



SECURITY TARGET LITE
IDEAL PASS V2.2-N - BAC JC EPASSPORT

Reference: 2017_2000032442



DOCUMENT EVOLUTION

Date	Index	Author	Revision
05/12/2017	1.0	IDEMIA	Initial Version

Table of Contents

TABLE OF CONTENTS	3
TABLE OF FIGURES	5
TABLE OF TABLES	6
1 ST INTRODUCTION	7
1.1 ST IDENTIFICATION	7
1.2 TOE REFERENCE.....	7
1.3 TOE OVERVIEW.....	8
1.4 TOE DESCRIPTION	8
1.4.1 <i>TOE Definition</i>	8
1.4.2 <i>TOE usage and security features for operational use</i>	9
1.4.3 <i>TOE life cycle</i>	12
2 CONFORMANCE CLAIMS	19
2.1 CC CONFORMANCE CLAIM	19
2.2 PP CLAIM.....	19
2.3 PACKAGE CLAIM	20
2.4 PP CONFORMANCE RATIONALE	20
2.4.1 <i>Main aspects</i>	20
2.4.2 <i>Overview of differences between the PP and the ST</i>	20
3 SECURITY PROBLEM DEFINITION	23
3.1 ASSETS.....	23
3.2 USERS / SUBJECTS.....	23
3.3 THREATS.....	25
3.3.1 <i>Threats to be averted by the TOE and its environment</i>	26
3.4 ORGANISATIONAL SECURITY POLICIES	29
3.5 ASSUMPTIONS	30
4 SECURITY OBJECTIVES	33
4.1 SECURITY OBJECTIVES FOR THE TOE	33
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	36
4.3 SECURITY OBJECTIVES RATIONALE	39
5 EXTENDED REQUIREMENTS	44
5.1 DEFINITION OF THE FAMILY FAU_SAS	44
5.1.1 <i>FAU_SAS Audit data storage</i>	44
5.2 DEFINITION OF THE FAMILY FCS_RND	44
5.2.1 <i>FCS_RND Generation of random numbers</i>	45
5.3 DEFINITION OF THE FAMILY FIA_API	45
5.3.1 <i>FIA_API Authentication Proof of Identity</i>	45
5.4 DEFINITION OF THE FAMILY FMT_LIM	46
5.4.1 <i>FMT_LIM Limited capabilities and availability</i>	46
5.5 DEFINITION OF THE FAMILY FPT_EMSEC.....	48
6 SECURITY REQUIREMENTS	50
6.1 SECURITY FUNCTIONAL REQUIREMENTS	50
6.1.1 <i>Class FAU Security Audit</i>	50
6.1.2 <i>Class Cryptographic Support (FCS)</i>	51

6.1.3	<i>Class FIA Identification and Authentication</i>	57
6.1.4	<i>Class FDP User Data Protection</i>	64
6.1.5	<i>Class FMT Security Management</i>	67
6.1.6	<i>Protection of the Security Functions</i>	72
6.2	SECURITY ASSURANCE REQUIREMENTS	75
6.3	SECURITY REQUIREMENTS RATIONALE	76
6.3.1	<i>Functional Security Requirements Rationale</i>	76
6.3.2	<i>Dependencies</i>	80
6.3.3	<i>Rationale for the Security Assurance Requirements</i>	84
7	TOE SUMMARY SPECIFICATION	85
7.1	TOE SUMMARY SPECIFICATION	85
7.1.1	<i>SF.IA Identification and Authentication</i>	85
7.1.2	<i>SF.CF Cryptographic functions support</i>	86
7.1.3	<i>SF.ILTB Protection against interference, logical tampering and bypass</i>	86
7.1.4	<i>SF.AC Access control / Storage and protection of logical travel document data</i>	86
7.1.5	<i>SF.SM Secure Messaging</i>	87
7.1.6	<i>SF.LCM Security and life cycle management</i>	88
7.2	SFRs AND TSS	90
7.2.1	<i>SFRs and TSS - Rationale</i>	90
8	ANNEX	94
	GLOSSARY	94
	ABBREVIATIONS	105
	REFERENCES	105



Table of figures

Figure 1: TOE Perimeter	9
Figure 2: TOE life-cycle	13

Table of tables

Table 1: Security Objective Rationale.....	40
Table 2: Overview on authentication SFR.....	57
Table 3: Coverage of Security Objective for the TOE by SFR	77
Table 4: Dependencies between the SFR for the TOE	83
Table 5: Life-cycle phases and states	88

1 ST Introduction

The aim of this document is to describe the Security Target for the Machine Readable Travel Document (MRTD) with the ICAO application, Basic Access Control and Active Authentication on the NXP JCOP 3 SECID P60 CS (OSB) open platform.

1.1 ST Identification

Title	Security Target Lite IDeal Pass v2.2-n - BAC JC ePassport
Reference	2017_2000032442
Version	1.0
Certification Body	ANSSI
Author	IDEMIA
CC Version	3.1 Revision 4
Assurance Level	EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3
Protection Profiles	Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March. 2009 [BAC-PP]

1.2 TOE Reference

TOE name	IDeal Pass v2.2-n - BAC JC ePassport
TOE version number	v2.2.0.12
Name of Platform	NXP JCOP 3 SECID P60 CS (OSB) certified by the Dutch NSCIB certification body (CC-17-98209) on 02-08-2017
Platform identification	PlatformID: JxHyyy0019790400 Patch level: 0x0000000000000000
IC reference	NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software (Certification ID: BSI-DSZ-CC-0973-2016)
Crypto Lib reference	Crypto Library V3.1.2 on P6022y VB (Certification ID CC-16-67206-CR)

1.3 TOE Overview

The Security Target (ST) defines the security objectives and requirements for the contactless and contact 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 method Basic Access Control and Active Authentication in the 'ICAO Doc 9303' [ICAO-9303].

Therefore the main feature is the following:

- **Authentication by the Basic Access Control (BAC),**
using the Document Basic Access Key Derivation Algorithm according to 'ICAO Doc 9303' [ICAO-9303], Normative Appendix 5.

As a feature that can be optionally configured the TOE supports:

- **Active Authentication (AA),**
to protect the MRTD's chip against chip substitution according to 'ICAO Doc 9303' [ICAO-9303], Volume II, Section IV, 5.6.2. It prevents copying the LDS Security Object (SO_D) and proves that the SO_D has been read from the authentic chip.

1.4 TOE Description

1.4.1 TOE Definition

The Target of Evaluation (TOE) is a contact or contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing Basic Access Control according to the ICAO document [ICAO-9303] and the protection profile [BAC-PP]. Additionally to the [BAC-PP] the TOE provides and Active Authentication according to [ICAO-9303].

The TOE is composed of

- the NXP JCOP 3 SECID P60 CS (OSB) open platform, comprising of
 - the circuitry of the MRTD's chip (NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software) with hardware for the contact and contactless interface;
 - the Crypto Library V3.1.2 on P6022y VB;
 - the IC Embedded Software (operating system): NXP JCOP3 OSB;
- the MRTD application **IDeal Pass v2.2-n - BAC JC ePassport** loaded in ROM or in EEPROM;
- the associated guidance documentation.

The TOE utilizes the evaluation of NXP JCOP 3 SECID P60 CS (OSB) open platform which has been certified by the Dutch NSCIB certification body (CC-17-98209).

A schematic overview of the TOE is shown in Figure 1:

- The MRTD’s chip circuitry and the IC dedicated software forming the Smart Card Platform (Hardware Platform and Hardware Abstraction Layer);
- The IC embedded software running on the Smart Card Platform consisting of
 - Java Card virtual machine, ensuring language-level security;
 - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
 - Java card API, providing access to card’s resources for the Applet;
 - Global Platform Card Manager, responsible for management of Applets on the card;
 - Mifare implementation can be enabled or disabled for this TOE.
 - Crypto Library
- The Applet Layer is the **IDEal Pass v2.2-n - BAC JC ePassport** Applet.

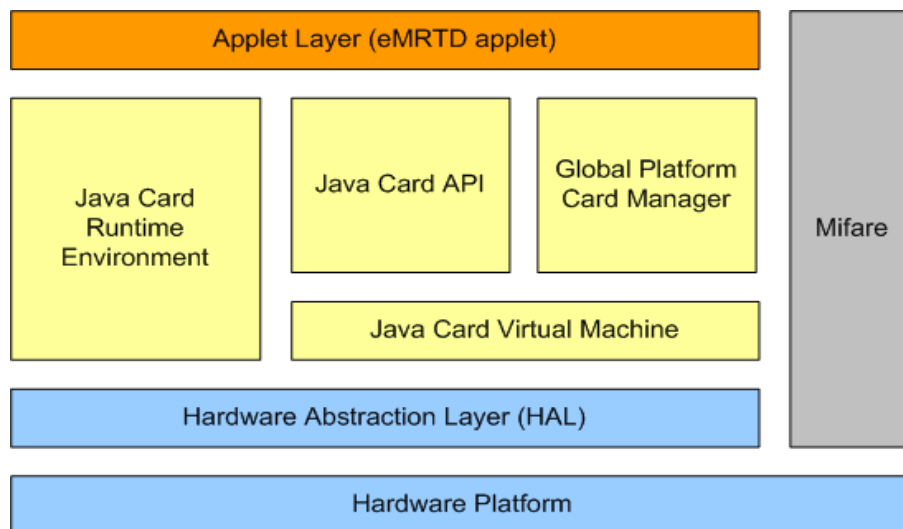


Figure 1: TOE Perimeter

1.4.2 TOE usage and security features for operational use

A State or organisation issues MRTD to be used by the holder for international travel. The traveler presents its MRTD to the inspection system to prove his or her identity. The MRTD in the context of this security target contains:

- i. visual (eye readable) biographical data and portrait of the holder,
- ii. a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and

- iii. data elements on the MRTD's chip according to the LDS for contactless and contact 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 genuine MRTD of issuing State or Organization.

The security functionality of the TOE will be externally available to the user by APDU commands according to the access conditions specified by the according policies considering the life cycle state, user role and security state.

