

CombICAO Applet in PACE and CA Configuration on Cosmo v9 Public Security Target


© IDEMIA. All rights reserved.

Specifications and information are subject to change without notice.

The products described in this document are subject to continuous development and improvement.

All trademarks and service marks referred to herein, whether registered or not in specific countries, are the properties of their respective owners.

- Printed versions of this document are uncontrolled -



DOCUMENT MANAGEMENT

Business Unit – Department	PSI
Document type	Public FQR
Document Title	CombICAO Applet in PACE and CA Configuration on Cosmo v9 Public Security Target
FQR No	110 9319
FQR Issue	3

DOCUMENT REVISION

Date	Revision	Modification
14/10/2019	1.0	Creation based on the full ST
29/10/2019	2.0	Update AGD version
20/11/2019	3.0	Review and Update

Table of contents

TABLE OF CONTENTS	3
TABLE OF TABLES.....	5
1 GENERAL.....	6
1.1 INTRODUCTION.....	6
1.2 PRODUCT OVERVIEW	6
2 ST INTRODUCTION.....	7
2.1 ST REFERENCE AND TOE REFERENCE.....	7
2.1.1 <i>ST reference</i>	7
2.1.2 <i>TOE reference</i>	7
2.2 TOE OVERVIEW	8
2.2.1 <i>Usage and major security features of the TOE</i>	8
2.2.2 <i>TOE type</i>	9
2.2.3 <i>Required non-TOE hardware/Software/firmware</i>	10
2.3 TOE DESCRIPTION	10
2.3.1 <i>Physical scope of the TOE</i>	10
2.3.2 <i>TOE delivery</i>	10
2.3.3 <i>Logical scope of the TOE</i>	12
2.3.4 <i>Authentication Protocols</i>	12
2.3.5 <i>Machine Readable Travel Document (MRTD)</i>	13
2.4 TOE LIFE CYCLE.....	13
2.4.1 <i>Life cycle overview</i>	13
2.4.2 <i>Development Environment</i>	14
2.4.3 <i>Production Environment</i>	15
2.4.4 <i>Preparation Environment</i>	16
2.4.5 <i>Operational Environment</i>	16
3 CONFORMANCE CLAIMS.....	17
3.1 COMMON CRITERIA CONFORMANCE	17
3.2 PROTECTION PROFILE CONFORMANCE	17
3.2.1 <i>Overview</i>	17
3.2.2 <i>Assumptions</i>	17
3.2.3 <i>Threats</i>	17
3.2.4 <i>Organisational Security Policies</i>	18
3.2.5 <i>Security Objectives</i>	18
4 SECURITY PROBLEM DEFINITION	19
4.1 ASSETS.....	19
4.1.1 <i>Primary Assets</i>	19
4.1.2 <i>Secondary Assets</i>	19
4.2 USERS / SUBJECTS.....	20
4.3 THREATS.....	22
4.4 ORGANISATIONAL SECURITY POLICIES	24
4.5 ASSUMPTIONS	25
5 SECURITY OBJECTIVES	26
5.1 SECURITY OBJECTIVES FOR THE TOE	26
5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	28
5.2.1 <i>Travel document Issuer as the general responsible</i>	28
5.2.2 <i>Travel document Issuer and CSCA: travel document's PKI (issuing) branch</i>	28



5.2.3	<i>Terminal operator: Terminal's receiving branch</i>	29
5.2.4	<i>Travel document holder Obligations</i>	30
5.2.5	<i>Miscellaneous</i>	30
5.3	SECURITY OBJECTIVES RATIONALE	30
5.3.1	<i>Threats</i>	30
5.3.2	<i>Organisational Security Policies</i>	32
5.3.3	<i>Assumptions</i>	32
5.3.4	<i>SPD and Security Objectives</i>	33
6	EXTENDED REQUIREMENTS	36
6.1	EXTENDED FAMILIES	36
6.1.1	<i>Extended Family FPT_EMS - TOE Emanation</i>	36
6.1.2	<i>Extended Family FIA_API - Authentication Proof of Identity</i>	37
6.1.3	<i>Extended Family FMT_LIM - Limited capabilities</i>	37
6.1.4	<i>Extended Family FAU_SAS - Audit data storage</i>	38
6.1.5	<i>Extended Family FCS_RND - Generation of random numbers</i>	39
7	SECURITY REQUIREMENTS	40
7.1	SECURITY FUNCTIONAL REQUIREMENTS	40
7.1.1	<i>Class FCS Cryptographic Support</i>	40
7.1.2	<i>Class FIA Identification and Authentication</i>	44
7.1.3	<i>Class FDP User Data Protection</i>	47
7.1.4	<i>Class FTP Trusted Path/Channels</i>	50
7.1.5	<i>Class FAU Security Audit</i>	51
7.1.6	<i>Class FMT Security Management</i>	51
7.1.7	<i>Class FPT Protection of the Security Functions</i>	54
7.2	SECURITY REQUIREMENTS RATIONALE	55
7.2.1	<i>Objectives</i>	55
7.2.2	<i>Rationale tables of Security Objectives and SFRs</i>	59
7.2.3	<i>Dependencies</i>	63
7.2.4	<i>Rationale for the Security Assurance Requirements</i>	67
8	TOE SUMMARY SPECIFICATION	68
8.1	TOE SUMMARY SPECIFICATION	68
8.2	SFRs AND TSS	72
8.2.1	<i>SFRs and TSS - Rationale</i>	72
8.2.2	<i>Association tables of SFRs and TSS</i>	76
9	GLOSSARY AND ACRONYMS	80
9.1	GLOSSARY	80
9.2	ACRONYMS	87
10	REFERENCES	88



Table of figures

Figure 1 Physical Form of the module	10
Figure 2 TOE Boundaries	11
Figure 3 Life cycle Overview.....	14

Table of tables

Table 1 ST Reference	7
Table 2 TOE reference	7
Table 3 Roles identification on the life cycle	13
Table 4 Image containing both Java Card platform and applet is loaded at IC manufacturer (Option 1)	15
Table 5 Cap file of CombICAO applet is loaded (using GP) (Option 2)	15
Table 6 Image containing both platform and applet is loaded through the loader of the IC (Option 3)	16
Table 7 Common Criteria conformance claim	17
Table 8 Protection Profile conformance	17
Table 9 Threats and Security Objectives - Coverage	33
Table 10 Security Objectives and Threats - Coverage	34
Table 11 OSPs and Security Objectives - Coverage	34
Table 12 Security Objectives and OSPs - Coverage	35
Table 13 Assumptions and Security Objectives for the Operational Environment - Coverage	35
Table 14 Security Objectives for the Operational Environment and Assumptions - Coverage	35
Table 15 Security Objectives and SFRs - Coverage	60
Table 16 SFRs and Security Objectives	63
Table 17 SFRs Dependencies	65
Table 18 SARs Dependencies	67
Table 19 SFRs and TSS - Coverage	78
Table 20 TSS and SFRs - Coverage	79

1 GENERAL

1.1 Introduction

This public security target describes the security needs induced by the CombICAO Applet product in PACE and CA configuration on IDEMIA underlying Java Card *ID-ONE Cosmo V9 Essential*, see 2.1.2 .

The objectives of this Security Target are:

- To describe the Target of Evaluation (TOE), its life cycle and to position it in the smart card life cycle,
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the platform active phases,
- To describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the product active phases,
- To specify the security requirements which include the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment,
- To describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements,
- To present evidence that this ST is a complete and cohesive set of requirements that the TOE provides on an effective set of IT security countermeasures.

1.2 Product overview

The product is designed to support the following usages:

1. **eMRTD as per [ICAO_9303]; scope of the current ST**
2. ISO compliant driving license as per [ISO/IEC_18013] and [ISO/IEC_19446]; (out of the scope of the current ST)
3. digital identity and electronic services; (out of the scope of the current ST)

It is achieved thanks to a flexible design allowing to “build” during personalization of the applet the required application(s) by configuring accordingly:

- the file system;
- authentication protocols;
- the user authentication credentials;
- access conditions on files;

The product can be personalized to support an eMRTD application compliant with [ICAO_9303].

The product allows four configurations in eMRTD.

The current ST addresses CombICAO Applet in eMRTD configuration (1) below.

- 1) CombICAO Applet product in **PACE** configuration with **CA**,
- 2) CombICAO Applet product in **EAC** configuration,
- 3) CombICAO Applet product in **EAC** with **PACE** configuration,
- 4) CombICAO Applet product in **BAC** configuration with **CA**.



2 ST INTRODUCTION

2.1 ST reference and TOE reference

2.1.1 ST reference

Title	CombICAO Applet in PACE and CA configuration on Cosmo V9 – Security Target
ST Version	3
ST Identification	FQR 110 9319
Authors	IDEMIA
ITSEF	BrightSight
Certification Body	TÜV Rheinland Nederland B.V.
CC version	3.1 revision 5
EAL	EAL5 augmented with: <ul style="list-style-type: none"> • AVA_VAN.5 • ALC_DVS.2
PP	See [PP_PACE]

Table 1 ST Reference

2.1.2 TOE reference

Product Name	CombICAO Applet
TOE Name	CombICAO Applet in PACE and CA configuration on ID-ONE Cosmo V9 Essential
Developer Name	IDEMIA
TOE Identification	SAAAAR code: 203297
Platform Name	ID-One Cosmo V9 Essential Platform
Platform Identification	089233
Platform certification	[PTF_CERT]
Guidance Documents	[Applet_Perso_Guide], [Applet_User_Guide] [PTF_AGD_PRE], [PTF_AGD_OPE], [PTF_AGD1], [PTF_AGD2] and [PTF_AGD3]

Table 2 TOE reference

In order to assure the authenticity of the card, the **TOE Identification** shall be verified by analyzing the response of the command GET DATA, see section 4 of [Applet_Perso_Guide].

2.2 TOE overview

2.2.1 Usage and major security features of the TOE

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

The 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 [ICAO_9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
 - (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
 - (2) the digitized portraits (EF.DG2),
 - (3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
 - (4) the other data according to LDS (EF.DG5 to EF.DG16) and
 - (5) the Document security object.

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 defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO_9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

During the prepersonalization and personalisation, the Personalisation Agent, once authenticated, gets the rights (access control) for (1) reading and writing data, (2) instantiating the application, and (4) writing of personalization data. The Personalisation Agent can so create the file structure (MF / ADF) required for this configuration.

Mutatis mutandis, the TOE may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446 supporting BAP-1 (the same protocol as BAC but used in the context of driving license), AA and CA, as both applications (MRTD and IDL) share the same protocols and data structure organization. Therefore, in the rest of the document, the word "MRTD" MAY be understood either as a MRTD in the sense of ICAO, or a driving license compliant to ISO/IEC 18013 or ISO/IEC TR 19446 depending on the targeted usage envisioned by the issuer.



The table below indicates how terms and concept present in the current document shall be read when considering the TOE to be an ISO driving license:

MRTD	ISO driving licence
MRTD	IDL
ICAO	ISO/IEC
ICAO 9303	ISO/IEC 18013 or ISO/IEC TR 19446
BAC	BAP-1
DG3	DG7
DG4	DG8
DG15	DG13
MRZ or CAN	MRZ or SAI (Scanning area identifier)
Traveler	Holder

NB: the ISO driving license is out of the scope of the current ST and not evaluated.

The protection of the communication provided by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE ([PP_PACE]). Note that [PP_PACE] considers high attack potential.

For the PACE protocol according to [ICAO_TR_SAC], the following steps shall be performed:

- (i) the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.
- (ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
- (iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
- (iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [TR_03110], [ICAO_TR_SAC].

The Chip Authentication defined in [TR_03110] is a security feature which is optionally supported by the TOE. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

This TOE addresses the Chip Authentication as an alternative to the Active Authentication stated in [ICAO_9303].

2.2.2 TOE type

The TOE is a composite product made up of an Embedded Software developed using Java Card technology, composed on a Java Card open platform. Both developed by IDEMIA.

The underlying Java Card open platform has already been certified, please see [PTF_CERT].

The TOE embedded is the dual (contactless and/or contact) integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing :

- Password Authenticated Connection Establishment (PACE)
- Chip Authentication (CA)

Please refer to 2.3.2 TOE delivery section for more details on TOE deliveries



2.2.3 Required non-TOE hardware/Software/firmware

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

Note: In particular, the TOE may be used in contact mode, without any inlay or antenna.

2.3 TOE description

2.3.1 Physical scope of the TOE

The TOE is physically made up of several components hardware and software.

Once constructed, the TOE is a bare microchip with its external interfaces for communication.

The physical medium on which the microchip is mounted is not part of the target of evaluation as it does not alter nor modify any security functions of the TOE.

The TOE may be used on several physical medium within an inlay, or eCover; in a plastic card are not part of the TOE.

