE itself. This resulted in this instantiation of the component FCS_CKM.1 as SFR for this key generation.*

6.1.2.2. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *none*.

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

6.1.2.3. Cryptographic operation (FCS_COP.1)

→ Hashing for Key Derivation

FCS_COP.1.1/ SHA — The TSF shall perform hashing in accordance with a specified cryptographic algorithm *SHA-1 or SHA-256* and cryptographic key sizes none that meet the following: *FIPS 180-2 [18]*.

Application note: *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 [16].*

→ SM Encrypt/Decrypt

FCS_COP.1.1/ ENC — The TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm TDES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [19] and [16]; normative appendix 5, A5.3.

Application note: *The TOE implements the cryptographic primitives (e.g. TDES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol according to the FCS_CKM.1. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the symmetric authentication mechanism.*

→ Authentication

FCS_COP.1.1/ AUTH — The TSF shall perform symmetric authentication – encryption and decryption in accordance with a specified cryptographic algorithm *TDES* and cryptographic key sizes *112 bits* that meet the following: *FIPS 46-3 [19]*.

Application note: *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).*

→ SM - MAC

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

Application note: *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.*

→ Signature generation

FCS_COP.1.1/ SIG_GEN — The TSF shall perform *digital signature generation* in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *RSA 1024-1280-1536-2048 bits* that meet the following: *ISO/IEC 9796-2 [17]*.

Application note: *For signature generation in the Active Authentication mechanism, the TOE uses ISO/IEC 9796-2 compliant cryptography (scheme 1).*

6.1.2.4. Random Number Generation (FCS_RND.1)

FCS_RND.1.1 — The TSF shall provide a mechanism to generate random numbers that meet *AIS31 class "P2 – SOF-High"*.

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

6.1.3. User data protection (FDP)

6.1.3.1. Subset access control (FDP_ACC.1)

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

6.1.3.2. Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the Basic Access Control SFP 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.

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.

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

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

1. Any terminal is not allowed to modify any of 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.

Application note: *The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this TOE (cf. [17] for details).*

6.1.3.3. Basic data exchange confidentiality (FDP_UCT.1)

Application note: *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.*

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

6.1.3.4. Data exchange integrity (FDP_UIT.1)

Application note: *See application in FDP_UCT.1.*

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

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

6.1.4. Identification and authentication (FIA)

The following table provides an overview on the authentication mechanisms used:

Name	SFR for the TOE	Cryptography
Basic Access Control Authentication Mechanism	FIA_UAU.4, FIA_UAU.6	TDES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agent	FIA_UAU.4	TDES with 112 bit keys (cf. FCS_COP.1/AUTH)
Active Authentication	FIA_API.1, FIA_UAU.4	RSA signature based on ISO9796-2 scheme 1, with Keys 1024, 1280, 1536, 2048 bits (cf. FCS_COP.1.1/ SIG_GEN)

6.1.4.1. Authentication Failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [0..255] of consecutive* unsuccessful authentication attempts occur related to *failure of a BAC Authentication*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall *block the BAC cryptographic key*.

Application note: *The terminal challenge eIFD and the TSF response eICC are described in [16], Appendix C. The refinement by inclusion of the word "consecutive" allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored in non-volatile memory in the TOE thus the "consecutive unsuccessful authentication attempts" are count independent on power-on sessions but reset to zero after successful authentication only.*

6.1.4.2. Authentication Proof of Identity (FIA_API.1)

FIA_API.1.1 The TSF shall provide an *Active Authentication Protocol according to [15]* to prove the identity of the *TOE*.

Application note: *The TOE may implement the Active Authentication Mechanism specified in [15] Part 1 Appendix 4 to section IV. This mechanism is a challenge response protocol where TOE challenge response is calculated being digital signature over the terminal's 8 bytes nonce.*

6.1.4.3. Timing of authentication (FIA_UAU.1)

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"

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.

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

6.1.4.4. Single-use authentication mechanisms (FIA_UAU.4)

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 *TDES,*
3. *Active Authentication Protocol*.

Application note: *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.*

Application note: *The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [16]. 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 fulfil the security objective OT.Identification and to prevent T.Chip_ID.*

6.1.4.5. Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide
1. Basic Access Control Authentication Mechanism,
2. Symmetric Authentication Mechanism based on *TDES*

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 *the Symmetric Authentication Mechanism with Personalization Agent Key*.
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

Application note: *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*

6.1.4.6. Re-authenticating (FIA_UAU.6)

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.