For this security target the MRTD is viewed as unit of:

- a) 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
 - (1) the biographical data on the biographical data page of the passport book,
 - (2) the printed data in the Machine Readable Zone (MRZ) and
 - (3) the printed portrait.
- b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure as specified by ICAO in [ICAO-9303] on the contactless or contact based integrated circuit. It presents contactless and/contact based readable data including (but not limited to) personal data of the MRTD holder
 - (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
 - (2) the digitized portraits (EF.DG2),
 - (3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both¹
 - (4) the other data according to LDS (EF.DG5 to EF.DG16) and
 - (5) the Document security object (SO_D).

¹ These additional biometric reference data are optional. Existing data are protected by means of extended access control.

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

This security target 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 Basic Access Control Mechanism, and
- iii. in authenticity by the Active Authentication of the MRTD's chip.

This security target does not address the Extended Access Control as optional security mechanism.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system:

- (i) reads optically the MRTD,
- (ii) authenticates itself as inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO-9303], normative appendix 5.

The Active 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 the LDS Document Security Object (SOD) from MRTD

- iii. the inspection system reads public key required for Active authentication from LDS DG15 and verifies by means of the Passive Authentication the authenticity of the MRTD's Active Authentication Public Key using the Document Security Object,
- iv. the inspection system submits the TOE's Active Authentication command and includes a generated 8 bytes random number as challenge data.
- v. The TOE signs this challenge with the MRTD's Active Authentication Private Key and returns the signed challenge response (authentication data),
- vi. the inspection system reads the signed challenge response and verifies its signature.

1.4.3 TOE life cycle

The TOE life cycle is described in terms of its four life cycle phases. (With respect to the [SIC-PP], the TOE life-cycle is additionally subdivided into 7 steps in the PP. These steps are denoted too in the following although the sequence of the steps differs for the TOE life cycle).

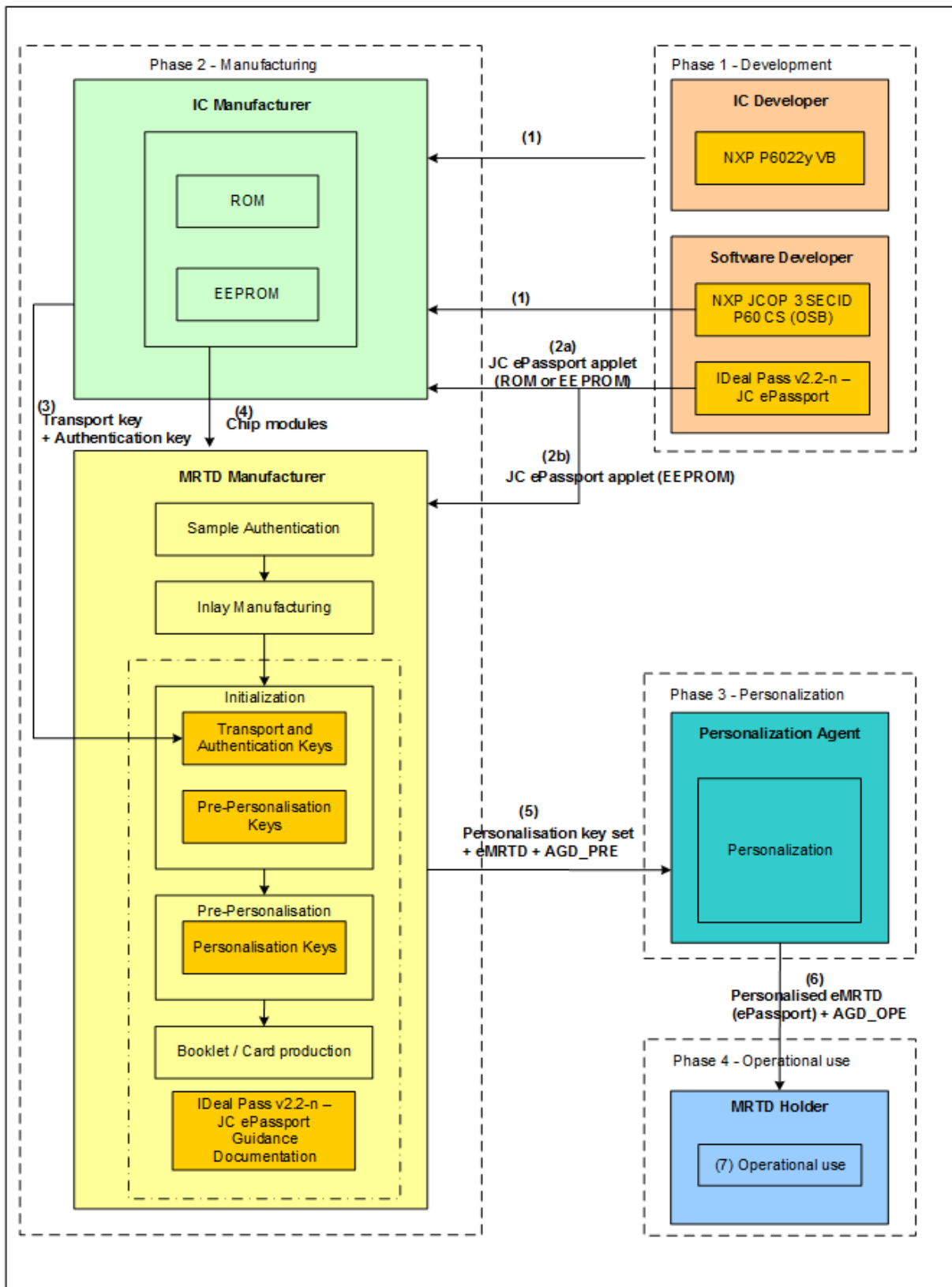


Figure 2: TOE life-cycle

Actors :

IC Developer, IC Manufacturer	NXP
Software Developer	Platform: NXP ePassport applet: IDEMIA R&D sites (Osny and Noida)
Travel document manufacturer	IDEMIA (Haarlem, NL)

1.4.3.1 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.

The IC developer also acts as the developer of the embedded software (operating system), which is the NXP JCOP 3 SECID P60 CS (OSB) open platform.

(Step 2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the NXP JCOP 3 SECID P60 CS (OSB) open platform and develops the ePassport application and the guidance documentation associated with these TOE components.

The ePassport application (i.e. the IDeal Pass v2.2-n - BAC JC ePassport Applet run time code) may be integrated either in ROM or in EEPROM of the chip. Depending on the intention:

- (a) the ePassport application is securely delivered directly from the software developer (IDEMIA development dept.) to the IC manufacturer (NXP). The applet code will be integrated into the ROM mask code (or EEPROM) by the IC manufacturer, or
- (b) either the ePassport application and the guidance documentation are securely delivered directly from the software developer (IDEMIA development dept.) to the travel document manufacturer (IDEMIA production dept.).

1.4.3.2 Phase 2 "Manufacturing"

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software, the parts of the travel document's chip Embedded Software and in case of alternative a) the ePassport application in the non-volatile non-programmable memories (ROM).

The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacturer to the travel document manufacturer.

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

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

(Step5) The travel document manufacturer

- I. adds the IC Embedded Software or part of it in the non-volatile programmable memories (for instance EEPROM) if necessary and in case of alternative (b), loads the ePassport application into the non-volatile programmable memories (for instance EEPROM) if necessary,
- II. creates the ePassport application and
- III. equips the travel document's chips with pre-personalization Data.

BAC PP Application note 1: Creation of the application for this TOE implies Applet instantiation.

For this Security Target the following name mappings to the protection profile [BAC-PP] apply:

- MRTD's chip Dedicated SW = Low level IC libraries
- travel document's chip Embedded Software = NXP JCOP 3 SECID P60 CS (OSB) open platform.
- ePassport application = the IDeal Pass v2.2-n - BAC JC ePassport Applet run time code or an instantiation of it.
- Pre-personalization Data = Personalization Agent Key Set, Card Production Life Cycle (CPLC) data and buffer settings.

Both the underlying platform and the IDeal Pass v2.2-n - BAC JC ePassport applet provide configuration and life-cycle management functions required for TOE preparation. TOE preparation steps are performed in manufacturing phase and consist of the following 2 activities:

1. Platform initialisation
2. Pre-personalisation

Platform initialization

Platform initialization consists of the configuration of the NXP JCOP 3 SECID P60 CS (OSB) open platform in accordance with requirements specified in the platform administrator guidance [PLTF-PRE] by using the dedicated platform commands. Furthermore the Pre-Personalisation Agent key set is installed and (a part of) the CPLC data is updated. To prevent unattended tracing of the MRTD document, the NXP JCOP 3 SECID P60 CS (OSB) open platform is configured such that unauthenticated access to any platform unique identifiable data is not possible.

Pre-personalisation

The pre-personalisation consists of the following steps:

- a. IC (chip) Authentication and getting chip access with the pre-personalisation key set.
- b. [optional] In case of the IDeal Pass v2.2-n - BAC JC ePassport Applet runtime code does not reside in ROM, it is loaded into EEPROM.
- c. Create applet instance for IDeal Pass v2.2-n - BAC JC ePassport Applet (i.e. installation of the IDeal Pass v2.2-n - BAC JC ePassport Applet);
- d. Set the MRTD applet irreversibly in its PERSONALISATION life-cycle state by installation of the Personalisation Agent specific personalization key set.

During step (c) the CPLC data with the IC Identifier is configured in the ePassport application instance as well as the other pre-personalisation data. The last step (d) finalizes the TOE. This is the moment the TOE starts to exist and is ready for delivery to the Personalisation Agent. The guidance documentation for the Personalisation Agent is [AGD_PRE].

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

1.4.3.3 Phase 3 "Personalisation of the travel document"

(Step 6) The personalization of the MRTD includes:

- i. the survey of the MRTD holder's biographical data,
- ii. the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- iii. the printing of the visual readable data onto the physical MRTD,
- iv. the writing of the TOE User Data and TSF Data into the logical MRTD and
- v. the configuration of the TSF if necessary.

The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of:

- i. the digital MRZ data (EF.DG1),
- ii. the digitized portrait (EF.DG2), and
- iii. the document security object.