The physical form of the module is depicted in Figure below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the following figure

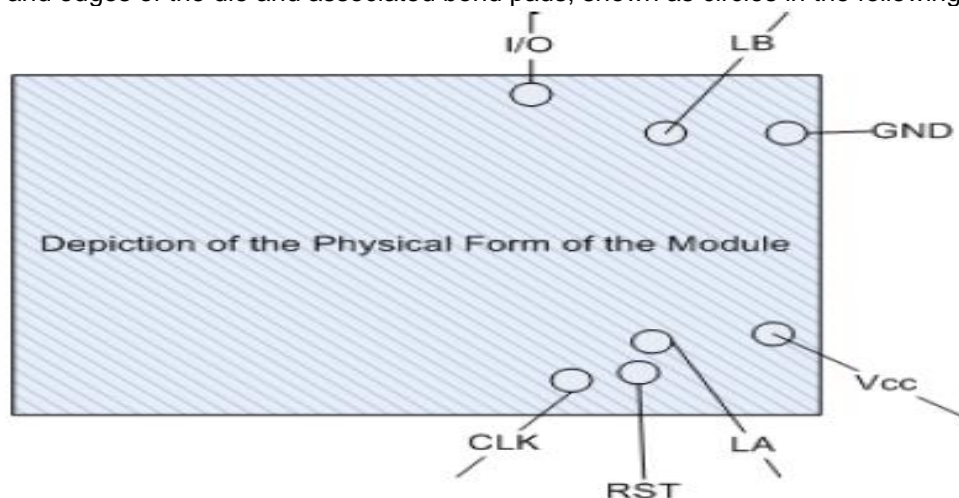


Figure 1 Physical Form of the module

2.3.2 TOE delivery

The TOE is composed of:

- Circuitry of the MRTD's chip (the IC) :
- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- ID-ONE Cosmo V9 Essential: see [ST_PTF] and [PTF_CERT]
- CombICAO application
- Associated guidance documentation (delivered in electronic version)

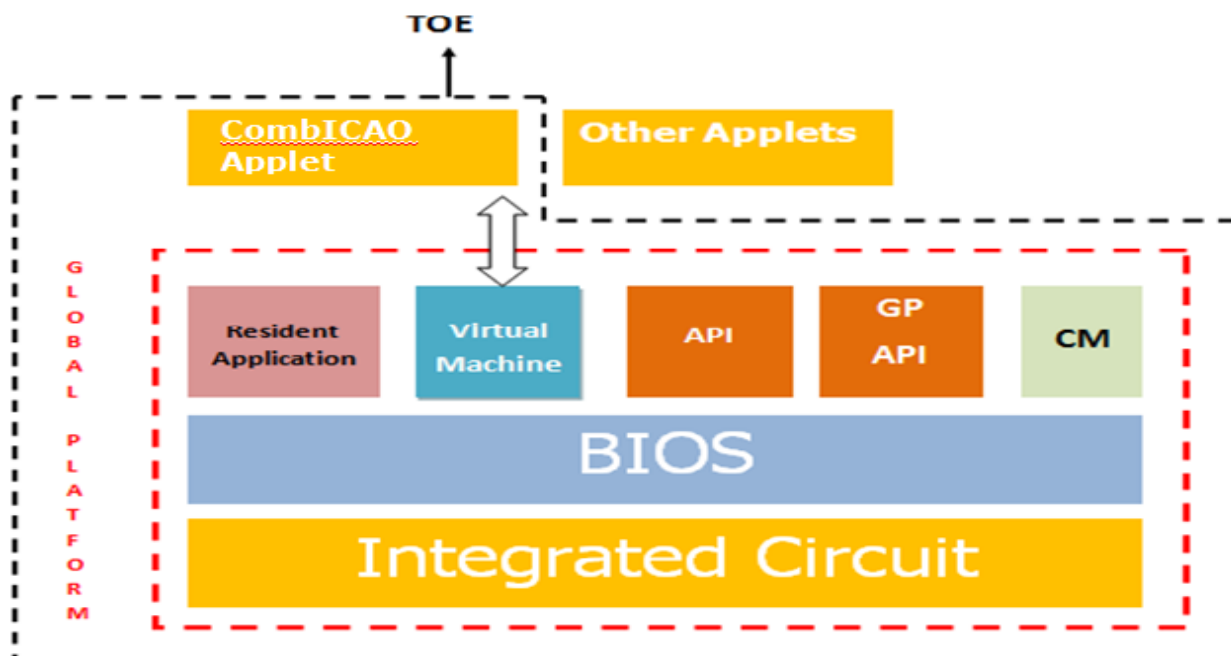
This ST Lite version will also be provided as a guidance document along with above-mentioned documents.



TOE Component	Identification	Form Factor of Delivery	Delivery method
CombICAO applet for MRTD	203297	ID1 or ID3 Passport booklets ID1 cards or ID3 holder pages Antenna ¹ inlays Chip in modules on a reel	CPS tool is used in the case of an Image delivery. Otherwise, trusted courier is used.
Personalizing Agent	[Applet_Perso_Guide]	Electronic doc	PGP-encrypted parts on USB or CD media, off-line registered distribution by trusted courier
End User of the TOE	[Applet_Uder_Guide]		
Underlying platform guidance	[PTF_AGD_OPE] [PTF_AGD1] [PTF_AGD2] [PTF_AGD3] [PTF_AGD_PRE]		

Form factor and Delivery Preparation:

1. As per the Software Development Process of IDEMIA, upon completion of development activities, particular applet will be uploaded into CPS in CAP file format. Before uploading, the applet will be verified through Oracle verifier and IDEMIA verifier.
2. During Release for Sample as project milestone, status of the applet in CPS will be changed into "Pilot version" to be used further for manufacturing samples.
3. During Software Delivery Review as the final R&D project milestone, status of the applet in CPS will be changed into "Industrial release" to be used further for mass production.


Figure 2 TOE Boundaries

¹ The inlay production including the application of the antenna is not part of the TOE

2.3.3 Logical scope of the TOE

The TOE is a smartcard, composed of:

- IC,
- Java Card Open Platform (OS) and
- CombICAO application (logical data structure).

The TOE scope encompasses the following features:

- Password Authentication Connection Establishment (PACE v2)
- Chip Authentication
- Prepersonalization phase
- Personalisation phase

The prepersonalization and personalisation are performed by the Manufacturer and the Personalisation Agent, which controls the TOE. All along this phase, the TOE is self-protected, as it requires the authentication of the Manufacturer and the Personalisation Agent prior to any operation. By being authenticated, the Personalisation Agent gets the rights (access control) for (1) reading and writing data,(2) instantiating the application, and (4) writing of personalization data. The Personalisation Agent can so create the file structure (MF / ADF) required for this configuration.

2.3.4 Authentication Protocols

2.3.4.1 Password Authenticated Connection Establishment (PACE)

PACE is an access control mechanism that is supplemental to BAC. It is a cryptographically stronger access control mechanism than BAC since it uses asymmetric cryptography compared to BAC's symmetric cryptography.

PACE is realized through five commands:

1. MSE SET – AT command
2. GENERAL AUTHENTICATE command – Encrypted Nonce
3. GENERAL AUTHENTICATE command – Map Nonce
4. GENERAL AUTHENTICATE command – Perform Key Agreement
5. GENERAL AUTHENTICATE command – Mutual Authentication

Once the mutual authentication is performed, a secure messaging is available to protect the communication between the chip and the IS.

This table lists the supported configurations for PACE protocol:

Configuration	Mapping	Key Algo	Key Length (in bytes)	Secure Messaging	Auth. Token	Hash Algo
PACE-ECDH-GM-3DES	Generic	3DES 2Key	16	CBC / Retail MAC	Retail MAC	SHA-1
PACE-ECDH-GM-AES-128	Generic	AES	16	CBC / CMAC	CMAC	SHA-1
PACE-ECDH-GM-AES-192	Generic	AES	24	CBC / CMAC	CMAC	SHA-256
PACE-ECDH-GM-AES-256	Generic	AES	32	CBC / CMAC	CMAC	SHA-256
PACE-ECDH-IM-3DES	Integrated	3DES 2Key	16	CBC / Retail MAC	Retail MAC	SHA-1
PACE-ECDH-IM-AES-128	Integrated	AES	16	CBC / CMAC	CMAC	SHA-1
PACE-ECDH-IM-AES-192	Integrated	AES	24	CBC / CMAC	CMAC	SHA-256
PACE-ECDH-IM-AES-256	Integrated	AES	32	CBC / CMAC	CMAC	SHA-256



PACE-ECDH-CAM-AES-128	Chip Authentication	AES	16	CBC / CMAC	CMAC	SHA-1
PACE-ECDH-CAM-AES-192	Chip Authentication	AES	24	CBC / CMAC	CMAC	SHA-256
PACE-ECDH-CAM-AES-256	Chip Authentication	AES	32	CBC / CMAC	CMAC	SHA-256

Table 1- PACE configuration

2.3.4.2 Chip Authentication (CA)

The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip.

The protocol establishes Secure Messaging between an MRTD chip and a terminal based on a static key pair stored on the MRTD chip. Chip Authentication is an alternative to the optional ICAO Active Authentication (AA protocol is not supported by the TOE), i.e. it enables the terminal to verify that the MRTD chip is genuine but has two advantages over the original protocol:

Challenge Semantics are prevented because the transcripts produced by this protocol are non-transferable.

Besides authentication of the MRTD chip this protocol also provides strong session keys.

The protocol in version 1 provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys.

The protocol in Version 2 provides explicit authentication of the MRTD chip by verifying the authentication token and implicit authentication of the stored data by performing Secure Messaging using the new session keys.

2.3.5 Machine Readable Travel Document (MRTD)

The MRTD is a complete set of commands, which allows the management of MRTD data in the Operational Use phase (data management and authentication process under MRTD ADF).

2.4 TOE life cycle

2.4.1 Life cycle overview

The following table presents the TOE roles and the corresponding subject:

Roles		Subject
IC developer		IC Manufacturer
TOE developer		IDEMIA
Manufacturer	IC manufacturer	IC Manufacturer
	MRTD packaging responsible	IDEMIA or another agent
	Embedded software loading responsible	IDEMIA
	Pre-personalization Agent (Manufacturer Role)	IDEMIA or another agent
Personalization Agent		IDEMIA or another agent

Table 3 Roles identification on the life cycle

Several life cycles are available, depending when the Flash Code is loaded.



The following tables present the subjects following TOE life cycle steps in accordance with the standard smart card life cycle [PP_IC], and describe for each of them, (1) the TOE delivery point and (2) the assurance coverage:

The TOE life cycle in the following figure distinguishes stages for development, production, preparation and operational use in accordance with the standard smart card life cycle [PP_IC].

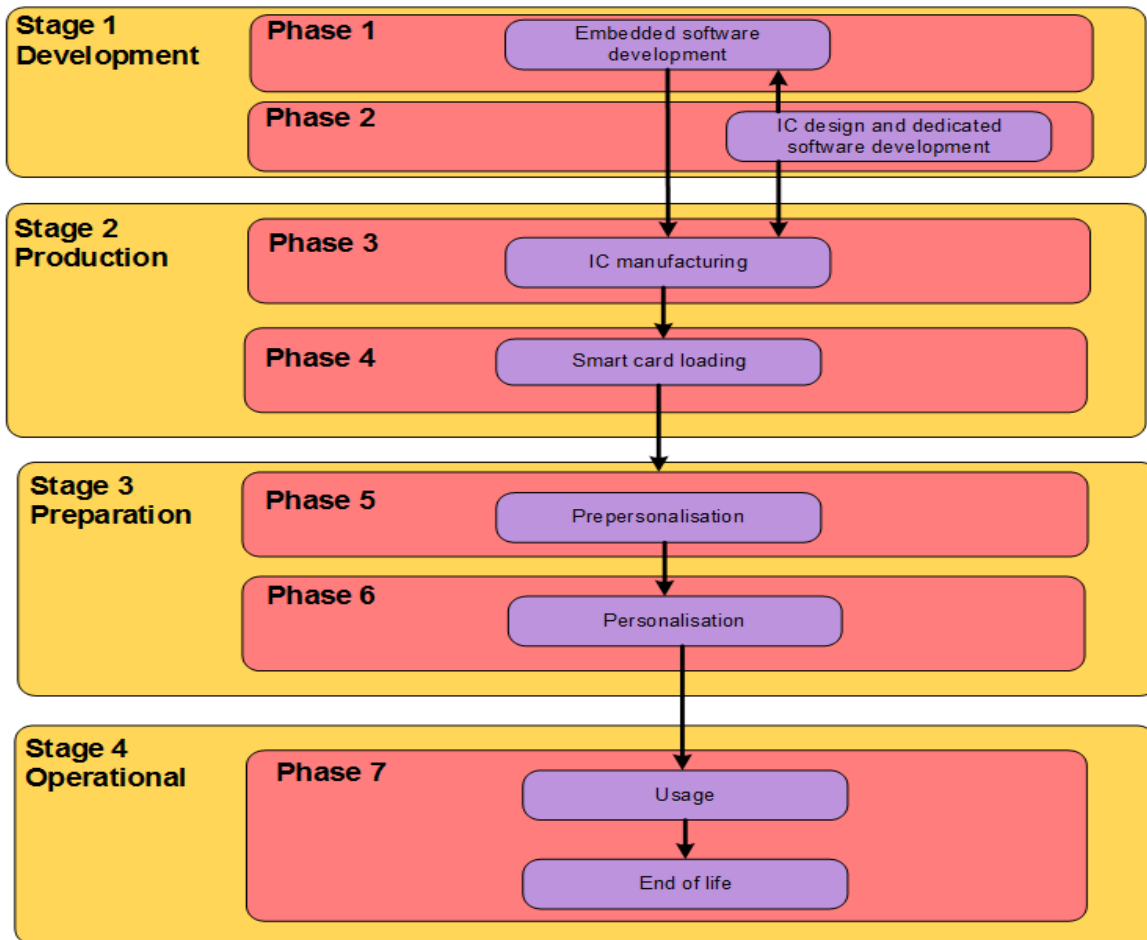


Figure 3 Life cycle Overview

2.4.2 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Java Card Open Platform components and CombICAO applet)
- Phase 2: IC Development

The IC Embedded Software Developer is in charge of the specification, development and validation of the software (Java Card Open Platform and CombICAO applet).