Application note: *The Basic Access Control Mechanism specified in [15] 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.*

Application note: *Note that in case the TOE should also fulfil [5] 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.*

6.1.4.7. Timing of identification (FIA_UID.1)

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"

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.

Application note: *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..*

Application note: *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 than one RFID. This identifier is randomly selected and it does not violate the OT.Identification.*

6.1.5. Security management (FMT)

6.1.5.1. Limited capabilities (FMT_LIM.1)

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

6.1.5.2. Limited availability (FMT_LIM.2)

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
5. which may enable other attacks.

Application note: *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 to 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.

6.1.5.3. Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to *disable* the functions *Card Content Loading and Installation, and Patching* to *the Manufacturer*.

Application note: *The Card Content Loading and Installation particularly refers to the loading and installation of Java Card applets into the TOE. Disabling these functions is permanent: the functions are terminated.*

6.1.5.4. Management of TSF data (FMT_MTD.1)

→ Writing of Initialization Data and Pre-personalization Data

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

Application note: *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.*

→ Disabling of Read Access to Initialization Data and Pre-personalization Data

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

Application note: *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 Pre-personalization 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.*

→ Key Write

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

Application note: *The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.*

→ Key Read

FMT_MTD.1.1/ KEY_READ The TSF shall restrict the ability to read the Document Basic Access Keys, *Active Authentication Private Key* and Personalization Agent Keys to none.

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

→ Active Authentication Private Key

FMT_MTD.1.1/ AAPK The TSF shall restrict the ability to *create* the *Active Authentication Private Key* to *the Terminal*.

Application note: *The verb "create" means here that the Terminal (after successful authentication of the Personalization Agent) is requesting the creation of the Active Authentication Key on the TOE and is requesting the secure generation of the Active Authentication Private Key by the TOE itself. See the instantiation of the component FCS_CKM.1 as SFR for this key generation.*

6.1.5.5. Specifications of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:
1. Initialization,
2. Pre-personalization,
3. Personalization,
4. *Card Content Loading and Installation termination,*
5. *Patching termination.*

6.1.5.6. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles
1. Manufacturer,
2. Personalization Agent,
3. Basic Inspection System.

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

6.1.6. Protection of the TSF (FPT)

6.1.6.1. TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit *information of IC Power consumption* in excess of *State of the Art values* enabling access to Personalization Agent Key(s) and *Active Authentication Private Key*.

FPT_EMSEC.1.2 The TSF shall ensure any users are unable to use the following interface smart card circuit contacts *to gain ac*cess to Personalization Agent Key(s) and *Active Authentication Private Key*.

Application note: *The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip provides a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.*

6.1.6.2. Failure with preservation of secure state (FPT_FLS.1)

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.

6.1.6.3. Resistance to physical attack (FPT_PHP.3)

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

Application note: *The TOE implements 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.*

Application note: *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.*

6.1.6.4. TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial start-up* to demonstrate the correct operation of the TSF.

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

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

Application note: *self-test for the verification of the integrity of stored TSF executable code are executed during initial start-up in the Phase 3 "Personalization" and Phase 4 "Operational Use".*

6.2. TOE Security Assurance Requirements

TOE Security Assurance Requirements as stated in section 6.2 of the claimed PP [4].

The augmentations compared to the CC V3.1 package for EAL4 are:

- ADV_FSP: augmented from 4 to 5
- ADV_INT: added at level 2
- ADV_TDS: augmented from 3 to 4
- ALC_CMS: augmented from 4 to 5
- ALC_DVS: augmented from 1 to 2
- ALC_TAT: augmented from 1 to 2
- ATE_DPT: augmented from 1 to 3

6.2.1. SARs Measures

The assurance measures that satisfy the TOE security assurance requirements are the following:

Assurance Class	Component	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	**Complete Semi-formal functional specification with additional error information**
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	**Well-structured internals**
	ADV_TDS.4	**Semi-formal modular design**
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	**Development tools CM coverage**
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	**Sufficiency of security measures**
	ALC_LCD.1	Developer defined lifecycle model
	ALC_TAT.2	**Compliance with implementation standards**
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Test	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	**Testing: modular design**
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis

Table 1 – Assurance Requirements: EAL4 augmented

6.2.2. SARs Rationale

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

Augmentation results from the selection of:

ADV_FSP.5 Complete Semi-formal functional specification with additional error information

The selection of the component ADV_FSP.5 provides a better coverage of the functional specification with semi-formal modelling and additional error information.