The signing of the Document security object by the Document signer [ICAO-9303] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance [AGD_OPE] for TOE use if necessary) is handed over to the MRTD holder for operational use.

BAC PP Application note 2

The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [CC-1] §92) comprise (but are not limited to) the Personalization

Agent Authentication Key(s), the Basic Authentication Control Key and (for this Security Target) the Active Authentication Key.

BAC PP Application note 3:

This Security Target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [ICAO-9303]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

The Personalization Agent authenticates by using two symmetric keys (MAC and ENC). In Personalisation life-cycle state the TOE enforces mutual authentication between Personalisation Agent and TOE based on either of the following symmetric key authentication mechanism:

- ICAO BAC authentication mechanism and secure messaging protocol defined in [ICAO-9303] for 112 bits 3DES with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.
- ISO18013 BAP authentication mechanism defined in [ISO18013-3] for AES-128, 192 or 256 bits using AES secure messaging (CMAC, IV value, tags etc.) as specified in EAC TR-03110 [TR-03110-1] with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.

1.4.3.4 Phase 4 "Operational Use"

(Step 7) The TOE is used as MRTD's 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.

BAC PP Application note 4: The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 "Operational Use". This will imply an update of the Document Security Object including the re-signing by the Document Signer.

BAC PP Application note 5: The intention of this Security Target is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this

phase 2 or later. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

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

1.4.3.5 Non-TOE hardware/software/firmware required by the TOE

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

2 Conformance Claims

2.1 CC Conformance Claim

This security target claims to be conformant to the Common Criteria version 3.1, which comprises

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [CC-1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [CC-2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [CC-3]

as follows:

- Part 2 extended with
 - FAU_SAS Audit data storage
 - FCS_RND Generation of random numbers
 - FIA_API Authentication proof of identity
 - FMT_LIM Limited capabilities and availability
 - FPT_EMSEC TOE emanation
- Part 3 conformant

The Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012 [CEM] has been taken into account.

2.2 PP Claim

This security target claims strict conformance to:

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

2.3 Package Claim

This ST is conforming to assurance package EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3 defined in CC part 3 [CC-3].

2.4 PP Conformance Rationale

This ST is claimed to be strictly conformant to the above mentioned PP [BAC-PP]. A detailed justification is given in the following.

2.4.1 Main aspects

- The TOE description (ch. 1.4) is based on the TOE description of [BAC-PP, 2]. It was only enhanced by product specific details.
- All definitions of the security problem definition in [BAC-PP, 3] have been taken exactly from the PP in the same wording.
- All security objectives have been taken exactly from [BAC-PP, 4] in the same wording with one exception (see ch. 2.3.2 below)
- The part of extended components definition has been taken originally from [BAC-PP, 5].
- All SFRs for the TOE have been taken originally from the [BAC-PP, 5.1] added by according iterations, selections and assignments.
- The security assurance requirements (SARs) have been taken originally from the PP.

2.4.2 Overview of differences between the PP and the ST

Assets

As a feature that can be optionally configured, the TOE supports **Active Authentication** which - according to [ICAO-9303] - prevents copying the SO_D and proves that it has been read from the authentic chip. It proves that the chip has not been substituted.

Threats

The threat **T.Counterfeit** has been added to describe an unauthorized copy or reproduction of a genuine MRTD's chip.

T.Counterfeit

MRTD's Chip

Adverse action: An attacker with high attack potential produces an unauthorized 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.

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

Asset: authenticity of logical MRTD data,

Assumptions

One assumption was added to cover Active Authentication during personalization:

A.Pers_Agent_AA Personalization of the MRTD's chip (Active Authentication)

Additionally to A.Pers_Agent, the Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.

Security objectives for the TOE

The **OT.Chip_Auth_Proof** was added to cover also Active Authentication as follows:

OT.Chip_Auth_Proof Proof of MRTD'S chip authenticity

The TOE must support the Basic and General 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 [ICAO-9303]. The authenticity prove provided by MRTD's chip shall be protected against attacks with high attack potential.

Security Objectives for the Environment

The **OE.Auth_Key_MRTD** was added to consider the AA Key pair.

The **OE.AA_MRTD** has been added by the Basic and General inspection systems. These additions to the original objectives of the PP do not contradict with any other objective nor mitigate a threat (or part of a threat) meant to be addressed by security objectives for the TOE in the PP.

Their definitions are:

OE.Auth_Key_MRTD MRTD Authentication Key

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

- i. generate the MRTD's Active Authentication Key Pair,*
- ii. store the Active Authentication Private Key, and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 (if generated), and*
- iii. 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.

OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the Receiving State 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 [ICAO-9303].*

OE.AA_MRTD Active Authentication – Inspection Systems

An Active Authentication (Basic, General or Extended) Inspection system performs all the functions of the Basic, General, respectively Extended Inspection System, and verifies the IC authenticity with an RSA or ECDSA signature generated by the MRTD (if available).

Security functional requirements

The Security Target enhances the following security functional requirements to support Active Authentication:

- FDP_ACF.1 Security attribute based access control- Basic Access Control
- FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write
- FMT_MTD.1/KEY_READ Management of TSF data – Key Read
- FPT_EMSEC.1/ TOE Emanation
- FMT_SMR.1 Security roles

This Security Target adds the following security functional requirements to support Active Authentication:

- FCS_COP.1/SIG_GEN Cryptographic operation – RSA or ECDSA Signature
- FIA_API.1/AA Authentication proof of identity

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 Data

The logical MRTD data consists of the EF.COM and the data groups DG1 to DG16 (with different security needs) and the Document security object EF.SOD according to LDS [ICAO-9303]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Active Authentication Public Key (EF.DG15) is used by the inspection system for Active Authentication of the chip. The Chip Authentication Public Key (EF.DG14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

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

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

The TOE prevents access to sensitive User Data

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

A sensitive asset is the following more general one.

Authenticity of the 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 Users / Subjects

This security target considers the following subjects:

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.

Personalization Agent

The agent is acting on the behalf of the issuing State or Organisation 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 [ICAO-9303].

Terminal

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

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 contactless/contact based 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.
- iv. recommends to perform Active Authentication (AA). AA verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.

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.

MRTD Holder

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

Traveler

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

Attacker

A threat agent trying

- i. to identify and to trace the movement the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD),
- ii. to read or to manipulate the logical MRTD without authorization, or
- iii. to forge a genuine MRTD.

BAC PP Application note 7: 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.

3.3 Threats

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

3.3.1 Threats to be averted by the TOE and its environment

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

T.Chip_ID

Identification of MRTD's chip

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

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

Asset: Anonymity of user

T.Skimming

Skimming the logical MRTD

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

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

Asset: confidentiality of logical MRTD data

T.Eavesdropping between TOE and inspection system

Eavesdropping to the communication

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

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

Asset: confidentiality of logical MRTD data

T.Forgery

Forgery of data on MRTD's chip

Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face

recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless/contact chip.

Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate MRTDs
Asset: authenticity of logical MRTD data,

The TOE shall avert the threats as specified below.

T.Abuse-Func Abuse of Functionality

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

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

Threat agent: having high attack potential, being in possession of a legitimate MRTD
Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

T.Information_Leakage Information Leakage from MRTD's chip

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

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

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

Asset: confidentiality of logical MRTD and TSF data

T.Phys-Tamper Physical Tampering

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

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

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

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

T.Malfunction Malfunction due to Environmental Stress

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

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

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

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

T.Counterfeit MRTD's chip²

Adverse action: An attacker with high attack potential produces an unauthorized 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.

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

Asset: authenticity of logical MRTD data

3.4 Organisational Security Policies

The TOE shall comply to the following organization security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1 [CC-1], sec. 3.2).

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.

² Added by the ST author

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) 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 [ICAO-9303].

BAC PP Application note 10: The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO-9303]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

3.5 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 4 to 6

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

A.MRTD_Delivery MRTD delivery during steps 4 to 6

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

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

A.Pers_Agent Personalization of the MRTD's chip

The Personalization Agent ensures the correctness of

- i. the logical MRTD with respect to the MRTD holder,
- ii. the Document Basic Access Keys,
- iii. the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip,

- iv. the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip, and
- v. 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 (Active Authentication)

Additionally to A.Pers_Agent the Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.

A.Insp_Sys Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State

- i. examining an MRTD presented by the traveler and verifying its authenticity and
- ii. verifying the traveler as MRTD holder.

The Basic Inspection System for global interoperability

- i. includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and
- ii. implements the terminal part of the Basic Access Control [ICAO-9303].

The Basic Inspection System reads the logical MRTD being under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

BAC PP Application note 8: According to [ICAO-9303] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

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

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [ICAO-9303], 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.



BAC PP Application note 9: 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.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO-9303] 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.

BAC PP Application note 11: The OT.AC_Pers implies that (1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization, (2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

OT.Data_Int Integrity of personal data

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

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.

BAC PP Application note 12: 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' [ICAO-9303] 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 protection profile. Thus the read access must be prevented even in case of a successful BAC Authentication.

OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the 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.

BAC PP Application note 13: The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the MRTD". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless/contact interface before successful authentication as Basic Inspection System or as Personalization Agent.

The TOE must support the General and 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 Active Authentication as defined in [ICAO-9303]5. The authenticity prove provided by MRTD's chip shall be protected against attacks with enhanced basic attack potential.

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

OT.Chip_Auth_Proof Proof of MRTD'S chip authenticity³

The TOE must support the Basic and General 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 [ICAO-9303]. The authenticity prove provided by MRTD's chip shall be protected against attacks with enhanced basic attack potential.

OT.Prot_Abuse-Func Protection against Abuse of Functionality

The TOE must prevent functions of the TOE which may not be used after TOE delivery can be abused in order

- i. to disclose critical User Data,
- ii. to manipulate critical User Data of the IC Embedded Software,
- iii. to 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.

BAC PP Application note 14: 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 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

³ Added by the ST author

- 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.

BAC PP Application note 15: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE's internals.