The IC Developer designs the IC, develops the IC dedicated software and provides information, software or tools to the IC embedded software developer.

Roles, actors, sites and coverage for this environment of the product life-cycle are listed in the table below:



Role	Actor	Site	Covered by
CombICAO Applet Developer	IDEMIA	MANILA and Courbevoie R&D sites	ALC
Platform Developer	IDEMIA	IDEMIA R&D sites Refer to [PTF_CERT]	ALC
IC Developer	IC Manufacturer	IC Manufacturer Refer to [PTF_CERT]	ALC

2.4.3 Production Environment

In this environment, the following two phases take place:

- Phase 3: IC manufacturing
- Phase 4: Smart card loading

The IC manufacturer is responsible for producing the IC (manufacturing, testing, and initialisation). Depending on the intention:

- **(Option 1)** the developer sends the image (containing both the Java Card platform and the CombICAO applet) to be flashed in the IC to the IC manufacturer in the phase 3.

Or

- **(Option 2)** the platform developer sends the image (containing only the Java Card platform) to be flashed in the IC to the IC manufacturer in the phase 3. Once the Java Card platform has been loaded, the package of CombICAO is securely delivered from the applet developer to the smart card loader. The cap file of the applet is then loaded (using GP) in the Java Card platform by the smart card loader in phase 4 at IDEMIA audited site.

Or

- **(Option 3)** the developer sends the image (containing both the Java Card platform and the CombICAO applet) to be loaded in Flash (using the loader of the IC) to the smart card loader in phase 4.

Several life cycles are available, depending when the Flash Code is loaded. The following tables present roles, actors, sites and coverage for this for this environment of the product life-cycle and describe for each of them the TOE delivery point.

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing both platform and applet	manufacturer	IC manufacturer production plants [PTF_CERT]	ALC
Smart card loader	-	-	-	-
TOE Delivery Point				

Table 4 Image containing both Java Card platform and applet is loaded at IC manufacturer (Option 1)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	Image containing only Java Card Platform	manufacturer	IC manufacturer production plants Refer to [PTF_CERT]	ALC
Smart card loader	Cap file of the applet	IDEMIA	IDEMIA plant (Shenzhen, Haarlem, Vitré)	ALC
TOE Delivery Point				

Table 5 Cap file of CombICAO applet is loaded (using GP) (Option 2)

Role	Package to be loaded	Actor	Site	Covered by
IC manufacturer	-	-	-	-
TOE Delivery Point				
Smart card loader	Image containing both the platform and applet	IDEMIA or another agent	Any	AGD

Table 6 Image containing both platform and applet is loaded through the loader of the IC (Option 3)

2.4.4 Preparation Environment

In this environment, the following two phases take place:

- Phase 5: Prepersonalisation of the applet
- Phase 6: Personalisation

The preparation environment may not necessarily take place in a manufacturing site, but may be performed anywhere. All along these two phases, the TOE is self-protected as it requires the authentication of the prepersonalisation agent or personalisation agent prior to any operation.

The CombICAO applet is prepersonalised and personalised according to [Applet_Perso_Guide].

At the end of phase 6, the TOE is constructed. These two phases are covered by [Applet_Perso_Guide] tasks of the TOE and [PTF_AGD_OPE] tasks of [PTF_CERT].

2.4.5 Operational Environment

The TOE is under the control of the User (Signatory and/or Administrator).

During this phase, the TOE may be used as described in [Applet_User_Guide] of the TOE.

This phase is covered by [Applet_User_Guide] tasks of the TOE and [PTF_AGD_OPE] tasks of [PTF_CERT].

3 Conformance claims

3.1 Common Criteria conformance

This Public Security Target claims conformance to [CC_2] and [CC_3].
The conformance to the CC is claimed as follows:

CC	Conformance Claim
Part 2	Conformance with extensions: <ul style="list-style-type: none"> • FAU_SAS.1 “Audit storage”, • FCS_RNG.1 “Quality metric for random numbers”, • FMT_LIM.1 “Limited capabilities”, • FMT_LIM.2 “Limited availability”, • FPT_EMS.1 “TOE Emanation”, • FIA_API.1² “Authentication Proof of Identity”,
Part 3	Conformance with package EAL5 augmented with: <ul style="list-style-type: none"> • ALC_DVS.2 “Sufficiency of security measures” defined in [CC_3], • AVA_VAN.5 “Advanced Methodical Vulnerability Analysis” defined in [CC_3]

Table 7 Common Criteria conformance claim

3.2 Protection Profile conformance

3.2.1 Overview

This ST claims strict conformance to the following Protection Profile (PP):

Title	Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)
CC Version	3.1 (Revision 4)
Assurance Level	The minimum assurance level for this PP is EAL4 augmented
Version Number	1.01
Registration	BSI-CC-PP-0068-V2-2011-MA-01

Table 8 Protection Profile conformance

This ST also addresses the Manufacturing and Personalization phases at TOE level.

The additions do not contradict any of the threats, assumptions, organizational policies, objectives or SFRs stated in the [PP_PACE] that covers the advanced security methods PACE in operational use phase.

The following parts list assumptions, threats, OSP, OT and OE for this TOE (i.e. from [PP_PACE] and additional).

3.2.2 Assumptions

The following Assumptions are assumed for this TOE:

- **A.Passive_Auth** “PKI for Passive Authentication” defined in [PP_PACE],

3.2.3 Threats

The following threats are averted by this TOE:

- **T.Counterfeit** “Counterfeit of travel document chip data” defined in this ST,
- **T.Skimming** “Skimming travel document / Capturing Card-Terminal Communication” defined in [PP_PACE],

² FIA_API.1 has been added to this security target for the needs of the Chip Authentication Protocol.



- **T.Eavesdropping** “Eavesdropping on the communication between the TOE and the PACE terminal” defined in [PP_PACE],
- **T.Tracing** “Tracing travel document” defined in [PP_PACE],
- **T.Forgery** “Forgery of Data” defined in [PP_PACE],
- **T.Abuse-Func** “Abuse of Functionality” and defined in [PP_PACE],
- **T.Information_Leakage** “Information Leakage from travel document” defined in [PP_PACE],
- **T.Phys-Tamper** “Physical Tampering” defined in [PP_PACE],
- **T.Malfunction** “Malfunction due to Environmental Stress” defined in [PP_PACE],
- **T.Configuration** “*Tampering attempt of the TOE during preparation*” defined in this ST,
- **T.Forgery_Supplemental_Data** “*Forgery of supplemental data stored in the TOE*” defined in this ST

3.2.4 Organisational Security Policies

This TOE complies with the following OSP:

- **P.Pre-Operational** “*Pre-operational handling of the travel document*” defined in [PP_PACE],
- **P.Card_PKI** “*PKI for Passive Authentication (issuing branch)*” defined in [PP_PACE],
- **P.Trustworthy_PKI** “*Trustworthiness of PKI*” r defined in [PP_PACE],
- **P.Manufact** “*Manufacturing of the travel document’s chip*” defined in [PP_PACE],
- **P.Terminal** “*Abilities and trustworthiness of terminals*” defined in [PP_PACE].

3.2.5 Security Objectives

The Security Objectives for this TOE are the following:

- **OT.Chip_Auth_Proof** “*Proof of the travel document’s chip authenticity*” defined in this ST,
- **OT.Data_Integrity** “*Integrity of Data*” defined in [PP_PACE],
- **OT.Data_Authenticity** “*Authenticity of Data*” defined in [PP_PACE],
- **OT.Data_Confidentiality** “*Confidentiality of Data*” defined in [PP_PACE],
- **OT.Tracing** “*Tracing travel document*” defined in [PP_PACE],
- **OT.Prot_Abuse-Func** “*Protection against Abuse of Functionality*” defined in [PP_PACE],
- **OT.Prot_Inf_Leak** “*Protection against Information Leakage*” defined in [PP_PACE],
- **OT.Prot_Phys-Tamper** “*Protection against Physical Tampering*” defined in [PP_PACE],
- **OT.Prot_Malfunction** “*Protection against Malfunctions*” defined in [PP_PACE],
- **OT.Identification** “*Identification of the TOE*” defined in [PP_PACE],
- **OT.AC_Pers** “*Access Control for Personalisation of logical MRTD*” defined in [PP_PACE].
- **OT.Configuration** “*Protection of the TOE preparation*” defined in this ST,
- **OT.Update_File** “*Modification of file in Operational Use Phase*” defined in this ST,
- **OT.Chip_Auth_Proof_PACE_CAM** “*Proof of the electronic document’s chip authenticity*” defined in this ST.

The Security Objectives for the environment of this TOE are the following:

- **OE.Legislative_Compliance** “*Issuing of the travel document*” defined in [PP_PACE],
- **OE.Passive_Auth_Sign** “*Authentication of travel document by Signature*” defined in [PP_PACE],
- **OE.Personalisation** “*Personalisation of travel document*” defined in [PP_PACE],
- **OE.Terminal** “*Terminal operating*” defined in [PP_PACE]
- **OE.Travel_Document_Holder** “*Travel document holder Obligations*” defined in [PP_PACE],



4 Security Problem Definition

4.1 Assets

4.1.1 Primary Assets

User Data stored on the TOE

All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [4] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [4]).

This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [9].

Generic Security Properties: Confidentiality, Integrity, Authenticity

User Data transferred between the TOE and the Terminal

All data (being not authentication data) being transferred in the context of the ePassport application of the travel document as defined in [4] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [4]). User data can be received and sent (exchange is receive, send).

Generic Security Properties: Confidentiality, Integrity, Authenticity

Travel Document Tracing Data

Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.

Generic Security Property: Unavailability

4.1.2 Secondary Assets

In order to achieve a sufficient protection of the primary assets, the following secondary assets also are protected by the TOE.

Accessibility of TOE Functions and Data only for Authorised Subjects

Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.

Generic Security Property: Availability

Genuineness of the TOE

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD's chip' in [9].

Generic Security Property: Availability



TOE internal secret cryptographic keys

Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

Generic Security Properties: Confidentiality, Integrity

Application Note:

Data for electronic document holder authentication and for authorization of communication with the electronic document can be categorized as (i) reference information that are persistently stored within the TOE, and (ii) verification information for the TOE that are input by a human user during an authentication and/or authorization attempt. The TOE shall secure both reference information, and, together with the connected terminal, verification information that are transferred in the channel between the TOE and the terminal.

TOE internal Non-Secret Cryptographic Material

Permanently or temporarily stored nonsecret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.

Generic Security Properties: Integrity, Authenticity

Travel Document Communication Establishment Authorization Data

Restricted-revealable authorization information for a human user used for verification of the authorization attempts as an authorized user (PACE password). These data are stored in the TOE and not send to it.

Generic Security Properties: Confidentiality, Integrity

4.2 Users / Subjects

Travel Document Holder

A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [PP_BAC]. Please note that a travel document holder can also be an attacker (s. below).

travel document presenter (traveller)

A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [PP_BAC]. Please note that a travel document presenter can also be an attacker (s. below).

Terminal

A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [PP_BAC].

Basic Inspection System with PACE (BISPACE)

A technical system being used by an inspecting authority 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). BIS-PACE implements the terminal's part of the PACE protocol and



authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.

Document Signer (DS)

An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C DS), see [ICAO_9303]. This role is usually delegated to a Personalisation Agent.

Country Signing Certification Authority (CSCA)

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 document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (C CSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO_9303], 5.5.1.

Personalisation Agent

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: (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 [ICAO_9303], (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). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [PP_BAC].

Manufacturer

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 cycle phase²⁴. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [PP_BAC].

Attacker

A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. This external entity is commensurate with 'Attacker' in [PP_BAC].