The component ADV_FSP.5 has the following dependencies: ADV_TDS.1 Basic design and ADV_IMP.1 Implementation representation of the TSF.

ADV_INT.2 Well-structured internals

The selection of the component ADV_INT.2 provides additional information regarding the TSF internals by analysing the complexity to justify it is well-structured.

The component ADV_INT.2 has the following dependencies: ADV_IMP.1 Implementation representation of the TSF, ADV_TDS.3 Basic modular design, and ALC_TAT.1 Well-defined development tools.

ADV_TDS.4 Semi-formal modular design

The selection of the component ADV_TDS.4 provides enhanced design of the TOE introducing semi-formal modelling of the subsystems and differentiating the roles of the modules regarding each TSF.

The component ADV_TDS.4 has the following dependency: ADV_FSP.5 Complete semi-formal functional specification with additional error information.

ALC_DVS.2 Life-cycle support- Sufficiency of security measures

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.

The component ALC_DVS.2 has no dependencies.

ALC_CMS.5 Development tools CM coverage

The selection of the component ALC_CMS.5 provides improved configuration management by covering the development tools (compiler options, build options etc…).

The component ALC_CMS.5 has no dependencies.

ALC_TAT.2 Compliance with implementation standards

The selection of the component ALC_TAT.2 provides additional information on the implementation standards applied by the developer.

The component ALC_TAT.2 has the following dependency: ADV_IMP.1 Implementation representation of the TSF.

ATE_DPT.3 Testing: modular design

The selection of the component ATE_DPT.3 provides improved testing depth by requiring modular testing versus testing focused on the TSF-enforcing modules.

The component ATE_DPT.3 has the following dependencies: ADV_ARC.1 Security architecture description, ADV_TDS.4 Semiformal modular design, and ATE_FUN.1 Functional testing.

All of these are met or exceeded in the EAL4 assurance package.

6.3. Security Requirements Rationale

[Rationale not provided in the Public version of this ST]

7. TOE summary specification

This set of TSFs manages the identification and/or authentication of the external user and enforces role separation (FMT_SMR.1).

7.1. SF.Access Control

This function checks that for each operation initiated by a user, the security attributes for user authorization (FMT_SMR.1) and data communication required are satisfied.

The function includes control over the Terminal gaining access to MRTD's chip data (FDP_ACC.1, FDP_ACF.1) based on authentication status of the Terminal and Terminal authorizations:

Control over the authorization of Manufacturer during Pre-personalization Phase 2 to:

- Write the initialization data and pre-personalization data (FMT_MTD.1/INI_ENA)

Control over the authorization of Personalization Agent during Personalization Phase 3 to:

- Write and Read EF.COM, EF.SOD, EF.DG1 to EF.DG16 (FDP_ACF.1.2 (1))
- Create initial Active Authentication Private Key (FMT_MTD.1/AAPK)
- Write Document Basic Access Keys (FMT_MTD.1/KEY_WRITE)
- Disable read access to initialization data for users (FMT_MTD.1/INI_DIS)

Control over the Basic Inspection System during Usage Phase 4 to:

- Read EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG16 (FDP_ACF.1.2 (2))
- Prevent reading of EF.DG3 (fingerprint) and EF.DG4 (Iris) (FDP_ACF.1.4 (3))
- Create new Active Authentication Keys (FMT_MTD.1/AAPK)

Control over any non-authenticated Terminal during Usage Phase 4 to:

- Prevent modification of EF.DG1 to EF.DG16 (FDP_ACF.1.4 (1))
- Prevent reading of EF.DG1 to EF.DG16 (FDP_ACF.1.4 (2))
- Prevent reading Document Basic Access Keys, Personalization Agent Keys, Active Authentication Private Key (FMT_MTD.1/KEY_READ)

Control over the enforcement of Secure Messaging over:

- Importation and exportation of data (including but not restricted to EF.COM, EF.SOD, EF.DG1-EF.DG16) after successful BAC Authentication (FDP_UCT.1, FDP_UIT.1)

7.2. SF.Card Personalization

This TSF provides Card initialization and pre-personalization services (FMT_SMF.1) as per GlobalPlatform. This includes but is not restricted to card initialization, patch loading, applet installation and instantiation.

This TSF also provides MRTD's chip personalization functions to allow the Personalization Agent to create and set the initial MRTD's LDS data (FMT_SMF.1). This includes disabling read access to Initialization data at completion of the personalization phase (FMT_SMF.1).