4.2 Security Objectives for the Operational Environment

Issuing State or Organization

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

OE.MRTD_Delivery Protection of the 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 the behalf of the issuing State or Organisation

- i. establish the correct identity of the holder and create biographic data for the MRTD,
- ii. enrol 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 Key Pair,
- ii. ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment, and
- iii. distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity.

The Issuing State or Organization must

- i. generate a cryptographic secure Document Signing 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 Signing 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 [ICAO-9303].

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' [ICAO-9303] 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.Auth_Key_MRTD MRTD Authentication Key⁴

The issuing State or Organization has to establish the necessary public key infra-structure in order to

- i. generate the MRTD's Active Authentication Key Pair,
- ii. store the Active Authentication Private Key, and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 (if generated), and
- iii. 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 Chip and Active Authentication Public Key by means of the Document Security Object.

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 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 [ICAO-9303].

⁴ Added by the ST author

OE.AA_MRTD Active Authentication - Inspection Systems

An Active Authentication (Basic, General or Extended) Inspection system performs all the functions of the Basic, General, respectively Extended Inspection System, and verifies the IC authenticity with an RSA or ECDSA signature generated by the MRTD (if available).

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 Signing Public Key maintaining their authenticity and availability in all inspection systems.

OE.Prot_Logical_MRTD Protection of data of 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

The following table provides an overview for security objectives coverage.

	OT.AC_Pers ⁵	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunton	OT.Chip_Auth_Proof ⁶	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Auth_Key_MRTD ⁷	OE.Exam_MRTD ⁸	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.AA_MRTD
T.Chip-ID				X										X					
T.Skimming			X											X					

⁵ Added in this ST with respect to [BAC-PP-055]

⁶ Added in this ST with respect to [BAC-PP-055]

⁷ Added in this ST with respect to [BAC-PP-055]

⁸ Added in this ST with respect to [BAC-PP-055]

	OT.AC_Pers ⁵	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Chip_Auth_Proof ⁶	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Auth_Key_MRTD ⁷	OE.Exam_MRTD ⁸	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.AA_MRTD
T.Eavesdropping			x																
T.Forgery	x	x				x							x				x		
T.Abuse-Func					x							x							
T.Information_Leakage						x													
T.Phys-tamper							x												
T.Malfunction								x											
T.Counterfeit ⁹									x						x	x			x
P.Manufact				x															
P.Personalization	x			x								x							
P.Personal_Data		x	x																
A.MRTD_Manufact										x									
A.MRTD_Delivery											x								
A.Pers_Agent												x							
A.Pers_Agent_AA ¹⁰												x							
A.Insp_Sys																x		x	x
A.BAC-Keys														x					

Table 1: Security Objective Rationale

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

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

⁹ Added in this ST with respect to [BAC-PP-055]

¹⁰ Added in this ST with respect to [BAC-PP-055]

Personalization Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and management of TSF to the Personalization Agent.

The OSP **P.Personal_Data** "Personal data protection policy" requires the TOE

- (i) to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and
- (ii) enforce the access control for reading as decided by the issuing State or Organization.

This policy is implemented by the security objectives **OT.Data_Int** "Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT.Data_Conf** "Confidentiality of personal data" describes the protection of the confidentiality.

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

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

The threat **T.Forgery** "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security

objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRTD passport book according to **OE.Exam_MRTD** "Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive contactless/contact chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** "Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif** "Verification by Passive Authentication".

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

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

The threat **T.Counterfeit** "MRTD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of MRTD's chip authentication" using an authentication key pair to be generated by the issuing state or organization. The Active Authentication Public Key has to be written into EF.DG15 as demanded by **OE.Auth_Key_MRTD** "MRTD Authentication Key". According to **OE.AA_MRTD** "Examination of the MRTD passport book" the Inspection

system has to perform the Active Authentication Protocol to verify the authenticity of the MRTD's chip.

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

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

The assumptions **A.Pers_Agent** "Personalization of the MRTD's chip" and **A.Pers_Agent_AA** "Personalization of the MRTD's chip (Active Authentication)" are covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD" including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the MRTD passport book" which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Active Authentication Protocol to verify the Authenticity of the presented MRTD's chip. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

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

5 Extended Requirements

5.1 Definition of the Family 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.

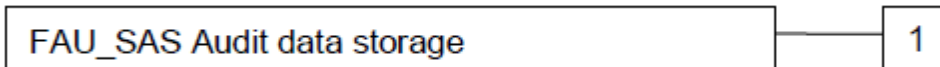
The family "Audit data storage (FAU_SAS)" is specified as follows.

5.1.1 FAU_SAS Audit data storage

Family behavior

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

Component leveling



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1
 There are no management activities foreseen.

Audit: FAU_SAS.1
 There are no actions defined to be auditable.

FAU_SAS.1 Audit Storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide [assignment: authorized users] with the capability to store [assignment: list of audit information] in the audit records.

5.2 Definition of the Family FCS_RND

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.

5.2.1 FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



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

Management: FCS_RND.1
 There are no management activities foreseen.

Audit: FCS_RND.1
 There are no actions defined to be auditable.

FCS_RND.1 Quality Metric for Random Numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3 Definition of the Family 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.

5.3.1 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 levelling:

FIA_API Authentication Proof of Identity

1

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: 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 Definition of the Family FMT_LIM

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

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

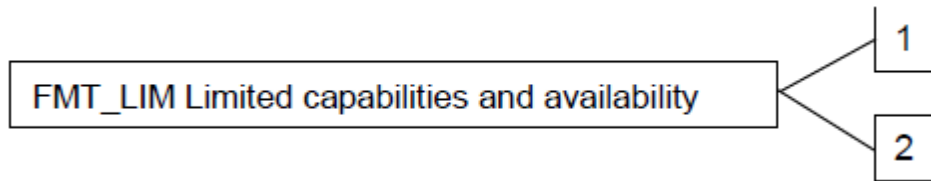
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

5.4.1 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].

5.5 Definition of the Family FPT_EMSEC

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.

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1
There are no management activities foreseen.

Audit: FPT_EMSEC.1
There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6 Security Requirements

6.1 Security Functional Requirements

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.

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

6.1.1 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below. For the extended components definition refer to [BAC-PP] chapter 4.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide the Manufacturer¹¹ with the capability to store the IC Identification Data¹² in the audit records.

Dependencies: No dependencies.

¹¹ [assignment: *authorized users*]

¹² [assignment: *list of audit information*]

BAC PP Application note 17: The manufacturer 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-personalisation data as TSF data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.1.2 Class Cryptographic Support (FCS)

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

FCS_CKM.1 Cryptographic key generation – Key Derivation Function by the MRTD

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm¹³ and specified cryptographic key sizes 112 bit¹⁴ that meet the following: [ICAO-9303], Volume 2, Section IV, Appendix 5¹⁵.

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

¹³ [assignment: cryptographic key generation algorithm]

¹⁴ [assignment: cryptographic key sizes]

¹⁵ [assignment: list of standards]

BAC PP Application note 18: 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 [ICAO-9393], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO-9393], normative appendix A5.1. The algorithm uses the random number RND.ICC generated by the TOE.

TSF as required by FCS_RND.1.

FCS_CKM.4 Cryptographic key destruction - MRTD

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys¹⁶ that meets the following: none¹⁷.

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

BAC PP Application note 19: The TOE shall destroy the Triple-DES encryption key and the Retail MAC message authentication keys for secure messaging.

6.1.2.1 Cryptographic operation (FCS_COP.1)

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

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

Hierarchical to: No other components.

¹⁶ [assignment: cryptographic key destruction method]

¹⁷ [assignment: list of standards]

FCS_COP.1.1/
SHA The TSF shall perform hashing¹⁸ in accordance with a specified cryptographic algorithm SHA-1, SHA-224, SHA-256, SHA-384 or SHA-512¹⁹ and cryptographic key sizes none²⁰ that meet the following: FIPS 180-4 [NIST-180-4]²¹.

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

Bac PP Application note 20: 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 [ICAO-9393].

¹⁸ [assignment: list of cryptographic operations]

¹⁹ [assignment: cryptographic algorithm]

²⁰ [assignment: cryptographic key sizes]

²¹ [assignment: list of standards]

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

Hierarchical to: No other components.

FCS_COP.1.1/
ENC The TSF shall perform secure messaging (BAC)– encryption and decryption²² in accordance with a specified cryptographic algorithm Triple-DES in CBC mode²³ and cryptographic key sizes 112 bit²⁴ that meet the following: FIPS 46-3 [FIPS46] and [ICAO-9303], Volume 2, Appendix 5, A5.3²⁵.

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

BAC Application note 21: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

FCS_COP.1/AUTH Cryptographic operation – Authentication

Hierarchical to: No other components.

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

FCS_COP.1.1/AUTH The TSF shall perform symmetric authentication - encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES and AES²⁶ and cryptographic key sizes respectively 112 bit for Triple-DES and 128,192 and 256 bit for AES²⁷ that meet the following: FIPS 46-3 [FIPS] for Triple-DES and [NIST-197]²⁸.

²² [assignment: *list of cryptographic operations*]

²³ [assignment: *cryptographic algorithm*]

²⁴ [assignment: *cryptographic key sizes*]

²⁵ [assignment: *list of standards*]

²⁶ [selection: Triple-DES, AES]

²⁷ [selection: 112, 128, 168, 192, 256]

²⁸ [selection: FIPS 46-3 [...], FIPS 197 [...]]

BAC PP Application note 22: This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalisation Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

FCS_COP.1/MAC Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/ MAC The TSF shall perform secure messaging – message authentication code²⁹ in accordance with a specified cryptographic algorithm Retail MAC³⁰ and cryptographic key sizes respectively 112 bit³¹ that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)³².

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

BAC PP Application note 23: 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.

FCS_COP.1/SIG_GEN Cryptographic operation – Signature generation by travel document

Hierarchical to: No other components.