4.3 Threats

T.Skimming

Adverse action: An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless/contact interface of the TOE.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical travel document data

T.Eavesdropping

Adverse action: An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical travel document data

T.Tracing

Adverse action: An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: privacy of the travel document holder

T.Forgery

Adverse action: An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS-PACE by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

Threat agent: having high attack potential

Asset: integrity of the travel document

T.Abuse-Func

Adverse action: An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the travel document holder.

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

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document



T.Information_Leakage

Adverse action: An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

Threat agent: having high attack potential

Asset: confidentiality of User Data and TSF-data of the travel document

T.Phys-Tamper

Adverse action: An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the travel document in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.

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

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

T.Malfunction

Adverse action: An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

T.Configuration

Adverse action: An attacker may access to the TOE at Manufacturing and Personalization phases (steps 5 and 6) to try 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.

Threat agent: having high attack potential, being in possession of one or more MRTD in Pre-personalization or Personalization phases.

Asset: authenticity of logical MRTD data

T. Forgery_Supplemental_Data

Adverse action: An attacker alters fraudulently the data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object. This may lead the inspection system using these data to be deceived.

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



Asset: authenticity of data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object

T.Counterfeit

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

4.4 Organisational Security Policies

P.Manufact

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

P.Pre-Operational

- 1.) The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
- 2.) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE.
- 3.) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase.
- 4.) If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

P.Card_PKI

- 1.) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (CCSCA).
- 2.) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C CSCA) having to be made available to the travel document Issuer by strictly secure means, see [ICAO_9303], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [ICAO_9303], 5.5.1.
- 3.) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer

Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

P.Trustworthy_PKI

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

P.Terminal

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

- 1.) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [ICAO_9303].
- 2.) They shall implement the terminal parts of the PACE protocol [ICAO_TR_SAC], of the Passive Authentication [ICAO_9303] and use them in this order²⁸. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- 3.) The related terminals need not to use any own credentials.
- 4.) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [ICAO_9303]).
- 5.) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

4.5 Assumptions

A.Passive_Auth

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [ICAO_9303].

5 Security Objectives

5.1 Security Objectives for the TOE

OT.Data_Integrity

Integrity of Data

The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying). The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Data_Authenticity

Authenticity of Data The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side.

The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

OT.Data_Confidentiality

Confidentiality of Data

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Tracing

Tracing travel document

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

Application Note:

Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity)³⁵ cannot be achieved by the current TOE.

OT.Prot_Abuse-Func

Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the



TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

OT.Prot_Inf_Leak

Protection against Information Leakage

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document

- o 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,
- o by forcing a malfunction of the TOE and/or
- o by a physical manipulation of the TOE.

Application Note:

This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Phys-Tamper

Protection against Physical Tampering

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the travel document's Embedded Software by means of

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

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 have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

OT.Identification

Identification of the TOE

The TOE must provide means to store Initialisation and Pre-Personalisation Data in its nonvolatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the PrePersonalisation data includes writing of the Personalisation Agent Key(s).

OT.AC_Pers***Personalization of the Electronic Document***

The TOE must ensure that the logical travel document 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 Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

OT.Configuration

During Pre-personalization and Personalization phases, the TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions. It must also ensure secure erasing of useless keys.

OT.Update_File

During Operational Use phase, the TOE must allow the modification of Updatable Data if the write access to these objects is fulfilled by the Terminal.

OT.Chip_Auth_Proof

The TOE must support the 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 Chip Authentication as defined in [TR_03110]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

OT.Chip_Auth_Proof_PACE_CAM

The TOE must support the terminals to verify the identity and authenticity of the electronic document's chip as issued by the identified issuing State or Organization by means of the PACE-Chip Authentication Mapping (PACE-CAM) as defined in [ICAO_9303]. The authenticity proof provided by electronic document's chip shall be protected against attacks with high attack potential.

5.2 Security Objectives for the Operational Environment

5.2.1 *Travel document Issuer as the general responsible*

The travel document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

OE.Legislative_Compliance***Issuing of the travel document***

The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.

5.2.2 *Travel document Issuer and CSCA: travel document's PKI (issuing) branch*

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment:



OE.Passive_Auth_Sign

Authentication of travel document by Signature

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (C CSCA). Hereby authenticity and integrity of these certificates are being maintained. A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [ICAO_9303]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO_9303]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

OE.Personalisation

Personalisation of travel document

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enrol the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO_9303], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [ICAO_9303] (in the role of a DS).

5.2.3 Terminal operator: Terminal's receiving branch

OE.Terminal

Terminal operating

The terminal operators must operate their terminals as follows:

- 1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [ICAO_9303].
- 2.) The related terminals implement the terminal parts of the PACE protocol [ICAO_TR_SAC], of the Passive Authentication [ICAO_TR_SAC] (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- 3.) The related terminals need not to use any own credentials.
- 4.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C CSCA and C DS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [ICAO_9303]).
- 5.) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI



certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST

5.2.4 *Travel document holder Obligations*

OE.Travel_Document_Holder

Travel document holder Obligations

The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

5.2.5 *Miscellaneous*

OE.Auth_Key_Travel_Document

Travel document Authentication Key

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Exam_Travel_Document

Examination of the physical part of the travel document

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The BIS-PACE for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [ICAO_TR_SAC]. Additionally to these points the Chip Authentication Protocol Version 1 or PACE-CAM are also performed to verify the Authenticity of the presented travel document's chip.

5.3 Security Objectives Rationale

5.3.1 *Threats*

T.Skimming The threat T.Skimming addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact interface. This threat is countered by the security objectives OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality through the PACE authentication. The objective OE.Travel_Document_Holder ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

T.Eavesdropping The threat T.Eavesdropping addresses listening to the communication between the TOE and a rightful terminal in order to gain the User Data transferred there.

This threat is countered by the security objective OT.Data_Confidentiality through a trusted channel based on the PACE authentication.

T.Tracing The threat T.Tracing addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE, whereby the attacker does not a priori know the correct values of the PACE password. This threat is directly countered by security objectives OT.Tracing (no gathering TOE tracing data) and OE.Travel_Document_Holder (the attacker does not a priori know the correct values of the shared passwords).

T.Forgery The threat T.Forgery addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective OT.AC_Pers requires the TOE to limit the write access for the travel document to the trustworthy Personalisation Agent (cf. OE.Personalisation). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives OT.Data_Integrity and OT.Data_Authenticity, respectively. The objectives OT.Prot_Phys-Tamper and OT.Prot_Abuse-Func contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to OE.Terminal and performing the Passive Authentication using the Document Security Object as aimed by OE.Passive_Auth_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE.

T.Abuse-Func The threat T.Abuse-Func addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-coded security functionality. The security objective OT.Prot_Abuse-Func ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

T.Information_Leakage The threat T.Information_Leakage is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is obviously addressed by the directly related security objective OT.Prot_Inf_Leak

T.Phys-Tamper The threat T.Phys-Tamper is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is obviously addressed by the directly related security objective OT.Prot_Phys-Tamper

T.Malfunction The threat T.Malfunction is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is obviously addressed by the directly related security objective OT.Prot_Malfunction

T.Configuration The threat T.Configuration "Tampering attempt of the TOE during preparation" addresses attacks in Pre-personalization and Personalization phases. The attacker trying to access to unauthorized TOE functions, trying to access or to modify sensitive information exchanged between the TOE and the Personalization system. Protection of the TOE during these two phases is directly addressed by OT.Configuration "Protection of the TOE preparation"



T. Forgery_Supplemental_Data The threat T. Forgery_Supplemental_Data “Forgery of supplemental data stored in the TOE” addresses the fraudulent alteration of Updatable Data. The TOE protects the update of these data thanks to OT.Update_File “Modification of file in Operational Use Phase” that ensures inspection system are authenticated and data to be updated are sent through a secure channel ensuring integrity, authenticity and confidentiality.

T.Counterfeit The threat T.Counterfeit “Counterfeit of travel document chip data” addresses the attack of unauthorized copy or reproduction of the genuine travel document’s chip. This attack is thwarted by chip an identification and authenticity proof required by OT.Chip_Auth_Proof “Proof of the travel document’s chip authenticity” using an authentication key pair to be generated by the issuing State or Organisation. OT.Chip_Auth_Proof_PACE_CAM ensures that the chip in addition to CA also supports the PACE-Chip Authentication Mapping (PACE-CAM) protocol, which supports the same security functionality as CA does. PACE-CAM enables much faster authentication of the of the chip than running PACE with general mapping followed by CA. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by OE.Auth_Key_Travel_Document “Travel document Authentication Key”. According to OE.Exam_Travel_Document “Examination of the physical part of the travel document” the General Inspection system has to perform the Chip Authentication Protocol Version 1 or PACE-CAM to verify the authenticity of the travel document’s chip.

5.3.2 Organisational Security Policies

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

P.Pre-Operational The OSP P.Pre-Operational is enforced by the following security objectives: OT.Identification is affine to the OSP’s property ‘traceability before the operational phase’; OT.AC_Pers and OE.Personalisation together enforce the OSP’s properties ‘correctness of the User- and the TSF-data stored’ and ‘authorisation of Personalisation Agents’; OE.Legislative_Compliance is affine to the OSP’s property ‘compliance with laws and regulations’.

P.Card_PKI The OSP P.Card_PKI is enforced by establishing the issuing PKI branch as aimed by the objectives OE.Passive_Auth_Sign (for the Document Security Object).

P.Trustworthy_PKI The OSP P.Trustworthy_PKI is enforced by OE.Passive_Auth_Sign (for CSCA, issuing PKI branch).

P.Terminal The OSP P.Terminal is obviously enforced by the objective OE.Terminal, whereby the one-to-one mapping between the related properties is applicable.

5.3.3 Assumptions

A.Passive_Auth The Assumption A.Passive_Auth “PKI for Passive Authentication” is directly addressed by OE.Passive_Auth_Sign requiring the travel document issuer to establish a PKI for Passive Authentication, generating Document Signing private keys only for rightful

organisations and requiring the Document Signer to sign exclusively correct Document Security Objects to be stored on travel document.

5.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Skimming	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OE.Travel Document Holder	Section 5.3.1
T.Eavesdropping	OT.Data Confidentiality	Section 5.3.1
T.Tracing	OT.Tracing , OE.Travel Document Holder	Section 5.3.1
T.Forgery	OT.AC Pers , OT.Data Authenticity , OT.Data Integrity , OT.Prot Abuse-Func , OT.Prot Phys-Tamper , OE.Personalisation , OE.Passive Auth Sign , OE.Terminal	Section 5.3.1
T.Abuse-Func	OT.Prot Abuse-Func	Section 5.3.1
T.Information Leakage	OT.Prot Inf Leak	Section 5.3.1
T.Phys-Tamper	OT.Prot Phys-Tamper	Section 5.3.1
T.Malfunction	OT.Prot Malfunction	Section 5.3.1
T.Configuration	OT.Configuration	Section 5.3.1
T.Forgery Supplemental Data	OT.Update File	Section 5.3.1
T.Counterfeit	OT.Chip Auth Proof , OT.Chip Auth Proof PACE CAM , OE.Exam Travel Document , OE.Auth Key Travel Document	Section 5.3.1

Table 9 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.Data Integrity	T.Skimming , T.Forgery
OT.Data Authenticity	T.Skimming , T.Forgery
OT.Data Confidentiality	T.Skimming , T.Eavesdropping
OT.Tracing	T.Tracing
OT.Prot Abuse-Func	T.Forgery , T.Abuse-Func
OT.Prot Inf Leak	T.Information Leakage
OT.Prot Phys-Tamper	T.Forgery , T.Phys-Tamper
OT.Prot Malfunction	T.Malfunction
OT.Identification	
OT.AC Pers	T.Forgery
OT.Configuration	T.Configuration



OT.Update File	T. Forgery Supplemental Data
OT.Chip Auth Proof	T.Counterfeit
OT.Chip Auth Proof PACE CAM	T.Counterfeit
OE.Legislative Compliance	
OE.Passive Auth Sign	T.Forgery
OE.Personalisation	T.Forgery
OE.Terminal	T.Forgery
OE.Travel Document Holder	T.Skimming, T.Tracing
OE.Auth Key Travel Document	T.Counterfeit
OE.Exam Travel Document	T.Counterfeit

Table 10 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.Manufact	OT.Identification	Section 5.3.2
P.Pre-Operational	OT.Identification, OT.AC Pers, OE.Personalisation, OE.Legislative Compliance	Section 5.3.2
P.Card PKI	OE.Passive Auth Sign	Section 5.3.2
P.Trustworthy PKI	OE.Passive Auth Sign	Section 5.3.2
P.Terminal	OE.Terminal	Section 5.3.2

Table 11 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.Data Integrity	
OT.Data Authenticity	
OT.Data Confidentiality	
OT.Tracing	
OT.Prot Abuse-Func	
OT.Prot Inf Leak	
OT.Prot Phys-Tamper	
OT.Prot Malfunction	
OT.Identification	P.Manufact, P.Pre-Operational
OT.AC Pers	P.Pre-Operational
OT.Configuration	
OT.Update File	

OT.Chip Auth Proof	
OT.Chip Auth Proof PACE CAM	
OE.Legislative Compliance	P.Pre-Operational
OE.Passive Auth Sign	P.Card PKI, P.Trustworthy PKI
OE.Personalisation	P.Pre-Operational
OE.Terminal	P.Terminal
OE.Travel Document Holder	
OE.Auth Key Travel Document	
OE.Exam Travel Document	

Table 12 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.Passive Auth	OE.Passive Auth Sign	Section 5.3.3

Table 13 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.Legislative Compliance	
OE.Passive Auth Sign	A.Passive Auth
OE.Personalisation	
OE.Terminal	
OE.Travel Document Holder	
OE.Auth Key Travel Document	
OE.Exam Travel Document	

Table 14 Security Objectives for the Operational Environment and Assumptions - Coverage

6 Extended Requirements

6.1 Extended Families

6.1.1 Extended Family FPT_EMS - TOE Emanation

6.1.1.1 Description

The additional family FPT_EMS (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 SCD 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, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

6.1.1.2 Extended Components

Extended Component FPT_EMS.1

Description

This family defines requirements to mitigate intelligible emanations.

FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Definition

FPT_EMS.1 TOE Emanation

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].

Dependencies: No dependencies.



6.1.2 Extended Family FIA_API - Authentication Proof of Identity

6.1.2.1 Description

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

Application note 10: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter 'Explicitly stated IT security requirements (APE_SRE)') from a TOE point of view.

6.1.2.2 Extended Components

Extended Component FIA_API.1

Description

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

Definition

FIA_API.1 Authentication Proof of Identity

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

Dependencies: No dependencies.

6.1.3 Extended Family FMT_LIM - Limited capabilities

6.1.3.1 Description

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 abuse of functions by limiting the capabilities of the functions and by limiting their availability.

6.1.3.2 Extended Components

Extended Component FMT LIM.1

Description

Definition

FMT_LIM.1 Limited capabilities

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]

Dependencies: No dependencies.

Extended Component FMT LIM.2

Description

Definition

FMT_LIM.2 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]

Dependencies: No dependencies.

6.1.4 Extended Family FAU_SAS - Audit data storage

6.1.4.1 Description

To describe the security functional requirements of the TOE, the 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:

6.1.4.2 Extended Components

Extended Component FAU SAS.1

Description

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



*Definition***FAU_SAS.1 Audit storage**

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

Dependencies: No dependencies.

6.1.5 Extended Family FCS_RND - Generation of random numbers**6.1.5.1 Description**

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

6.1.5.2 Extended Components**Extended Component FCS_RND.1***Description*

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

*Definition***FCS_RND.1 Quality metric for random numbers**

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

Dependencies: No dependencies.

7 Security Requirements

7.1 Security Functional Requirements

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter.

7.1.1 Class FCS Cryptographic Support

FCS_CKM.1/DH_PACE Cryptographic key generation

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to [TR03111]** and specified cryptographic key sizes **192 to 521 bit** that meet the following: **[ICAO_TR_SAC]**.

FCS_CKM.1/CA Cryptographic key generation

FCS_CKM.1.1/CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below**:

Key Generation Algorithm	Key Sizes	Standard
based on ECDH compliant to [ISO_11770]	192 to 512 bit	[TR_03111]
based on DH	1024, 1536 and 2048	[TR_03110] and PKCS#3

FCS_CKM.1/CAM Cryptographic key generation

FCS_CKM.1.1/CAM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **based on ECDH compliant to [ISO_11770]** and specified cryptographic key sizes **192 to 521 bit** that meet the following: **[TR_03110]**.

FCS_CKM.1/CA_DATA_GEN Cryptographic key generation

FCS_CKM.1.1/CA_DATA_GEN The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below**

Algorithm	Key Size	Standard
Chip Authentication Data Generation using DH keys compliant to PKCS#3	1024 to 2048 bits in steps of 512 bits	PKCS#3
Chip authentication data generation using ECDH keys compliant to [ISO_15946]	192 to 512 bits	[TR_03111]

FCS_CKM.1/GP Cryptographic key generation

FCS_CKM.1.1/GP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below:**

Key Generation Algorithm	Key Sizes	Standard
Triple-DES in CBC mode	112 bit	[GPC_SPE_034]
AES in CBC mode	128, 192 and 256	[GPC_SPE_014]

FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1/PACE_ENC Cryptographic operation

FCS_COP.1.1/PACE_ENC The TSF shall perform **refer to table below** in accordance with a specified cryptographic algorithm **refer to table below** and cryptographic key sizes **refer to table below** that meet the following: **refer to table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging-encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[ICAO_TR_SAC]
secure messaging-encryption and decryption	TDES in CBC mode	112 bits	[ICAO_TR_SAC]

FCS_COP.1/PACE_MAC Cryptographic operation

FCS_COP.1.1/PACE_MAC The TSF shall perform **refer table below** in accordance with a specified cryptographic algorithm **refer table below** and cryptographic key sizes **refer table below** that meet the following: **refer table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging - message authentication code	AES CMAC	128, 192 and 256 bits	[ICAO_TR_SAC]
secure messaging - message authentication code	Retail MAC	112 bits	[ICAO_TR_SAC]

FCS_COP.1/CAM Cryptographic operation

FCS_COP.1.1/CAM The TSF shall perform **the PACE-CAM protocol** in accordance with a specified cryptographic algorithm **PACE-CAM** and cryptographic key sizes **192 to 521 bits** that meet the following: **[ICAO_9303]**.

FCS_COP.1/CA_ENC Cryptographic operation

FCS_COP.1.1/CA_ENC The TSF shall perform **refer to table below** in accordance with a specified cryptographic algorithm **refer to table below** and cryptographic key sizes **refer to table below** that meet the following: **refer to table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging-encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[TR-03110]
secure messaging-encryption and decryption	TDES in CBC mode	112 bits	[TR-03110]

FCS_COP.1/CA_MAC Cryptographic operation

FCS_COP.1.1/CA_MAC The TSF shall perform **refer table below** in accordance with a specified cryptographic algorithm **refer table below** and cryptographic key sizes **refer table below** that meet the following: **refer table below**

Cryptographic Operations	Algorithms	Key sizes	Norms
secure messaging - message authentication code	AES CMAC	128, 192 and 256 bits	[TR-03110]
secure messaging - message authentication code	Retail MAC	112 bits	[TR-03110]



FCS_COP.1/GP_ENC Cryptographic operation

FCS_COP.1.1/GP_ENC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

Cryptographic Operation	Algorithm	Key Sizes	Standard
secure messaging (GP) – encryption and decryption	Triple-DES in CBC mode	112 bit	[FIPS_46_3]
secure messaging (GP) – encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[NIST_800_38A]

FCS_COP.1/GP_AUTH Cryptographic operation

FCS_COP.1.1/GP_AUTH The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic Operation	Algorithm	Key Sizes	Standard
symmetric authentication – message authentication code	Full 3DES MAC	112 bit	[ISO_9797_1]
symmetric authentication – message authentication code	AES CMAC	128, 198 and 256 bits	[NIST_800_38B]

FCS_COP.1/GP_MAC Cryptographic operation

FCS_COP.1.1/GP_MAC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

Cryptographic Operation	Algorithm	Key Size(s)	Standard
secure messaging - message authentication code	Retail MAC	112 bit	[ISO_9797_1]
secure messaging (GP) - encryption and decryption	AES CMAC	128, 192 and 256 bits	[NIST_800_38B]

FCS_COP.1/GP_KEY_DEC Cryptographic operation

FCS_COP.1.1/GP_KEY_DEC The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**:

Cryptographic Operation	Algorithm	Key Sizes	Standard
key decryption	Triple-DES in ECB mode	112 bit	[FIPS_46_3]
key decryption	AES in CBC mode	128, 192 and 256 bits	[FIPS_197]

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **the average Shannon entropy per internal random bit exceeds 0.999**.

7.1.2 Class FIA Identification and Authentication
FIA_AFL.1/PACE Authentication failure handling

FIA_AFL.1.1/PACE The TSF shall detect when **10** unsuccessful authentication attempts occur related to **authentication attempts using the PACE password as shared password**.

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the PACE authentication attempts**.

Application Note:

The PACE password being referred here are MRZ or CAN

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow

- o **To establish a communication channel,**
- o **Carrying out the PACE protocol according to [ICAO_TR_SAC],**
- o **To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS**
- o **To carry out the Chip Authentication Protocol v.1 according to [TR-03110]**
- o **To carry out the PACE CAM protocol according to [ICAO-9303]**

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



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

FIA_UAU.1/PACE Timing of authentication

FIA_UAU.1.1/PACE The TSF shall allow

- o **to establish the communication channel,**
- o **carrying out the PACE Protocol according to [ICAO_TR_SAC]**
- o **to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS,**
- o **to identify themselves by selection of the authentication key**
- o **to carry out the Chip Authentication Protocol v.1 according to [TR_03110]**
- o **to carry out the PACE CAM Protocol according to [ICAO-9303]**
- o **to carry out the authentication of the Manufacturer and Personalization Agent**

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

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

FIA_UAU.4/PACE Single-use authentication mechanisms

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

- o **PACE Protocol according to [ICAO_TR_SAC],**
- o **Authentication Mechanisms based on Triple-DES or AES**
- o **none.**

Application Note:

The authentication mechanisms based on Triple-DES and AES is the authentication process performed in phases 5 and 6.

FIA_UAU.5/PACE Multiple authentication mechanisms

FIA_UAU.5.1/PACE The TSF shall provide

- o **PACE protocol (all mappings) according to [ICAO_TR_SAC],**
- o **Passive Authentication according to [ICAO_9303],**
- o **Secure messaging in MAC-ENC mode according to [ICAO_TR_SAC]**
- o **Symmetric Authentication Mechanism based on Triple-DES or AES**
- o **none**

to support user authentication.



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

- **Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.**
- **The TOE accepts the authentication attempt as Personalisation Agent by the Authentication Mechanism with Personalization Agent Key(s).**
- **After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.**
- **After run of the PACE-CAM Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the PACE-CAM.**
- **The TOE accepts the authentication attempt as Personalisation Agent by the Authentication Mechanism with Personalization Agent Key(s).**
- **none.**

FIA_UAU.6/PACE Re-authenticating

FIA_UAU.6.1/PACE The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.**

FIA_UAU.6/CA Re-authenticating

FIA_UAU.6.1/CA The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after a successful run of Chip Authentication shall be verified as being sent by the PACE Terminal.**

FIA_AFL.1/MP Authentication failure handling

FIA_AFL.1.1/MP The TSF shall detect when **1** unsuccessful authentication attempts occur related to **authentication of the Manufacturer and the Personalization Agent.**

FIA_AFL.1.2/MP When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **slow down exponentially the next authentication.**



FIA_UAU.6/MP Re-authenticating

FIA_UAU.6.1/MP The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful authentication of the terminal with the Symmetric Authentication Mechanism shall be verified as being sent by the authenticated terminal.**

FIA_API.1/CA Authentication Proof of Identity

FIA_API.1.1/CA The TSF shall provide a **Chip Authentication Protocol Version 1 according to [TR_03110]** to prove the identity of the TOE.

FIA_API.1/CAM Authentication Proof of Identity

FIA_API.1.1/CAM The TSF shall provide a **PACE-CAM according to [ICAO_9303]** to prove the identity of the TOE.

7.1.3 Class FDP User Data Protection**FDP_ACC.1/TRM Subset access control**

FDP_ACC.1.1/TRM The TSF shall enforce the **Access Control SFP on terminals gaining access to user data and data stored in EF.SOD of the logical travel document and none.**

FDP_ACF.1/TRM Security attribute based access control

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

- o **Subjects:**
 - **Terminal,**
 - **BIS-PACE.**
- o **Objects:**
 - **data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document,**
 - **data in EF.DG3 of the logical travel document,**
 - **data in EF.DG4 of the logical travel document,**
 - **all TOE intrinsic secret cryptographic keys stored in the travel document**
- o **Security attributes:**
 - **Authentication status of terminals**
- o **none.**



FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **a BIS-PACE is allowed to read data objects from FDP_ACF.1/TRM according to [4] after a successful PACE authentication as required by FIA_UAU.1/PACE.**

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

FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- o **Any terminal being not authenticated as PACE authenticated BIS- PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.**
- o **Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.**
- o **none.**

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

- o **Session Keys (immediately after closing related communication session),**
- o **the ephemeral private key ephem-SK picc -PACE (by having generated a DH shared secret K)**
- o **none.**

FDP_UCT.1/TRM Basic data exchange confidentiality

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

FDP_UIT.1/TRM Data exchange integrity

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

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

FDP_ACC.1/UPD_FILE Subset access control

FDP_ACC.1.1/UPD_FILE The TSF shall enforce the **UPD_FILE Access Control SFP** on terminals gaining write, read and modification access to data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD.