7.3. SF.Manufacturer Authentication

The Manufacturer is the only user authenticated through the GlobalPlatform Mutual Authentication process. He authenticates during the Manufacturing Phase of the TOE (FAU_SAS.1) using the Secure Channel protocol (SCP01 or SCP02).

This user is able to authenticate with the Operating System to launch the installation of the ICAO applet and to perform TOE Operating System (OS) personalization (MRTD IC pre-personalization). He is also able to read the Initialization Data (FIA_UAU.1, FIA_UID.1).

When the TOE is ready to be personalized, the Manufacturer will create the authentication data for the Personalization Agent and terminate this manufacturing stage by disabling the card content loading and installation functions (FMT_MOF.1).

In Usage phase, the Manufacturer could only authenticate to set TERMINATE the TOE.

7.4. SF.Personalizer Authentication

The Personalization Agent is authenticated by the TOE using its symmetric key (FIA_UAU.5). He is able to read the random identifier in that phase (FIA_UAU.1, FIA_UID.1).

The authentication requires a symmetric encryption using TDES in CBC mode with a key length of 112 bits (FCS_COP.1/ENC).

IC power variation emanation is below state of the art values, and physical access to the authentication data is protected during this SF activity (FPT_EMSEC.1).

7.5. SF.BAC Authentication

This TSF provides the Basic Access Control passive authentication protocol (The Terminal is then allowed to select this authentication key and proceed with BAC Authentication (FIA_UAU.1, FIA_UID.1, and FIA_UAU.5). This is the only authentication mechanism that involves symmetric keys (KB_{Enc} and KB_{MAC}): TDES 112 bits (FCS_COP.1/AUTH).

As part of the protocol, the BAC Session Keys are derived from the MRZ of the MRTD's chip: this is done using SHA-1 (FCS_COP.1/SHA). The authentication initialization requires that the MRTD's chip generates 8 bytes challenge (nonce r_{PICC}) that is read by the Basic Inspection System (FIA_UAU.1), and 16 bytes Key (K_{PICC}) (FCS_RND.1). The MRTD BAC authentication stages also require TDES encryption of 32 bytes of concatenated data and a Retail MAC computation over the 32 bytes of encryption output (FCS_COP.1/MAC). The Basic Inspection System also generated a pair (K_{PCD}, r_{PCD}). The use of challenges enforces a protection against replay (FIA_UAU.4).

Completion of the BAC Authentication protocol means that a Secure Messaging session is started with the session keys (K_{ENC} and K_{MAC}) derived from the derived according to [15] from the common master secret $K_{Master} = K_{PICC} \oplus K_{PCD}$ and a Send Sequence Counter SSC derived from r_{PICC} and r_{PCD} (FCS_CKM.1/BAC). All further communication with the TOE is handled by SF.Secure Messaging Security Function, enforcing confidentiality and integrity over transferred data (FIA_UAU.5).

In case the BAC authentication protocol fails (the TOE being unable to identify the Terminal as being a legitimate Basic Inspection System) the TOE records one authentication failure. If the Terminal reaches a pre-defined amount of successive authentication failures, the BAC Authentication Key is blocked (FIA_AFL.1).

7.6. SF.Active Authentication

Active Authentication is provided by this TSF based on the availability of DG15 in the MRTD's chip information data (FIA_API.1). This is decided by the Personalization Agent during phase 3 when the LDS is personalized. The Terminal is then allowed to select this authentication key and proceed with Active Authentication after successful BAC Authentication (to prevent the privacy threat Challenge Semantics). See the inspection procedures in section 2.1 of [16].

This TSF involves an optional asymmetric Key Pair (KPr_{AA}, KPu_{AA}) which public part is stored in DG15 and private part is stored securely within the chip. This Key Pair is securely generated on the TOE under request of the Personalization Agent (FCS_CKM.1/KP).

This TSF ensures that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the MRTD's chip. The TOE's challenge is a true random generated by the TOE (FCS_RND.1). And the challenge-response involves an RSA signature generation based on ISO/IEC 9796-2 Digital Signature scheme 1 (FCS_COP.1/SIG_GEN). The use of challenges enforces a protection against replay (FIA_UAU.4).

IC power variation emanation is below state of the art values, and physical access to the authentication data is protected during this SF activity (FPT_EMSEC.1).

7.7. SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device. This TSF provides a secure mean for the terminal and the card to exchange data (FIA_UAU.1, FIA_UAU.5): such as (and not restricted to) EF.COM, EF.SOD, EF.DG1 to EF.DG16.