²⁹ [assignment: *list of cryptographic operations*]

³⁰ [assignment: *cryptographic algorithm*]

³¹ [assignment: *cryptographic key sizes*]

³² [assignment: *list of standards*]

FCS_COP.1.1/
SIG_GEN The TSF shall perform digital signature generation³³ in accordance with a specified cryptographic algorithm ECDSA and RSA³⁴ with cryptographic key sizes 192, 224, 256, 320, 384, 512 and 521 bits for ECDSA and 1024, 1536, 1792 and 2048 bits for RSA³⁵ that meet the following: ISO15946-2 specified in [ISO15946-2] for ECDSA and ISO9796-2 specified in [ISO9796-2] for RSA, in combination with SHA1, SHA224, SHA256, SHA384 and SHA512 digest algorithms specified in [NIST-180-4] for both ECDSA and RSA signatures³⁶.

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

Guidance: This SFR has been added to this ST in order to support the signing of challenges generated by the Inspection System as part of the optional Active Authentication protocol specified in [ICAO-9303].

³³ [assignment: *list of cryptographic operations*]

³⁴ [assignment: *cryptographic algorithm*]

³⁵ [assignment: *cryptographic key sizes*]

³⁶ [assignment: *list of standards*]

6.1.2.2 Random Number Generation (FCS_RND.1)

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

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet FCS_RNG.1 Quality metric for random numbers of [PLTF-ST]

Dependencies: No dependencies.

BAC PP Application note 24: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

6.1.3 Class FIA Identification and Authentication

BAC PP Application note 25: The following table provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO-9303], Appendix 5
Basic Access Control Authentication Mechanism		Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Active Authentication	FIA_API.1/AA	RSA and ECDSA, (cf. FCS_COP.1/SIG_GEN) RSA: 1536, 1792 and 2048 bits ECDSA: 192, 224, 256, 320, 384, 512 and 521 bits
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	Triple-DES with 112 bit keys or AES with 128, 192 and 256 bit keys (cf. FCS_COP.1/AUTH)

Table 2: Overview on authentication SFR

6.1.3.1 Timing of identification (FIA_UID.1)

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

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

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"³⁷

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.

Dependencies: No dependencies.

BAC PP Application note 26: 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.

BAC PP Application note 27: 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. In the TOE of this ST this

³⁷ [assignment: *list of TSF-mediated actions*]

identifier is randomly selected and will not violate the OT.Identification.

6.1.3.2 Timing of authentication (FIA_UAU.1)

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

- 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"³⁸

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

Dependencies: FIA_UID.1 Timing of identification.

BAC PP Application note 28: The Basic Inspection System and the Personalization Agent authenticate themselves.

³⁸ [assignment: *list of TSF-mediated actions*]

6.1.3.3 Single-use authentication mechanisms (FIA_UAU.4)

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

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

Hierarchical to: No other components.

- FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to
1. Basic Access Control Authentication Mechanism,
 2. Authentication Mechanism based on Triple-DES³⁹.

Dependencies: No dependencies.

BAC PP Application note 29: 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.

BAC PP Application note 30: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO-9303]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

Multiple authentication mechanisms (FIA_UAU.5)

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

³⁹ [assignment: *identified authentication mechanism(s)*]

FIA_UAU.5 Multiple authentication mechanisms

- FIA_UAU.5.1 The TSF shall provide
1. Basic Access Control Authentication Mechanism
 2. Symmetric Authentication Mechanism based on Triple-DES and AES ⁴⁰
- to support user authentication.
- FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:
1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms
 - (a) The Basic Access Control Authentication Mechanism with the Personalization Agent Keys.
 - (b) The Symmetric Authentication Mechanism with the 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.

Dependencies: No dependencies.

BAC PP Application note 31: In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [EAC-PP] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES. The Personalization Agent could be authenticated by using the symmetric AES-based authentication mechanism or other (e.g. the Terminal Authentication Protocol using the Personalization Key, cf. [EAC-PP] FIA_UAU.5.2).

BAC PP Application note 32: 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.

⁴⁰ [assignment: *list of multiple authentication mechanisms*]

6.1.3.4 Re-authenticating (FIA_UAU.6)

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

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

Hierarchical to: No other components.

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 Mechanism⁴¹.

Dependencies: No dependencies.

BAC PP Application note 33: The Basic Access Control Mechanism specified in [ICAO-9303] 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.

BAC PP Application note 34: Note that in case the TOE should also fulfill [EAC-PP] 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.

⁴¹ [assignment: *list of conditions under which re-authentication is required*]

6.1.3.5 Authentication Failure Handling (FIA_AFL.1)

The TOE shall meet the requirement “Authentication Failure Handling (FIA_AFL.1)” as specified below.

FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components.

- FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within one to 32767*⁴² consecutive unsuccessful authentication attempts occur related to *BAC authentication*⁴³.
- FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *wait an administrator configurable time before the next authentication attempt can be performed*⁴⁴.

Dependencies: FIA_UAU.1 Timing of authentication

Application note 35:

In this ST the assigned values for FIA_AFL.1.1 and FIA_AFL.1.2 ensure especially the strength of authentication function as terminal part of the Basic Access Control Authentication Protocol to resist enhanced basic attack potential.

In FIA_AFL.1.1 the TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 32767 consecutive unsuccessful authentication attempts occur related to BAC authentication protocol.

FIA_AFL.1.2 specifies when the defined number of unsuccessful authentication attempts has been met or surpassed, that the TSF shall wait for an administrator configurable time between the receiving the terminal challenge eIFD and sending the TSF response eICC during the BAC authentication attempts.

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

⁴² [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]

⁴³ [assignment: list of authentication events]

⁴⁴ [assignment: list of actions]

FIA_API.1/AA Authentication Proof of Identity - MRTD

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

Hierarchical to: No other components.

FIA_API.1/AA The TSF shall provide an Active Authentication Protocol according to [ICAO-9303]⁴⁵ to prove the identity of the TOE⁴⁶.

Dependencies: No dependencies.

6.1.4 Class FDP User Data Protection

6.1.4.1 Subset access control (FDP_ACC.1)

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

FDP_ACC.1 Subset access control - Basic Access Control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the Basic Access Control SFP⁴⁷ on terminals gaining write, read and modification access to the data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD⁴⁸.

Dependencies: FDP_ACF.1 Security attribute based access control

⁴⁵ [assignment: *authentication mechanism*]

⁴⁶ [assignment: *authorized user or rule*]

⁴⁷ [assignment: *access control SFP*]

⁴⁸ [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

6.1.4.2 Security attribute based access control (FDP_ACF.1)

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

FDP_ACF.1 Security attribute based access control- Basic Access Control⁴⁹

Hierarchical to: No other components.

- FDP_ACF.1.1 The TSF shall enforce the Access Control SFP⁵⁰ 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 terminals⁵¹.
- 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 data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD and perform Active Authentication.
- FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:
none⁵².

⁴⁹ The bold text below has been added to allow the use of active authentication.

⁵⁰ [assignment: *access control SFP*]

⁵¹ [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

FDP_ACF.1.4

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. No terminal is 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

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

BAC PP Application note 36: The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this protection profile (cf. [EAC-PP] for details).

6.1.4.3 Inter-TSF-Transfer

BAC PP Application note 37: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

FDP_UCT.1 Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

FDP_UCT.1.1

The TSF shall enforce the Access Control SFP⁵³ to be able to transmit and receive⁵⁴ user data in a manner protected from unauthorized disclosure.

⁵² [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

⁵³ [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

⁵⁴ [selection: *transmit, receive*]

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

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

FDP_UIT.1/ Data exchange integrity - MRTD

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the Access Control SFP⁵⁵ to be able to transmit and receive⁵⁶ user data in a manner protected from modification, deletion, insertion and replay⁵⁷ errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay⁵⁸ has occurred.

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

6.1.5 Class FMT Security Management

BAC PP Application note 38: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

⁵⁵ [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

⁵⁶ [selection: *transmit, receive*]

⁵⁷ [selection: *modification, deletion, insertion, replay*]

⁵⁸ [selection: *modification, deletion, insertion, replay*]

- FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:
1. Initialization,
 2. Pre-personalization
 3. Personalization⁵⁹.

Dependencies: No Dependencies

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

FMT_SMR.1 Security roles

Hierarchical to: No other components.

- FMT_SMR.1.1 The TSF shall maintain the roles
1. Manufacturer,
 2. Personalization Agent,
 3. Basic Inspection System⁶⁰.
- FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification.

BAC PP Application note 39: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below. For the extended components definition is referred to [BAC-PP] chapter 4.

⁵⁹ [assignment: *list of security management functions to be provided by the TSF*]

⁶⁰ [assignment: *the authorized identified roles*]

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 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 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 attacks⁶¹.

Dependencies: FMT_LIM.2 Limited availability.

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below. For the extended components definition refer to [BAC-PP] chapter 4.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability 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 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 attacks⁶².

Dependencies: FMT_LIM.2 Limited capabilities.

BAC PP Application note 40: The formulation of "Deploying Test Features ..." in

⁶¹ [assignment: *Limited capability and availability policy*]

⁶² [assignment: *Limited capability and availability policy*]

FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term “software” in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

BAC PP Application note 41: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

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

Hierarchical to: No other components.

FMT_MTD.1/INI_ENA The TSF shall restrict the ability to write⁶³ the Initialization Data and Pre-personalization Data⁶⁴ to the Manufacturer⁶⁵.

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

BAC PP Application note 42: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

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

Hierarchical to: No other components.

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to disable read access for users to⁶⁶ the Initialization Data⁶⁷ to the Personalization Agent⁶⁸.

⁶³ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁶⁴ [assignment: *list of TSF data*]

⁶⁵ [assignment: *the authorized identified roles*]

⁶⁶ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁶⁷ [assignment: *list of TSF data*]

⁶⁸ [assignment: *the authorized identified roles*]

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

BAC PP Application note 43: 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.

FMT_MTD.1/ KEY_WRITE Management of TSF data – Key Write⁶⁹

Hierarchical to: No other components.

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to write⁷⁰ the Document Basic Access Keys and the Active Authentication Keys⁷¹ to the Personalization Agent⁷².

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

FMT_MTD.1/KEY_READ Management of TSF data – Key Read⁷³

Hierarchical to: No other components.