FDP_ACF.1/UPD_FILE Security attribute based access control

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

- o **Subjects:**
 - **Personalization Agent,**
 - **Terminal,**
- o **Objects:**
 - **data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**
- o **Security attributes**
 - **authentication status of terminals,**

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

- o **the Personalization Agent is allowed to write, read and modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD.**

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

FDP_ACF.1.4/UPD_FILE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Any Terminal is not allowed to modify the data in the file(s) EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD.**

FDP_UCT.1/CA Basic data exchange confidentiality

FDP_UCT.1.1/CA [Editorially Refined] The TSF shall enforce the **CA Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure after Chip Authentication.

FDP_UIT.1/CA Data exchange integrity

FDP_UIT.1.1/CA [Editorially Refined] The TSF shall enforce the **CA Access Control SFP** to **transmit and receive** user data in a manner protected from **deletion, modification, insertion and replay** errors after Chip Authentication.

FDP_UIT.1.2/CA [Editorially Refined] The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred after Chip Authentication.

FDP_ACC.1/CA Subset access control

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

FDP_ACF.1/CA Security attribute based access control

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

- o **Subjects:**
 - **General Inspection System,**
 - **Terminal,**
- o **Objects:**
 - **data EF.DG1 to EF.DG16 of the logical MRTD,**
 - **data in EF.COM,**
 - **data in EF.SOD,**
- o **Security attributes**
 - **authentication status of terminals.**

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

- o **the successfully authenticated General Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD..**

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

FDP_ACF.1.4/CA The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**

7.1.4 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE Inter-TSF trusted channel

FTP_ITC.1.1/PACE The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/PACE The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE [Editorially Refined] The TSF shall **enforce** communication via the trusted channel for **any data exchange between the TOE and the Terminal**.

FTP_ITC.1/MP Inter-TSF trusted channel

FTP_ITC.1.1/MP The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/MP The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/MP The TSF shall initiate communication via the trusted channel for **loading sensitive data (Pre-Perso_K, Perso_K, PACE_PWD, CA_SK) shall be encrypted**.

7.1.5 Class FAU Security Audit**FAU_SAS.1 Audit storage**

FAU_SAS.1.1 The TSF shall provide **the Manufacturer** with the capability to store **the Initialisation and Pre-Personalisation Data** in the audit records.

7.1.6 Class FMT Security Management**FMT_SMF.1 Specification of Management Functions**

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

- o **Initialization,**
- o **Pre-personalisation,**
- o **Personalisation,**
- o **Configuration,**
- o **Protection of incoming user data,**
- o **Protection of outgoing user data.**



FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles

- o **Manufacturer,**
- o **Personalization Agent,**
- o **Terminal,**
- o **PACE authenticated BIS-PACE,**
- o **General Inspection System.**

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

FMT_LIM.1 Limited capabilities

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

Deploying test features after TOE delivery do not allow

- o **User Data to be manipulated and disclosed,**
- o **TSF data to be manipulated or disclosed,**
- o **software to be reconstructed,**
- o **substantial information about construction of TSF to be gathered which may enable other attacks and,**
- o **none**

FMT_LIM.2 Limited capabilities

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

Deploying test features after TOE delivery do not allow

- o **User Data to be manipulated and disclosed,**
- o **TSF data to be manipulated or disclosed,**
- o **software to be reconstructed,**
- o **substantial information about construction of TSF to be gathered which may enable other attacks,**
- o **none**

FMT_MTD.1/INI_ENA Management of TSF data

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to **write** the **Initialisation Data and the Pre-personalisation Data** to **the Manufacturer**.

Application Note:

Please refer to F.ACW for details of the data written by the manufacturer.

FMT_MTD.1/INI_DIS Management of TSF data

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to **read out** the **Initialisation Data and the Pre-personalisation Data** to **the Personalisation Agent**.

FMT_MTD.1/KEY_READ Management of TSF data

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the

- o **PACE passwords,**
- o **Manufacturer Keys**
- o **Pre-personalization Agent Keys,**
- o **Personalisation Agent Keys,**
- o **The Chip Authentication private key**

to **none**.

FMT_MTD.1/PA Management of TSF data

FMT_MTD.1.1/PA The TSF shall restrict the ability to **write** the **document Security Object (SO D)** to **the Personalization Agent**.

FMT_MTD.1/CAPK Management of TSF data

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **load** the **Chip Authentication private key** to **the personalization agent**.

FMT_MTD.1/UPD_FILE Management of TSF data

FMT_MTD.1.1/UPD_FILE The TSF shall restrict the ability to **set** the **identifiers of files that can be modified in phase 7 (different from EF.COM, EF.SOD, EF.DG1 to EF.DG16)** to **the Personalization Agent**.



FMT_MTD.1/LCS_PERS Management of TSF data

FMT_MTD.1.1/LCS_PERS The TSF shall restrict the ability to **switch the LCS from phase 6 to phase 7 to the Personalization Agent.**

7.1.7 Class FPT Protection of the Security Functions**FPT_EMS.1 TOE Emanation**

FPT_EMS.1.1 The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to

- o **PACE session keys (PACE-K mac, PACE-K enc),**
- o **the ephemeral private key ephem-SK picc -PACE,**
- o **Personalization Agent Key(s),**
- o **Chip Authentication Private Key**
- o **Chip Authentication Session Keys**

and **none.**

FPT_EMS.1.2 The TSF shall ensure **any users** are unable to use the following interface **travel document's contactless/contact interface and circuit contacts** to gain access to

- o **PACE session keys (PACE-K mac, PACE-K enc),**
- o **the ephemeral private key ephem-SK picc -PACE,**
- o **Personalization Agent Key(s),**
- o **Chip Authentication Private Key**
- o **Chip Authentication Session Keys**

and **none.**

FPT_FLS.1 Failure with preservation of secure state

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

- o **Exposure to operating conditions causing a TOE malfunction,**
- o **Failure detected by TSF according to FPT_TST.1,**
- o **none.**

FPT_PHP.3 Resistance to physical attack

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



FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions**

- o **At reset**

to demonstrate the correct operation of **the TSF**.

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

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

7.2 Security Requirements Rationale

7.2.1 Objectives

7.2.1.1 Security Objectives for the TOE

OT.Data_Integrity The security objective OT.Data_Integrity aims that the TOE always ensures integrity of the User and TSF-data stored and, after the PACE authentication, of these data exchanged (physical manipulation and unauthorised modifying). Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_ACC.1/CA and FDP_ACF.1/CA). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. Unauthorised modifying of the exchanged data is addressed, in the first line, by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FDP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). A trusted channel using CA can also be established as defined in FIA_UAU.6/CA, FDP_UCT.1/CA and FDP_UIT.1/CA that utilizes FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC. FCS_CKM.1/CA and FCS_CKM.1/CAM are used for key establishment.

The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords.

The SFR FMT_MTD.1/CAPK helps maintain integrity of the CA key.

FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The SFR FCS_RND.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE control write access to data on file thus helping maintain its integrity.

FIA_UAU.6/MP ensures that all data sent during personalization is via a secure channel.



OT.Data_Authenticity The security objective OT.Data_Authenticity aims ensuring authenticity of the User- and TSFdata (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE Authentication or Chip Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE or FCS_CKM.1/CA, FCS_CKM.1/CAM and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/CA, FDP_UCT.1/CA and FDP_UIT.1/CA. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FCS_RND.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related. FIA_UAU.6/MP ensures that all data sent during personalization is via a secure channel.

OT.Data_Confidentiality The security objective OT.Data_Confidentiality aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication, of these data exchanged. This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. FDP_RIP.1 requires erasing the values of session keys (here: for Kenc). The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy. The SFR FCS_RND.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related. FIA_UAU.6/CA, FDP_UCT.1/CA and FDP_UIT.1/CA ensure all data after a successful Chip Authentication is sent via a secure channel that utilizes FCS_COP.1/CA_ENC and FCS_COP.1/CA_ENC. The keys are established using FCS_CKM.1/CA and FCS_CKM.1/CAM. FIA_UAU.6/MP ensures that all data sent during personalization is via a secure channel.

OT.Tracing The security objective OT.Tracing aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without a priori knowledge of the correct values of shared PACE passwords. This objective is achieved as follows: (i) while establishing PACE communication with a PACE password (non-blocking authorisation data) – by FIA_AFL.1/PACE; (ii) for listening to PACE communication (is of importance for the current PP, since SOD is cardindividual) – FTP_ITC.1/PACE.

OT.Prot_Abuse-Func The security objective OT.Prot_Abuse_Func aims preventing TOE's functions being not intended to be used in the operational phase from manipulating and disclosing the User- and TSF-data. This objective is achieved by FMT_LIM.1 and FMT_LIM.2



preventing misuse of test and other functionality of the TOE having not to be used in the TOE's operational life cycle phase.

OT.Prot_Inf_Leak The security objective OT.Prot_Inf_Leak aims protection against disclosure of confidential User- and TSF-data stored on / processed by the TOE. This objective is achieved

- o by FPT_EMS.1 for 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,
- o by FPT_FLS.1 and FPT_TST.1 for forcing a malfunction of the TOE, and
- o by FPT_PHP.3 for a physical manipulation of the TOE.

OT.Prot_Phys-Tamper The security objective OT.Prot_Phys-Tamper aims protection of the confidentiality and integrity of the User- and TSF-data as well as embedded software stored in the TOE. This objective is completely covered by FPT_PHP.3 in an obvious way.

OT.Prot_Malfunction The security objective OT.Prot_Malfunction aims ensuring a correct operation of the TOE by preventing its operation outside the normal operating conditions. This objective is covered by FPT_TST.1 requiring self tests to demonstrate the correct operation of the TOE and tests of authorised users to verify the integrity of the TSF-data and the embedded software (TSF code) as well as by FPT_FLS.1 requiring entering a secure state of the TOE in case of detected failure or operating conditions possibly causing a malfunction.

OT.Identification The security objective OT.Identification addresses the storage of Initialisation and PrePersonalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip.

This will be ensured by TSF according to SFR FAU_SAS.1. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialisation and Prepersonalisation Data (including the Personalisation Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cycle phase 'operational use'. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.AC_Pers The security objective OT.AC_Pers aims that only Personalisation Agent can write the User- and the TSF-data into the TOE. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data. FIA_UAU.5/PACE ensures access is granted only after authentication as personalization agent. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SOD and, in generally, personalisation data). The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related. The SFR FMT_MTD.1/KEY_READ restricts the access to the Personalisation Agent Keys. The SFRs FMT_MTD.1/KEY_READ and FPT_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key. FIA_UAU.6/MP ensures that all data sent during personalization is via a secure channel. FIA_AFL.1/MP handles authentication failures during personalization phase. FMT_MTD.1/LCS_PERS ensures only Personalization Agent can change life cycle state from Phase 6 to Phase 7. FDP_ACF.1/UPD_FILE and FDP_ACC.1/UPD_FILE control the write access to the files.

OT.Configuration The security objective OT.Configuration "Protection of the TOE preparation" addresses management of the Data Configuration, Pre-personalization Agent keys, Personalization Agent keys and the Life Cycle State of the TOE.

The authentication of the terminal as Manufacturer is performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5/MP. The Manufacturer can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH) with the Pre-personalization key. FIA_UAU.6/MP describes the re-authentication. In case of failed authentication attempts FIA_AFL.1/MP enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The SFR FTP_ITC.1/MP allows the Manufacturer to communicate with the OS.

Once step 4 is done, the MRTD packaging responsible is allowed to set the Pre-personalization Agent keys according to the SFR FCS_COP.1/GP_KEY_DEC. The SFR FMT_MTD.1/MP_KEY_READ prevents read access to the Pre-personalization keys and ensure together with the SFR FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentiality of these keys.

In step 5, the authentication of the terminal as Manufacturer shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5/MP. The Manufacturer shall be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH).

In case of failed authentication attempts FIA_AFL.1/MP enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack

The SFR FIA_UAU.6/MP describes the re-authentication and FDP_UCT.1/MP the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/GP, FCS_RND.1 (for key generation), and FCS_COP.1/GP_ENC as well as FCS_COP.1/GP_MAC for the ENC_MAC_Mode. The SFR FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

The Manufacturer and the Personalization Agent can select the protection mode of user data following FMT_MOF.1.1/GP.

The SFR FMT_MTD.1/MP_KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentiality of these keys.

OT.Update_File The security objective OT.Update_File "Modification of file in Operational Use Phase" addresses the modification of Updatable Data as defined in FDP_ACC.1/UPD_FILE. The SFR FDP_ACF.1/UPD_FILE clarifies what can be done by which subject: after a correct authentication the Personalization Agent is allowed to write, read and modify these Updatable Data during Pre-Personalisation and Personalisation phases. Any Terminal is not allowed to modify them during Operational phase. Only a successfully authenticated Inspection System is allowed to modify Updatable Data, only the files set following FMT_MTD.1/UPD_FILE by the Personalization Agent during Pre-Personalisation and Personalisation phases.