The SF.Secure Messaging function is capable of providing a trusted path between legitimate end points both of the TOE and the external device. The secure communication channels are enforced by cryptographic functions.

This function enforces confidentiality (FDP_UCT.1) and integrity (FDP_UIT.1) of the transferred data (transmitted and received):

- Confidentiality is ensured by a TDES encryption (FCS_COP.1/ENC)
- Integrity is achieved by calculation, embodiment and verification of a Retail MAC (FCS_COP.1/MAC)

This function provides means to detect if modification, deletion, insertion or replay is occurring during a Secure Messaging session. In such cases, this TSF will terminate the session and securely destroyed the session keys (FCS_CKM.4). A session is also terminated upon reset of the TOE. A re-authentication using the Chip Authentication protocol is required after termination of a Secure Messaging session (FIA_UAU.6).

7.8. SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation, secure random generator, and data hashing:

- Secure generation of asymmetric Key Pair (FCS_CKM.1/KP), key generation is protected against SPA, Timing attacks, and electromagnetic emanation (FPT_EMSEC.1) and includes Key Pair Correspondence verification.
  - RSA key pair with length from 1024 to 2048 bits
  - Elliptic Curves ECDSA Keys with length 192, 224, 256, 384, 521 bits
- Data hashing using SHA-1, SHA-224, SHA-256 (FCS_COP.1/SHA)
- RSA Sign and Verify operations with both CRT and standard Key Pairs of length 1024, 1280, 1536, 2048 bits (FCS_COP.1/SIG_GEN)
- ECDSA Signature Verification with ECC Keys of length 192, 224, 256, 384, 521 bits
- TDES 2 Keys and 3 Keys in CBC and ECB modes (FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/AUTH)
- Secure destruction of cryptographic key secret or private material (FCS_CKM.4).
- The random number generator of the underlying IC is used by the TOE whenever the generation of a nonce is required (FCS_RND.1).
- Adequate number of Rabin Miller test rounds is performed in addition to GCD test in order to ensure correct generation of primes.
- MAC is generated and verified using TDES with 2 or 3 keys
- BAC protocol related cryptography (FCS_CKM.1/BAC)

This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMSEC.1)

7.9. SF.Protection

This Security Function is responsible for protection of the TSF data, user data, and TSF functionality.

The SF. Protection function is composed of software implementations of test and security functions including:

- Performing self-tests of the TOE at each power-up (FPT_TST.1)
- Deleting authentication resources (Biometrics, PINs, secret and private keys) when relevant memory is de-allocated (FCS_CKM.4)
- Validating the integrity of all stored cryptographic keys and PINs before use and informing the Terminal when such validation fails (FPT_TST.1).
- Ensuring that Information is not leaked.
- Performing a set of test to verify that the underlying cryptographic algorithms are operating correctly (FPT_TST.1).
- Initializing memory after reset
- Initializing memory of de-allocated data
- Preserving secure state after sensitive processing failure (RNG, EEPROM handling) or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.3)
- Termination of the Card Content Loading and Installation services (FMT_MOF.1, FMT_SMF.1)
- Patch loading and termination (FMT_MOF.1, FMT_SMF.1)

The TOE provides the ability to patch some identified native functions of the original TOE. This mechanism is available during Initialization phase but in the case of this TOE, no patch is loaded. The patch activities during the initialization phase are reduced to the termination of the patch mechanism.

This TSF prevents re-activation of de-activated or disabled or terminated mechanisms: the code area and data area are protected (FMT_LIM.1, FMT_LIM.2)

8. Additional Rationale

8.1. Security Requirements Grounding in Objectives

This chapter covers the grounding that have not been done in the precedent chapter

Requirement	Security Objectives
Security Assurance Requirements	
ADV_ARC.1	EAL 4
ADV_FSP.4	EAL 4
ADV_IMP.1	EAL 4
ADV_TDS.3	EAL 4
AGD_OPE.1	EAL 4
AGD_PRE.1	EAL 4
ALC_CMC.4	EAL 4
ALC_CMS.4	EAL 4
ALC_DEL.1	EAL 4
ALC_DVS.2	EAL 4+
ALC_LCD.1	EAL 4
ALC_TAT.1	EAL 4
ATE_COV.2	EAL 4
ATE_DPT.2	EAL 4
ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_VAN.4	EAL 4

Table 2 – Assurance Requirement to Security Objective Mapping

8.2. Rationale for Extensions

Extensions are based on the Protection Profile [4] and have all been adopted by the TOE developer:

- FAU_SAS.1 ‘Audit data storage’
- FCS_RND.1 ‘Generation of random numbers’
- FIA_API.1 ‘Authentication Proof of Identity’
- FPT_EMSEC.1 ‘TOE emanation’

8.3. PP Claim Rationale

This ST includes all the security objectives and requirements claimed by PP [4], and, all of the operations applied to the SFRs are in accordance with the requirements of this PP.