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read⁷⁴ the Document Basic Access Keys, the Active Authentication Private Key and the Personalization Agent Keys⁷⁵ to none⁷⁶.

⁶⁹ The bold text below has been added to allow the use of active authentication.

⁷⁰ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁷¹ [assignment: *list of TSF data*]

⁷² [assignment: *the authorized identified roles*]

⁷³ The bold text below has been added to allow the use of active authentication.

⁷⁴ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

⁷⁵ [assignment: *list of TSF data*]

⁷⁶ [assignment: *the authorized identified roles*]

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

BAC PP Application note 44: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

6.1.6 Protection of the Security Functions

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

The TOE shall meet the requirement "TOE Emanation (FPT_EMSEC.1)" as specified below. For the extended components definition refer to [BAC-PP] chapter 4.

FPT_EMSEC.1 TOE Emanation⁷⁷

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit variations in power consumption or timing during command execution⁷⁸ in excess of non-useful information⁷⁹ enabling access to Personalisation Agent Authentication Key, **Active Authentication Private Key**,⁸⁰ and none⁸¹

⁷⁷ The bold text below has been added to allow the use of active authentication.

⁷⁸ [assignment: types of emissions]

⁷⁹ [assignment: specified limits]

⁸⁰ [assignment: list of types of TSF data]

⁸¹ [assignment: list of types of user data]

FPT_EMSEC.1.2 The TSF shall ensure any users⁸² are unable to use the following interface smart card circuit contacts⁸³ to gain access to Personalization Agent Authentication Key, Active Authentication Private Key,⁸⁴ and none⁸⁵.

Dependencies: No other components.

BAC PP Application note 45: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless/contact interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

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

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

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

- (1) exposure to operating conditions where therefore a malfunction could occur,
- (2) failure detected by TSF according to FPT_TST.1⁸⁶.

Dependencies: ADV_SPM.1 Informal TOE security policy model

⁸² [assignment: *type of users*]

⁸³ [assignment: *type of connection*]

⁸⁴ [assignment: *list of types of TSF data*]

⁸⁵ [assignment: *list of types of user data*]

⁸⁶ [assignment: *list of types of failures in the TSF*]

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

- FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up⁸⁷ to demonstrate the correct operation of the TSF.
- FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
- FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

BAC PP Application note 46: If the MRTD’s chip uses state of the art smart card Technology, it will run some self tests at the request of the authorized user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the “authorized user” Manufacturer in the Phase 2 Manufacturing. Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 “Operational Use”, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

- FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing⁸⁸ to the TSF⁸⁹ by responding automatically such that the SFRs are always enforced.

Dependencies: No dependencies.

BAC PP Application note 47: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of

⁸⁷ [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions]

⁸⁸ [assignment: physical tampering scenarios]

⁸⁹ [assignment: list of TSF devices/elements]

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.

BAC PP Application note 48: 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.

The following security functional requirements protect the TSF against bypassing and support the separation of TOE parts.

6.2 Security Assurance Requirements

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

- Evaluation Assurance Level 4 (EAL4)

and augmented by the following component:

- ADV_FSP.5
- ADV_INT.2
- ADV_TDS.4
- ALC_DVS.2
- ALC_CMS.5
- ALC_TAT.2
- ATE_DPT.3

6.3 Security Requirements Rationale

6.3.1 Functional Security Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT. Data_Conf	OT.Identification	OT:Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Chip_Auth_Proof ⁹⁰
FAU_SAS.1				x					
FCS_CKM.1	x	x	x						
FCS_CKM.4	x		x						
FCS_COP.1/SHA	x	x	x						
FCS_COP.1/ENC	x	x	x						
FCS_COP.1/AUTH	x	x							
FCS_COP.1/MAC	x	x	x						
FCS_COP.1/SIG_GEN ⁹¹									x
FCS_RND.1	x	x	x						
FIA_UID.1			x	x					
FIA_AFL.1			x	x					
FIA_API.1/AA ⁹²									x
FIA_UAU.1			x	x					
FIA_UAU.4	x	x	x						
FIA_UAU.5	x	x	x						
FIA_UAU.6	x	x	x						
FDP_ACC.1	x	x	x						
FDP_ACF.1	x	x	x						x
FDP_UCT.1	x	x	x						
FDP_UIT.1	x	x	x						
FMT_SMF.1	x	x	x						
FMT_SMR.1	x	x	x						
FMT_LIM.1								x	
FMT_LIM.2								x	

⁹⁰ TOE objective added in this ST with respect to [PP-BAC]

⁹¹ SFR added in this ST with respect to [PP-BAC]

⁹² SFR added in this ST with respect to [PP-BAC]

	OT.AC_Pers	OT.Data_Int	OT. Data_Conf	OT.Identification	OT:Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Chip_Auth_Proof ⁹⁰
FMT_MTD.1/INI_ENA				x					
FMT_MTD.1/INI_DIS				x					
FMT_MTD.1/KEY_WRITE	x	x	x						x
FMT_MTD.1/KEY_READ	x	x	x						x
FPT_EMSEC.1	x				x				
FPT_TST.1					x		x		
FPT_FLS.1	x				x		x		
FPT_PHP.3	x				x	x			

Table 3: Coverage of Security Objective for the TOE by SFR

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

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [BSI-PP-0056, Version 1.10, 25th March 2009] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the

Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentiality of these keys.

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

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

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

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

authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

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

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

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

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

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

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

- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

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

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

The security objective **OT.Chip_Auth_Proof** "Proof of MRTD's chip authenticity" is ensured by Active Authentication provided by FIA_API.1/AA proving the identity of the TOE.

The Active Authentication defined by FCS_COP.1/SIG_GEN for the generation of the RSA and ECDSA Signature is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ. According to FDP_ACF.1, only the successfully authenticated Basic, Generic and Extended Inspection Systems are allowed to request active authentication (FDP_ACF.1.2, rule 2).

6.3.2 Dependencies

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

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

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Justification 1 for non-satisfied dependencies Fulfilled by FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1 and FCS_CKM.4,
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Justification 2 for non-satisfied dependencies
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1 and FCS_CKM.4
FCS_COP.1/SIG_GEN	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1, FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled
FIA_API.1/AA	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of authentication	Fulfilled
FIA_UAU.4/	No dependencies	n.a.
FIA_UAU.5/	No dependencies	n.a.
FIA_UAU.6/	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 3 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.1, justification 4 for non-satisfied dependencies
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1, justification 4 for non-satisfied dependencies
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled
FMT_LIM.1	FMT_LIM.2	Fulfilled
FMT_LIM.2	FMT_LIM.1	Fulfilled
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled

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

Table 4: Dependencies between the SFR for the TOE

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

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

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

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

No. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use of secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not

provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

6.3.3 Rationale for the Security Assurance Requirements

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

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

The component ALC_DVS.2 has no dependencies.

Notice that it the augmentation components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3 come from the EAL5 level.

7 TOE Summary Specification

7.1 TOE Summary Specification

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

The TOE provides security features which can be associated into following groups:

- Identification and Authentication mechanisms
- Cryptographic functions support
- Access control /Storage and protection of logical MRTD data
- Secure messaging
- Security and Life-cycle management

Moreover the TOE will protect itself against interference, logical tampering and bypass. The security functionality of the TOE respectively the **IDeal Pass v2.2-n - BAC JC ePassport** applet will be externally available to the user by APDU commands according to the access conditions specified by the according policies considering the life cycle state, user role and security state.

Remark:

The numbering of the security functions is consistent with the Security Target [ST-SAC-EAC], where it supports in addition to BAC and Active Authentication also PACEV2 and Extended Access Control (EACv1) in accordance with respectively [ICAO-9303] and [TR-03110-1] and [TR-03110-3].

7.1.1 SF.IA Identification and Authentication

The different authentication mechanisms are supported by APDU commands and parameters using the cryptographic functions provided by the platform. The authentication mechanisms are enforced by protocols and APDU methods as specified in the functional specification.

The TOE supports the following authentication mechanisms:

- **SF.IA.0:** Basic Access Control Authentication mechanism (BAC)
- **SF.IA.4:** Authentication of the Personalization Agent with a personalisation key set based on a symmetric authentication mechanism.
- **SF.IA.5:** Active Authentication

7.1.2 SF.CF Cryptographic functions support

Cryptographic function support is provided by the underlying NXP JCOP 3 SECID P60 CS (OSB) open platform, i.e. the TOE relies on the underlying platform for performing its required cryptographic operations.

SF.CF Cryptographic functions include:

- **SF.CF.1:** 3DES and AES cipher operations for secure messaging
- **SF.CF.2:** Digest calculations (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512)
- **SF.CF.3:** Signature generation (ECDSA, RSA)
- **SF.CF.6:** Cryptographic key generation
- **SF.CF.7:** Key Destruction
- **SF.CF.8:** True Random Number generation

7.1.3 SF.ILTB Protection against interference, logical tampering and bypass

SF.ILTB.1

Protection against interference, logical tampering and bypass

Security domains are supported by the Java Card platform used by the TOE underlying NXP JCOP 3 SECID P60 CS (OSB) open platform. The NXP JCOP 3 SECID P60 CS (OSB) open platform provides protection against physical attack and performs self-tests as described in [PLTF-ST].

The platform protects the TOE against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.

The IDeal Pass v2.2-n - BAC JC ePassport Applet uses transient memory where a hardware reset always reverts the IDeal Pass v2.2-n - BAC JC ePassport Applet into an unauthenticated state.

7.1.4 SF.AC Access control / Storage and protection of logical travel document data

SF.AC.1

Access control / Storage and protection of logical travel document data

The TOE provided access control, storage and protection of logical travel document data including access control to MRTD data. The TOE implements the subjects, objects, security attributes and rules according to the security attribute based access control. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

7.1.5 SF.SM Secure Messaging

SF.SM.1

Secure Messaging

Secure messaging MAC and ENC operations are performed by the TOE's platform.