OT.Chip_Auth_Proof The security objective OT.Chip_Auth_Proof "Proof of travel document's chip authenticity" is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1/CA proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Data is generated by using FCS_CKM.1/CA_DATA_GEN. The Chip Authentication Protocol v.1 [TR_03110] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure

messaging). The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Chip_Auth_Proof_PACE_CAM OT.Chip_Auth_Proof_PACE_CAM aims to ensure the authenticity of the electronic document's chip by the PACE-CAM protocol. This is supported by FCS_CKM.1/CAM for cryptographic key-generation, and FIA_API.1/CAM and FCS_COP.1/CAM for the implementation itself, as well as FIA_UID.1/PACE and FIA_UAU.5/PACE, the latter supporting the PACE protocol.

7.2.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Data Integrity	FCS_CKM.1/DH_PACE , FCS_COP.1/PACE_MAC , FIA_UAU.1/PACE , FIA_UAU.5/PACE , FIA_UAU.6/CA , FIA_UID.1/PACE , FIA_UAU.4/PACE , FIA_UAU.6/PACE , FDP_ACF.1/TRM , FDP_ACC.1/TRM , FDP_UCT.1/TRM , FDP_UIT.1/TRM , FTP_ITC.1/PACE , FMT_MTD.1/PA , FMT_MTD.1/CAPK , FMT_MTD.1/KEY_READ , FCS_COP.1/CA_MAC , FCS_CKM.1/CA , FCS_CKM.4 , FCS_COP.1/CA_ENC , FDP_RIP.1 , FMT_SMF.1 , FMT_SMR.1/PACE , FPT_PHP.3 , FIA_UAU.6/MP , FDP_ACC.1/UPD_FILE , FDP_ACF.1/UPD_FILE , FDP_UCT.1/CA , FDP_UIT.1/CA , FCS_RND.1 , FDP_ACC.1/CA , FDP_ACF.1/CA , FCS_CKM.1/CAM	Section 7.3.1
OT.Data Authenticity	FCS_CKM.1/DH_PACE , FCS_COP.1/PACE_MAC , FIA_UAU.1/PACE , FIA_UAU.5/PACE , FIA_UAU.6/CA , FIA_UID.1/PACE , FIA_UAU.4/PACE , FIA_UAU.6/PACE , FTP_ITC.1/PACE , FMT_MTD.1/PA , FMT_MTD.1/KEY_READ , FCS_CKM.1/CA , FCS_CKM.4 , FDP_RIP.1 , FMT_SMF.1 , FMT_SMR.1/PACE , FIA_UAU.6/MP , FDP_UCT.1/CA , FDP_UIT.1/CA , FCS_RND.1 , FCS_CKM.1/CAM	Section 7.3.1
OT.Data Confidentiality	FCS_CKM.1/DH_PACE , FCS_COP.1/PACE_ENC , FIA_UAU.1/PACE , FIA_UAU.5/PACE , FIA_UAU.6/CA , FIA_UID.1/PACE , FIA_UAU.4/PACE , FIA_UAU.6/PACE , FDP_ACF.1/TRM , FDP_ACC.1/TRM , FDP_UCT.1/TRM , FDP_UIT.1/TRM , FTP_ITC.1/PACE , FMT_MTD.1/PA ,	Section 7.3.1

	FMT_MTD.1/KEY_READ , FCS_CKM.1/CA , FCS_CKM.4 , FCS_COP.1/CA_ENC , FDP_RIP.1 , FMT_SMF.1 , FMT_SMR.1/PACE , FIA_UAU.6/MP , FDP_UCT.1/CA , FDP_UIT.1/CA , FCS_RND.1 , FCS_CKM.1/CAM	
OT.Tracing	FTP_ITC.1/PACE , FIA_AFL.1/PACE	Section 7.3.1
OT.Prot_Abuse-Func	FMT_LIM.1 , FMT_LIM.2	Section 7.3.1
OT.Prot_Inf_Leak	FPT_EMS.1 , FPT_FLS.1 , FPT_PHP.3 , FPT_TST.1	Section 7.3.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 7.3.1
OT.Prot_Malfunction	FPT_FLS.1 , FPT_TST.1	Section 7.3.1
OT.Identification	FMT_MTD.1/INI_ENA , FMT_MTD.1/INI_DIS , FAU_SAS.1 , FMT_SMF.1 , FMT_SMR.1/PACE	Section 7.3.1
OT.AC_Pers	FMT_MTD.1/PA , FMT_MTD.1/KEY_READ , FMT_MTD.1/INI_ENA , FMT_MTD.1/INI_DIS , FAU_SAS.1 , FIA_UAU.5/PACE , FMT_SMF.1 , FMT_SMR.1/PACE , FPT_EMS.1 , FIA_UAU.6/MP , FIA_AFL.1/MP , FDP_ACC.1/UPD_FILE , FDP_ACF.1/UPD_FILE , FMT_MTD.1/LCS_PERS	Section 7.3.1
OT.Configuration	FCS_CKM.1/GP , FCS_COP.1/GP_ENC , FCS_COP.1/GP_MAC , FCS_COP.1/GP_AUTH , FCS_COP.1/GP_KEY_DEC , FIA_UAU.6/MP , FTP_ITC.1/MP , FCS_CKM.4 , FIA_AFL.1/MP , FPT_EMS.1 , FPT_FLS.1 , FPT_PHP.3 , FCS_RND.1	Section 7.3.1
OT.Update_File	FDP_ACC.1/UPD_FILE , FDP_ACF.1/UPD_FILE , FMT_MTD.1/UPD_FILE	Section 7.3.1
OT.Chip_Auth_Proof	FCS_CKM.1/CA , FCS_COP.1/CA_ENC , FCS_COP.1/CA_MAC , FIA_API.1/CA , FMT_SMF.1 , FMT_SMR.1/PACE , FMT_MTD.1/KEY_READ , FMT_MTD.1/CAPK , FCS_CKM.1/CA_DATA_GEN	Section 7.3.1
OT.Chip_Auth_Proof_PACE_CAM	FCS_COP.1/CAM , FIA_UAU.5/PACE , FIA_UID.1/PACE , FIA_API.1/CAM , FCS_CKM.1/CAM	Section 7.3.1

Table 15 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FCS_CKM.1/DH_PACE	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality
FCS_CKM.1/CA	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.Chip Auth Proof
FCS_CKM.1/CAM	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.Chip Auth Proof PACE CAM
FCS_CKM.1/CA_DATA_GEN	OT.Chip Auth Proof
FCS_CKM.1/GP	OT.Configuration
FCS_CKM.4	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.Configuration
FCS_COP.1/PACE_ENC	OT.Data Confidentiality
FCS_COP.1/PACE_MAC	OT.Data Integrity , OT.Data Authenticity
FCS_COP.1/CAM	OT.Chip Auth Proof PACE CAM
FCS_COP.1/CA_ENC	OT.Data Integrity , OT.Data Confidentiality , OT.Chip Auth Proof
FCS_COP.1/CA_MAC	OT.Data Integrity , OT.Chip Auth Proof
FCS_COP.1/GP_ENC	OT.Configuration
FCS_COP.1/GP_AUTH	OT.Configuration
FCS_COP.1/GP_MAC	OT.Configuration
FCS_COP.1/GP_KEY_DEC	OT.Configuration
FCS_RND.1	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.Configuration
FIA_AFL.1/PACE	OT.Tracing
FIA_UID.1/PACE	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.Chip Auth Proof PACE CAM
FIA_UAU.1/PACE	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality
FIA_UAU.4/PACE	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality
FIA_UAU.5/PACE	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.AC Pers , OT.Chip Auth Proof PACE CAM
FIA_UAU.6/PACE	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality
FIA_UAU.6/CA	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality

FIA AFL.1/MP	OT.AC Pers , OT.Configuration
FIA UAU.6/MP	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.AC Pers , OT.Configuration
FIA API.1/CA	OT.Chip Auth Proof
FIA API.1/CAM	OT.Chip Auth Proof PACE CAM
FDP ACC.1/TRM	OT.Data Integrity , OT.Data Confidentiality
FDP ACF.1/TRM	OT.Data Integrity , OT.Data Confidentiality
FDP RIP.1	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality
FDP UCT.1/TRM	OT.Data Integrity , OT.Data Confidentiality
FDP UIT.1/TRM	OT.Data Integrity , OT.Data Confidentiality
FDP ACC.1/UPD FILE	OT.Data Integrity , OT.AC Pers , OT.Update File
FDP ACF.1/UPD FILE	OT.Data Integrity , OT.AC Pers , OT.Update File
FDP UCT.1/CA	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality
FDP UIT.1/CA	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality
FDP ACC.1/CA	OT.Data Integrity
FDP ACF.1/CA	OT.Data Integrity
FTP ITC.1/PACE	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.Tracing
FTP ITC.1/MP	OT.Configuration
FAU SAS.1	OT.Identification , OT.AC Pers
FMT SMF.1	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.Identification , OT.AC Pers , OT.Chip Auth Proof
FMT SMR.1/PACE	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.Identification , OT.AC Pers , OT.Chip Auth Proof
FMT LIM.1	OT.Prot Abuse-Func
FMT LIM.2	OT.Prot Abuse-Func
FMT MTD.1/INI ENA	OT.Identification , OT.AC Pers
FMT MTD.1/INI DIS	OT.Identification , OT.AC Pers
FMT MTD.1/KEY READ	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.AC Pers , OT.Chip Auth Proof
FMT MTD.1/PA	OT.Data Integrity , OT.Data Authenticity , OT.Data Confidentiality , OT.AC Pers

FMT_MTD.1/CAPK	OT.Data Integrity , OT.Chip Auth Proof
FMT_MTD.1/UPD_FILE	OT.Update File
FMT_MTD.1/LCS_PERS	OT.AC Pers
FPT_EMS.1	OT.Prot Inf Leak , OT.AC Pers , OT.Configuration
FPT_FLS.1	OT.Prot Inf Leak , OT.Prot Malfunction , OT.Configuration
FPT_PHP.3	OT.Data Integrity , OT.Prot Inf Leak , OT.Prot Phys-Tamper , OT.Configuration
FPT_TST.1	OT.Prot Inf Leak , OT.Prot Malfunction

Table 16 SFRs and Security Objectives

7.2.3 Dependencies

7.2.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1/DH_PACE	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4 , FCS_COP.1/PACE_ENC , FCS_COP.1/PACE_MAC
FCS_CKM.1/CA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4 , FCS_COP.1/CA_ENC , FCS_COP.1/CA_MAC
FCS_CKM.1/CAM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4 , FCS_COP.1/CAM
FCS_CKM.1/CA_DATA_GEN	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4 , FCS_COP.1/CA_ENC , FCS_COP.1/CA_MAC
FCS_CKM.1/GP	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4 , FCS_COP.1/GP_ENC , FCS_COP.1/GP_AUTH , FCS_COP.1/GP_MAC , FCS_COP.1/GP_KEY_DEC
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/DH_PACE , FCS_CKM.1/CA , FCS_CKM.1/CAM , FCS_CKM.1/CA_DATA_GEN , FCS_CKM.1/GP
FCS_COP.1/PACE_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE , FCS_CKM.4
FCS_COP.1/PACE_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE , FCS_CKM.4
FCS_COP.1/CAM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CAM , FCS_CKM.4
FCS_COP.1/CA_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA , FCS_CKM.4
FCS_COP.1/CA_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/CA , FCS_CKM.4
FCS_COP.1/GP_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/GP , FCS_CKM.4
FCS_COP.1/GP_AUTH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and	FCS_CKM.1/GP , FCS_CKM.4

	(FCS_CKM.4)	
FCS_COP.1/GP_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/GP , FCS_CKM.4
FCS_COP.1/GP_KEY_DEC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/GP , FCS_CKM.4
FCS_RND.1	No Dependencies	
FIA_AFL.1/PACE	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_UID.1/PACE	No Dependencies	
FIA_UAU.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FIA_UAU.4/PACE	No Dependencies	
FIA_UAU.5/PACE	No Dependencies	
FIA_UAU.6/PACE	No Dependencies	
FIA_UAU.6/CA	No Dependencies	
FIA_AFL.1/MP	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_UAU.6/MP	No Dependencies	
FIA_API.1/CA	No Dependencies	
FIA_API.1/CAM	No Dependencies	
FDP_ACC.1/TRM	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_ACF.1/TRM	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM
FDP_RIP.1	No Dependencies	
FDP_UCT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM , FTP_ITC.1/PACE
FDP_UIT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM , FTP_ITC.1/PACE
FDP_ACC.1/UPD_FILE	(FDP_ACF.1)	FDP_ACF.1/UPD_FILE
FDP_ACF.1/UPD_FILE	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/UPD_FILE
FDP_UCT.1/CA	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/CA
FDP_UIT.1/CA	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/CA
FDP_ACC.1/CA	(FDP_ACF.1)	FDP_ACF.1/CA
FDP_ACF.1/CA	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/CA
FTP_ITC.1/PACE	No Dependencies	
FTP_ITC.1/MP	No Dependencies	
FAU_SAS.1	No Dependencies	
FMT_SMF.1	No Dependencies	
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FMT_LIM.1	No Dependencies	
FMT_LIM.2	No Dependencies	
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and	FMT_SMF.1 , FMT_SMR.1/PACE



	(FMT_SMR.1)	
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 , FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 , FMT_SMR.1/PACE
FMT_MTD.1/PA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 , FMT_SMR.1/PACE
FMT_MTD.1/CAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 , FMT_SMR.1/PACE
FMT_MTD.1/UPD_FILE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 , FMT_SMR.1/PACE
FMT_MTD.1/LCS_PERS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 , FMT_SMR.1/PACE
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FPT_TST.1	No Dependencies	

Table 17 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FMT_MSA.3 of FDP_ACF.1/TRM is discarded. The access control TSF according to FDP_ACF.1/TRM uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary.