8.3.1. PP compliancy

The TOE type is compliant with the claimed PP: the TOE is an ICAO MRTD’s chip providing all means of identification and authentication of the TOE itself, the MRTD’s traveler and possibly the Terminal.

The TOE is compliant with the representation provided in the ICAO Machine Readable Travel Document Chip with Basic Access Control PP [4].

The compliance is strict: the addition of specific TOE security mechanisms to the security principles of this Security Target required only the addition of one Threat and three TOE Objectives.

These additions do not affect the concept defined in the PP [4] and this ST is a suitable solution to the generic security problem described in the PP.

9. Terminology

Term	Definition
Active Authentication	Security mechanism defined in [15] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of Organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined in [15] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [15]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [15]
Country Signing CA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing State or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [15], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

Term	Definition
Document Basic Access Keys	Pair of symmetric (two-key) TDES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [15]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [15]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations.
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [15]
Extended Access Control	Security mechanism identified in [15] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate itself with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [15]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [15]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.

Term	Definition
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [15]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [15]
Initialization	Process of writing Initialization Data (see below) to the TOE (cf.1.7.2, TOE lifecycle phase 2 step 3).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [15]
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.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization.
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [15]
Issuing State	The Country issuing the MRTD. [15]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [15]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [15] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) a. personal data of the MRTD holder b. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), c. the digitized portraits (EF.DG2), d. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and e. the other data according to LDS (EF.DG5 to EF.DG16) f. EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [15]

Term	Definition
Machine readable visa (MRV)	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [15]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [15]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [15]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [15], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. **Error! Reference source not found.**, OE lifecycle phase 3 step 6).
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (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) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.

Term	Definition
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove his identity and to get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6.
Physical travel Document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf. 1.7.2, TOE lifecycle phase 2 step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between lifecycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.
Receiving State	The Country to which the Traveler is applying for entry. [15]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [15]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 Skimming Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel.
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
Un-personalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User data	Data created by and for the user that does not affect the operation of the TSF.
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [15]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

10. References

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

[2] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-002 - Part 2: Security functional requirements, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-003 - Part 3: Security assurance requirements, Revision 4, September 2012.

[4] BSI-CC-PP0055 – Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control – EAL 4+ – Version: 1.10, 25th March 2009

[5] BSI-CC-PP0056 – Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control – EAL 4+ – Version: 1.10, 25th March 2009

[6] Inside Secure AT90SC28880RCFV Technical Datasheet – TPR0397 revision FX

[7] Inside Secure AD-X Technical Datasheet – TPR0116 revision FX

[8] BSI-PP-0035-2007 – Security IC Platform Protection Profile – version 1.0 – EAL4+

[9] Certification Report ANSSI-CC-2012/22 – ANSSI for Inside Secure – Apr 18, 2012

Maintenance Report ANSSI-CC-2012/22-M01 – ANSSI for Inside Secure – Dec 21, 2012

[10] AT90SC28880RCFV Revision J Security Target - Public Version – Ref: TPG0210 - Revision C

[11] PKCS#1: RSA Cryptography Standard, Version 1.5

[12] Java Card 2.2.2 Specification. March 2006. Published by Sun Microsystems, Inc.

- Virtual Machine Specification [JCVM]
- Application Programming Interface [JCAPI]
- Runtime Environment Specification [JCRE]

[13] GlobalPlatform, Card Specification, Version 2.1.1, March 2003

[14] CCDB-2007-09-001 – Composite product evaluation for Smart Cards and similar devices – Version: 1.0, revision 1, September 2007

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

[16] TR-03110, Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, BSI

[17] ISO/IEC 9796-2: Information technology — Security techniques — Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms, 2002

[18] FIPS PUB 180-2, FIPS Publication – Secure hash standard (+ Change Notice to include SHA-224), 2002, NIST

[19] FIPS PUB 46-3, FIPS Publication – Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department of Commerce/NIST

[20] IEEE 1363-2000 – IEEE Standard Specification for Public-Key Cryptography