In PERSONALISATION life-cycle state the TOE supports 3DES or AES secure messaging in ENC_MAC mode, after a successful mutual authentication between TOE and Personalisation Agent terminal have been accomplished (see SF.I&A.4):

- ICAO secure messaging protocol defined in [ICAO-9303] for 112 bits 3DES with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.
- ISO18013 BAP secure messaging defined in [ISO18013-3] for AES-128, 192 or 256 bits using AES secure messaging (CMAC, IV value, tags etc.) as specified in EAC TR-03110 [TR-03110-1] with pre-installed MAC, ENC (and KEK) keys as Personalisation Agent Key set.

In OPERATIONAL life-cycle state the TOE runs secure messaging in ENC_MAC mode using 112 bit Triple-DES in CBC mode only after successful BAC authentication. The MAC is calculated according to the Retail MAC cryptographic algorithm specified in [ISO9797], MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2. Secure messaging in ENC_MAC mode is established during BAC and is based on SF.CF.1, 6 and 8.

SF.SM.2

Secure Messaging – Re-authentication

In OPERATIONAL life-cycle state, the Retail MAC for 3DES is part of every APDU command/response when secure messaging is active after a successful BAC authentication has been accomplished. Re-authentication after reset of the SM protocol is assured by accepting only valid mandatory MAC cryptograms.

In PERSONALISATION life-cycle state either the Retail MAC for 3DES or the CMAC for AES are part of every APDU command/response when secure messaging is active after a successful mutual authentication between TOE and Personalisation Agent has been accomplished. Re-authentication after reset of the SM protocol is assured by accepting only valid (mandatory) MAC or CMAC cryptograms.

7.1.6 SF.LCM Security and life cycle management

For the IDEal Pass v2.2-n - BAC JC ePassport the following life-cycle phases have been identified:

1. Manufacturing phase
2. Personalisation phase
3. Operational phase
4. Termination phase

The life-time phases are reflected within the IDEal Pass v2.2-n - BAC JC ePassport applet by an internal life-cycle state machine which supports the following life-cycle states:

1. Not instantiated (applet resides in EEPROM or ROM)
2. PRE-PERSONALISATION state
3. PERSONALISATION state
4. OPERATIONAL state
5. TERMINATED state (irreversibly)

Each life-cycle phase (or state) has its typical user acting as role holder.

Life-cycle phase	Life-cycle state (maintained by applet)	Role
<i>Manufacturing phase</i>	- (Applet not instantiated)	IC Manufacturer
	- (Applet not instantiated)	MRTD Manufacturer (Platform initialisation)
	PRE-PERSONALISATION	MRTD Manufacturer (Pre-personalisation)
<i>Personalisation phase</i>	PERSONALISATION	Personalisation Agent
<i>Operational phase</i>	OPERATIONAL	Basic or Extended Inspection system
<i>Termination phase</i>	TERMINATED	None

Table 5: Life-cycle phases and states

All role holders in Manufacturing, Pre-Personalisation and Personalisation phases are identified by cryptographic authentication keys. In Operational phase the BAC password is required to authenticate the Basic or Extended Inspection System in order to get access to the non-sensitive ICAO LDS datagroups.

The IDEal Pass v2.2-n - BAC JC ePassport Applet maintains the internal life-cycle state the moment the applet is installed. This state, together with the access control mechanisms force the Terminal into a specific role, for the pre-personalisation and subsequent, personalisation and operational phases. The

phases (and corresponding life-cycle states) are controlled by APDU commands. The life-cycle phase and state transitions are irreversible.

SF.LCM.1

Management of phases, roles and MRTD life-cycle states – Manufacturing phase

This security feature supports the management of roles and life-cycle state during Manufacturing phase.

SF.LCM.2

Management of phases, roles and MRTD life-cycle states – Personalisation phase

This security feature supports the management of roles and life-cycle state during Personalisation phase.

SF.LCM.4

Protection of test features

The IDeal Pass v2.2-n - BAC JC ePassport Applet does not have any dedicated test features implemented.

The test features of the NXP JCOP 3 SECID P60 CS (OSB) open platform are protected by ways described in [PLTF-ST] and guidance documentation.

SF.LCM.5

Protection of keys and BAC password

In PRE-PERSONALISATION life-cycle state, the personalisation Agent Key Set is installed on the TOE's platform and protected by the platform.

In all TOE life-cycle states the Personalization Agent Key set (MAC, ENC, KEK), the BAC keys (derived from MRZ) and the Active Authentication Private Key are also protected from disclosure. The IDeal Pass v2.2-n - BAC JC ePassport Applet only stores keys in Java Card specified Key structures, which are protected by NXP JCOP 3 SECID P60 CS (OSB) open platform.

SF.LCM.6

IC Identification data

During initialisation the IDeal Pass v2.2-n - BAC JC ePassport Applet is installed and initiated with the Pre-Personalisation Agent key and the IC Identification data. The INSTALL for INSTALL method of the NXP JCOP 3 SECID P60 CS (OSB) open platform will be used to store the IC Identification data.

7.2 SFRs and TSS

7.2.1 SFRs and TSS - Rationale

7.2.1.1 TOE Summary Specification

7.2.1.1.1 SF.IA Identification and Authentication

SF.IA.0 The implementation of BAC contributes to:

- FIA_UID.1 Timing of Identification
- FIA_UAU.1 Timing of Authentication
- FIA_UAU.4 Single-use authentication of the Terminal by the TOE
- FIA_UAU.5 Multiple authentication mechanisms
- FIA_UAU.6 Re-authenticating of Terminal by the TOE
- FMT_SMR.1 Security Roles
- FCS_COP.1/AUTH
- FIA_AFL.1 Authentication Failure Handling

SF.IA.4 The implementation contributes to

- FIA_UID.1 Timing of Identification
- FIA_UAU.1 Timing of authentication
- FIA_UAU.4 Single-use authentication of the Terminal by the TOE
- FIA_UAU.5 Multiple authentication mechanisms
- FMT_SMR.1 Security Roles

SF.IA.5 The implementation of Active Authentication contributes to

- FIA_API.1/AA Authentication Proof of Identity – MRTD
- FMT_MTD.1/KEY_WRITE, Management of TSF data – Key Write
- FMT_MTD.1/KEY_READ, Management of TSF data – Key Read
- FCS_COP.1/SIG_GEN, Cryptographic operation – Signature generation by travel document (RSA and ECDSA)

7.2.1.1.2 SF.CF Cryptographic functions support

SF.CF.1 The implementation of this security function contributes to:

- FCS_COP.1/ ENC Cryptographic operation – Encryption / Decryption Triple DES
- FCS_COP.1/ MAC Cryptographic operation Retail MAC

SF.CF.2 The implementation of this security function contributes to:

- FCS_COP.1/SIG_GEN
- FIA_API.1/AA
- FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation by MRTD and according the application in this ST

SF.CF.3 The implementation of this security function contributes to:

- FCS_COP.1/SIG_GEN (Supports ECDSA and RSA signature generation)

SF.CF.6 The implementation of this security function contributes to:

- FCS_CKM.1 Cryptographic key generation – Key Derivation Function by the MRTD
- FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation by MRTD and according the application in this ST

SF.CF.7 The implementation of this security function contributes to:

- FCS_CKM.4/ Cryptographic key destruction

SF.CF.8 The implementation of this security function contributes to:

- FCS_RND.1/ Quality metric for random numbers

7.2.1.1.3 SF.ILTB Protection against interference, logical tampering and bypass

SF.ILTB.1 The implementation of this security function contributes to:

- FPT_FLS.1 Failure with preservation of secure state
- FPT_TST.1 TSF testing
- FPT_PHP.3 Resistance to physical attack

7.2.1.1.4 SF.AC Access control / Storage and protection of logical travel document data

SF.AC.1 The implementation of this security function contributes to:

- FDP_ACC.1 Subset access control - Basic Access Control
- FDP_ACF.1 Security attribute based access control - Basic Access Control
- FDP_UIT.1 Data exchange integrity - MRTD
- FDP_UCT.1 Basic data exchange confidentiality – MRTD

7.2.1.1.5 SF.SM Secure Messaging

SF.SM.1 The implementation of this security function contributes to:

- FCS_COP.1/ENC: Encryption/Decryption 3DES
- FCS_COP.1/MAC: Cryptographic operation – Retail MAC
- FDP_UCT.1 Basic data exchange confidentiality
- FDP_UIT.1 Data exchange integrity

SF.SM.2 The implementation of this security function contributes to:

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

7.2.1.1.6 SF.LCM Security and life cycle management

SF.LCM.1 The implementation of this security function contributes to:

- FMT_SMF.1 Specification of Management Functions (Initialization part)
- FMT_SMR.1.1 Security roles (Manufacturer)
- FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data
- FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

SF.LCM.2 The implementation of this security function contributes to:

- FMT_SMF.1 Specification of Management Functions (Personalization)
- FMT_SMR.1.1 Security roles (Personalization Agent)
- FMT_MTD.1/KEY_WRITE (Management of TSF data – Key Write) Restriction of the ability to write (load) the Active Authentication Private Key, the BAC keys or refresh the Personalisation Agent Key Set to the Personalisation Agent in PERSONALISATION life-cycle state.

SF.LCM.4 The platform implementation provides this security function and contributes to:

- FMT_LIM.1 Limited capabilities
- FMT_LIM.2 Limited availability

SF.LCM.5 The implementation of this security function contributes to:

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

- FPT_EMSEC.1 TOE Emanation

SF.LCM.6

- FAU_SAS.1 Audit storage The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS).

8 Annex

Glossary

Term	Definition
<i>Accurate Terminal Certificate</i>	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [TR-03110-1].
<i>Advanced Inspection Procedure (with PACE)</i>	A specific order of authentication steps between a travel document and a terminal as required by [TR-03110-1], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SOD and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
<i>Agreement</i>	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
<i>Active Authentication</i>	Security mechanism defined in [ICAO-9303]. Option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
<i>Application note</i>	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 (cf. CC part 1, section B.2.7).
<i>Audit records</i>	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialisation Data and Pre-personalization Data.
<i>Authenticity</i>	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
<i>Basic Access Control</i>	Security mechanism defined in [ICAO-9303] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
<i>Basic Inspection System (BIS)</i>	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.
<i>Biographical data (bio data).</i>	The personalized details of the bearer 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.

Term	Definition
<i>Biometric reference data</i>	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
<i>Card Access Number (CAN)</i>	Password derived from a short number printed on the front side of the data-page.
<i>Certificate chain</i>	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
<i>Counterfeit</i>	An unauthorized copy or reproduction of a genuine security document made by whatever means.
<i>Country Signing CA Certificate (CCSCA)</i>	Self-signed certificate of the Country Signing CA Public Key ($K_{Pu\ CSCA}$) issued by CSCA stored in the inspection system.
<i>Country Signing Certification Authority (CSCA)</i>	<p>An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI.</p> <p>The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO-9303], 5.5.1.</p> <p>The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-1].</p>
<i>Country Verifying Certification Authority (CVCA)</i>	<p>An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [TR-03110-1].</p> <p>Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this ST.</p> <p>The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO-9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key</p>

Term	Definition
	pairs must be used for different roles, see [TR-03110-1].
<i>Current date</i>	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used to validate card verifiable certificates.
<i>CV Certificate</i>	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.
<i>CVCA link Certificate</i>	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.
<i>Document Basic Access Key Derivation Algorithm</i>	The [ICAO-9303] 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.
<i>Document Details Data</i>	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
<i>Document Basic Access Keys</i>	Pair of symmetric Triple-DES 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 [ICAO-9303]. 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.
<i>Document Security Object (SO_D)</i>	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). [ICAO-9303]
<i>Document Signer (DS)</i>	<p>An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication.</p> <p>A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [TR-03110-1] and [ICAO-9303].</p> <p>This role is usually delegated to a Personalisation Agent.</p>
<i>Document Verifier (DV)</i>	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g.

Term	Definition
	<p>terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [TR-03110-1].</p> <p>Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this ST.</p> <p>There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy)^{93 94}</p>
<i>Eavesdropper</i>	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
<i>Enrolment</i>	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO-9303]
<i>ePassport application</i>	<p><u>[PP-SAC] definition</u> A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [TR-03110-1].</p> <p><u>[PP-EAC] definition</u> Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes</p> <ul style="list-style-type: none"> • the file structure implementing the LDS [ICAO-9303], • 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.
<i>Extended Access Control</i>	Security mechanism identified in [ICAO-9303] by which means the MTRD'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

⁹³ The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the current ST in order to reflect an appropriate relationship between the parties involved.

⁹⁴ Existing of such an agreement may be technically reflected by means of issuing a CCVCA-F for the Public Key of the foreign CVCA signed by the domestic CVCA.

Term	Definition
	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 themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
<i>Extended Inspection System (EIS)</i>	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.
<i>Forgery</i>	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.
<i>Global Interoperability</i>	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. [ICAO-9303]
<i>IC Dedicated Software</i>	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
<i>IC Dedicated Support Software</i>	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.
<i>IC Dedicated Test Software</i>	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.
<i>IC Embedded Software</i>	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
<i>IC Identification Data</i>	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
<i>Impostor</i>	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.
<i>Improperly documented person</i>	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO-9303]

Term	Definition
<i>Initialisation</i>	Process of writing Initialisation Data (see below) to the TOE (TOE life-cycle, Phase 2 Manufacturing, Step 3).
<i>Initialisation Data</i>	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).
<i>Inspection</i>	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO-9303]
<i>Inspection system (IS)</i>	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.
<i>Integrated circuit (IC)</i>	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
<i>Integrity</i>	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
<i>Issuing Organization</i>	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303]
<i>Issuing State</i>	The Country issuing the MRTD. [ICAO-9303]
<i>Logical Data Structure (LDS)</i>	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the MRTD's chip.
<i>Logical travel document</i>	Data of the travel document holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) <ol style="list-style-type: none"> 1. personal data of the travel document holder 2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 3. the digitized portraits (EF.DG2), 4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5. the other data according to LDS (EF.DG5 to EF.DG16). 6. EF.COM and EF.SOD
<i>Machine readable travel document (MRTD)</i>	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO-9303]
<i>Machine readable zone (MRZ)</i>	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO-9303]

Term	Definition
	The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
<i>Machine-verifiable biometrics feature</i>	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO-9303]
<i>Manufacturer</i>	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
<i>Metadata of a CV Certificate</i>	Data within the certificate body (excepting Public Key) as described in [TR-03110-1]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
<i>Optional biometric reference data</i>	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
<i>Password Authenticated Connection Establishment (PACE)</i>	A communication establishment protocol defined in [ICAO-9303] part 11. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password n). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
<i>PACE passwords</i>	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO-9303] part 11
<i>Passive authentication</i>	(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.
<i>Personalisation</i>	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. paragraph 1.4.3.3, TOE life-cycle, Phase 3, Step 6).

Term	Definition
<i>Personalisation Agent</i>	<p>An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:</p> <ul style="list-style-type: none"> (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [TR-03110-1], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303] (in the role of DS). <p>Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.</p> <p>Generating signature key pair(s) is not in the scope of the tasks of this role.</p>
<i>Personalisation Data</i>	<p>A set of data incl.</p> <ul style="list-style-type: none"> (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Document Security Object). <p>Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.</p>
<i>Personalization Agent Authentication Information</i>	<p>TSF data used for authentication proof and verification of the Personalisation Agent.</p>
<i>Personalisation Agent Key</i>	<p>Symmetric cryptographic key or key set (MAC, ENC) used</p> <ul style="list-style-type: none"> (i) by the Personalisation Agent to prove his identity and get access to the logical travel document and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE.
<i>Physical part of the travel document</i>	<p>Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to)</p> <ol style="list-style-type: none"> 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.

Term	Definition
<i>Pre-personalization</i>	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (TOE life-cycle, Phase 2, Step 5)
<i>Pre-personalization Data</i>	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 life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair and Chip Life-Cycle Production data (CPLC data).
<i>Pre-personalised travel document's chip</i>	Travel document's chip equipped with a unique identifier.
<i>Receiving State</i>	The Country to which the MRTD holder is applying for entry. [ICAO-9303]
<i>Reference data</i>	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.
<i>RF-terminal</i>	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
<i>Secondary image</i>	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means [ICAO-9303].
<i>Secure messaging in encrypted /combined mode</i>	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
<i>Service Provider</i>	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
<i>Skimming</i>	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless or contact based communication channel of the TOE without knowledge of the printed MRZ data.
<i>Standard Inspection Procedure</i>	<p>A specific order of authentication steps between an travel document and a terminal as required by [ICAO- 9303] and [TR-03110-1], namely</p> <ul style="list-style-type: none"> (i) PACE or BAC and (ii) Passive Authentication with SO_D. <p>SIP can generally be used by BIS-PACE and BIS-BAC.</p>
<i>Terminal</i>	<p>A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter.</p> <p>In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE.</p>

Term	Definition
	Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).
<i>Terminal Authorization</i>	Intersection of the Certificate Holder Authorizations of the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be valid for the Current Date.
<i>Terminal Authorisation Level</i>	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
<i>TOE tracing data</i>	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
<i>Travel document</i>	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO-9303] (there "Machine readable travel document").
<i>Travel document (electronic)</i>	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: <i>ePassport</i> .
<i>Travel Document Holder</i>	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
<i>Travel document's Chip</i>	A contact based / contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO-9303], sec III.
<i>Traveler</i>	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
<i>TSF data</i>	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC-1]).
<i>Unpersonalised travel document</i>	The travel document that contains the travel document chip holding only Initialisation Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
<i>User data</i>	<p>All data (being not authentication data)</p> <ul style="list-style-type: none"> (i) stored in the context of the ePassport application of the travel document as defined in [5] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. <p>CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC-1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and</p>



Term	Definition
	upon which the TSF places no special meaning (CC part 2 [CC-2]).
<i>Verification</i>	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO-9303]
<i>Verification data</i>	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.

Abbreviations

CC	Common Criteria, see [CC]
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
SEF	Security Enforcing Functions
SOF	Strength Of Function
TOE	Target of Evaluation
TSF	TOE Security Functions

References

Reference	Description
[AGD_OPE]	2016_2000021061 - OPERATIONAL PROCEDURES FOR IDEAL PASS V2.2-N - SAC/EAC JC EPASSPORT (WITH MICA0 APPLET)
[AGD_PRE]	2016_2000021062 - PREPARATIVE PROCEDURES FOR IDEAL PASS V2.2-N - SAC/EAC JC EPASSPORT (WITH MICA0 APPLET)
[BAC-PP]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1:Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2:Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
[CEM]	The Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
[ICAO-9303]	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7th edition, 2015
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11
[ISO15946-2]	ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.
[ISO18013-3]	ISO/IEC 18013-3: Information technology – Personal identification – ISO-compliant driving licence. Part 3: Access control, authentication and integrity validation, 2009-03-01 Including ISO/CEI 18013-3/AC1:2011, TECHNICAL CORRIGENDUM 1, Published 2011-12-01
[ISO7816]	ISO/IEC 7816: Identification cards – Integrated circuit cards, Version Second Edition, 2008
[ISO9796-2]	ISO/IEC 9796-2: 2002, Information Technology - Security Techniques



Reference	Description
	- Digital Signature Schemes giving message recovery - Part 2: Integer factorization based mechanisms
[ISO9797]	ISO/IEC 9797-1:1999, Information technology –Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.
[PLTF-ST]	JCOP 3 SECID P60 CS (OSB) Security Target, Revision 2.5, 2017-06-29. NXP
[PLTF-PRE]	JCOP 3 SECID P60 CS (OSB), User Guidance and Administration Manual, Rev. 2.4 - 2017-06-07. NXP
[NIST-180-4]	NIST. FIPS 180-4, Secure Hash Standard, February 2011.
[NIST-197]	NIST. Specification for the Advanced Encryption Standard (AES), FIPS PUB 197, 2001
[SIC-PP]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.
[ST-SAC-EAC]	2017_2000032441 - Security Target Lite IDeal Pass v2.2-n - SAC/EAC JC ePassport. IDEMIA
[TR-03110-1]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012 by BSI
[TR-03110-3]	TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, version 2.10, 2012-03-07 by BSI