The dependency FMT_MSA.3 of FDP_ACF.1/UPD_FILE is discarded. The access control TSF according to FDP_ACF.1/UPD_FILE uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/CA is discarded. The SFR requires the use of secure messaging between the MRTD and the BIS-PACE. There is no need for SFR FTP_ITC.1 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.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/CA is discarded. The SFR requires the use of secure messaging between the MRTD and the BIS-PACE. There is no need for SFR FTP_ITC.1 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.

The dependency FMT_MSA.3 of FDP_ACF.1/CA is discarded. The access control TSF according to FDP_ACF.1/CA uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary.

7.2.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.5
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	

ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

Table 18 SARs Dependencies

7.2.4 Rationale for the Security Assurance Requirements

The EAL5 was chosen to permit a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

7.2.4.1 AVA_VAN.5 Advanced methodical vulnerability analysis

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfill the security objectives OT.Chip_Auth_Proof.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 "Security architecture description"
- ADV_FSP.4 "Security-enforcing functional specification"
- ADV_TDS.3 "Basic modular design"
- ADV_IMP.1 "Implementation representation of the TSF"
- AGD_OPE.1 "Operational user guidance"
- AGD_PRE.1 "Preparative procedures"
- ATE_DPT.1 "Testing: basic design"

All of these are met or exceeded in the EAL5 assurance package

7.2.4.2 ALC_DVS.2 Sufficiency of security measures

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

The component ALC_DVS.2 augmented to EAL5 has no dependencies to other security requirements.



8 TOE Summary Specification

8.1 TOE Summary Specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions.

The security functionalities concerning the IC and the JC Platform are described in [ST-IC], [ST-PL] and are not redefined in this security target, although they must be considered for the TOE.

F.ACR - Access Control in Reading

This function controls access to read functions and enforces the security policy for data retrieval. Prior to any data retrieval, it authenticates the actor trying to access the data, and checks the access conditions are fulfilled as well as the life cycle state. It ensures that at any time, the following keys are never readable:

- o Manufacturer keys
- o Pre-personalization Agent keys,
- o Personalization Agent keys,
- o PACE passwords,
- o CA private key

Regarding the file structure:

In the Operational Use phase:

- o The terminal can read user data, the Document Security Object, EF.COM only after PACE authentication and through a valid secure channel.

In the Production and preparation stage:

The Manufacturer can read the Initialization Data in Stage 2 "Production". The pre-personalization agent and the Personalization Agent can read only the random identifier in Stage 3 "Preparation" stored in the TOE. Other data-elements can only be read after they are authenticated by the TOE (using their authentication keys).

It ensures as well that no other part of the memory can be accessed at anytime

F.ACW - Access Control in Writing

This function controls access to write functions (in NVM) and enforces the security policy for data writing. Prior to any data update, it authenticates the actor, and checks the access conditions are fulfilled as well as the life cycle state.

Regarding the file structure:

In the Operational Use phase:

It is not possible to create any files (system or data files). Furthermore, it is not possible to update any files (system or data files).

In the Production and preparation stage:

The Manufacturer can write all the Initialization and data for the Pre-personalization. The Personalization Agent can write through a valid secure channel all the data, PACE Passwords and CA Private key after it is authenticated by the TOE (using its authentication keys).

The Pre-Personalization Agent can write through a valid secure channel data to be used by the personalization agent (after it is authenticated by the TOE using its authentication keys).



The Pre-personalization agent is only active after delivery. The key that is written in the TOE for authentication purposes during manufacturing is meant for the pre-personalization agent. The Pre-personalization agent (which is seen as a sub-role of the Personalization agent) will refresh this key.

F.CA - Chip Authentication

This TSF provides Chip Authentication and session key generation to be used by F.SM, as described in [TR_03110].

F.CLR_INFO - Clear Residual Information

This security function ensures clearing of sensitive information

- o Authentication state is securely cleared in case an error is detected or a new authentication is attempted
- o Authentication data related to GP authentication and PACE authentication is securely cleared to prevent reuse
- o Session keys and the ephemeral private key ephem-SK picc -PACE are securely erased in case an error is detected or the secure communication session is closed

F.CRYPTO - Cryptographic Support

This Security Function provides the following cryptographic features:

- o Key Generation based on ECDH with key sizes 192 to 521 bits.
- o Key generation based on DH with key sizes 1024, 1536 and 2048.
- o Key generation for Triple-DES in CBC mode for 112 bits.
- o Key generation for AES in CBC mode with key sizes 128, 192 and 256 bits.
- o Secure messaging (encryption and decryption) using:
 - Triple DES in CBC mode (key size 112 bits) following [ICAO_TR_SAC].
 - AES in CBC mode (key sizes 128,192,256 bits) following [ICAO_TR_SAC].
- o Secure messaging (message authentication code) using:
 - Retail MAC with key size 112 bits following [ICAO_TR_SAC].
 - AES CMAC with key sizes 128,192 and 256 bits [ICAO_TR_SAC].
- o Secure messaging (encryption and decryption) using:
 - Triple DES in CBC mode (key size 112 bits) following [TR-03110].
 - AES in CBC mode (key sizes 128,192,256 bits) following [TR-03110].
- o Secure messaging (message authentication code) using:
 - Retail MAC with key size 112 bits following [TR-03110].
 - AES CMAC with key sizes 128,192 and 256 bits following [TR-03110].
- o GP Secure Messaging (encryption and decryption) using:
 - Triple-DES in CBC mode with key size 112 bits as defined in [FIPS_46_3].
 - AES with key sizes 128, 192 and 256 bits as defined in [NIST_800_38A].
- o GP Secure Messaging (message authentication code) using:
 - Retail MAC with key size 112 bits as defined in [ISO_9797_1].
 - AES CMAC with key sizes 128, 192 and 256 bits as defined in [NIST_800_38B].
- o Random number generation that meets the requirement the average Shannon entropy per internal random bit exceeds 0.999.



- o Symmetric Authentication - encryption and decryption using:
 - Full 3DES MAC with key size 112 bits as defined in [ISO_9797_1].
 - AES CMAC with key sizes 128, 192 and 256 bits as defined in [NIST_800_38B].
- o Key decryption using:
 - Triple-DES in ECB mode with key size 112 bits as defined in [FIPS_46_3].
 - AES in CBC mode with key sizes 128, 192 and 256 bits as defined in [FIPS_197].
- o Chip Authentication Data Generation using DH, with key sizes 1024 to 2048 bits in steps of 512 bits.
- o Chip Authentication Data Generation using ECDH, with key sizes 192 to 512 bits.
- o PACE-CAM as defined in [ICAO_9303] with key sizes 192 to 521 bits.

F.PACE - Authentication using PACE

This TSF provides the Password Authenticated Connection Establishment authentication (all mappings) and session keys generation to be used by F.SM, as described in [ICAO_9303].

In case the number of consecutive failed authentication attempts crosses number defined in FIA_AFL.1/PACE the TSF will slow down further authentication attempts.

F.PERS - MRTD Personalization

This security functionality ensures that the TOE, when delivered to the Personalization Agent, provides and requires authentication for data exchange. This authentication is based on a Triple DES and AES authentication mechanism. This function allows to:

- o Manage symmetric authentication using Personalization Agent keys,
- o Configuration of the TOE
- o Compute session keys to be used by F.SM,
- o Load user data,
- o Load Chip Authentication keys in encrypted form,
- o Disable read access to initialization data
- o Write the document Security Object (SO D)
- o Set the files that are allowed to be modified in phase 7,
- o Set TOE life cycle to Operational Use phase

In case the number of consecutive failed authentication attempts crosses 1 the TSF will slow down further authentication attempts.

F.PHY - Physical Protection

This Security Function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data, configuration data and TOE life cycle. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE.

This Security Function also limits any physical emanations from the TOE so as to prevent any information leakage via these emanations that might reveal or provide access to sensitive data.

Furthermore, it prevents deploying test features after TOE delivery.

F.PREP - MRTD Pre-personalization

This security functionality ensures that the TOE, when delivered to the Manufacturer, provides and requires an authentication mechanism for data exchange. This authentication is based on Triple DES and AES symmetric authentication mechanism. This function allows to:

- o Manage symmetric authentication using Pre-personalization Agent keys,
- o Compute session keys to be used by F.SM,
- o Initialization of the TOE,
- o Load Personalization Agent keys in encrypted form,
- o Store the Initialization and Pre-Personalization data in audit records.

In case the number of consecutive failed authentication attempts crosses 1 the TSF will slow down further authentication attempts.

F.SM - Secure Messaging

This security functionality ensures the confidentiality, authenticity and integrity of the communication between the TOE and the interface device. In the operational phase, after a successful Authentication Procedure (i.e. PACE or CA), a secure channel is established. This security functionality also provides a Secure Messaging (SCP02 and SCP03) for the Pre-personalization and Personalization phases. The protocols can be configured to protect the exchanges integrity and/or confidentiality. If an error occurs in the secure messaging layer or if the session is closed, the session keys are destroyed. This ensures protection against replay attacks as session keys are never reused.

F.SS - Safe State Management

This security functionality ensures that the TOE gets back to a secure state when:

- o a tearing occurs (during a copy of data in NVM).
- o an error due to self test as defined in FPT_TST.1.
- o any physical tampering is detected.

This security functionality ensures that if such a case occurs, the TOE either is switched in the state "kill card" or becomes mute

F.STST - Self Test

This security function implements self test features through platform functionalities at reset as defined in FPT_TST.1 to ensure the integrity of the TSF and TSF data.

8.2 SFRs and TSS

8.2.1 SFRs and TSS - Rationale

Class FCS Cryptographic Support

FCS_CKM.1/DH_PACE is met by F.PACE - Authentication using PACE that generates session keys after a successful PACE authentication using F.CRYPTO - Cryptographic Support

FCS_CKM.1/CA is met by F.CA - Chip Authentication that generates a key pair using F.CRYPTO - Cryptographic Support

FCS_CKM.1/CAM is met by F.CA - Chip Authentication that generates a key pair using F.CRYPTO - Cryptographic Support

FCS_CKM.1/CA_DATA_GEN is met by F.CRYPTO - Cryptographic Support.

FCS_CKM.1/GP is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that generate the keys using F.CRYPTO - Cryptographic Support.

FCS_CKM.4 is met by F.SM - Secure Messaging and F.CLR_INFO - Clear Residual Information that securely erase keys in case a secure messaging session is closed.

FCS_COP.1/PACE_ENC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement

FCS_COP.1/PACE_MAC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement

FCS_COP.1/CAM is met by F.PACE - Authentication using PACE that uses F.CRYPTO - Cryptographic Support to provide PACE-CAM functionality

FCS_COP.1/CA_ENC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement

FCS_COP.1/CA_MAC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement

FCS_COP.1/GP_ENC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement

FCS_COP.1/GP_AUTH is met by F.PREP - MRTD Pre-personalization and F.PERS - MRTD Personalization that use F.CRYPTO - Cryptographic Support to perform symmetric authentication

FCS_COP.1/GP_MAC is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support to maintain a secure messaging session as defined in the requirement



FCS_COP.1/GP_KEY_DEC is met by F.CRYPTO - Cryptographic Support

FCS_RND.1 is met by F.CRYPTO - Cryptographic Support that generates a random number using platform functionality

Class FIA Identification and Authentication

FIA_AFL.1/PACE is met by F.PACE - Authentication using PACE that handles the consecutive failed authentication attempts related to PACE

FIA_UID.1/PACE is met by F.ACR - Access Control in Reading that manages access to data based on the current authentication state.

It is also met by F.PACE - Authentication using PACE and F.CA - Chip Authentication that provide PACE and Chip Authentication.

FIA_UAU.1/PACE is met by F.ACR - Access Control in Reading that manages access to data based on the current authentication state.

It is also met by F.PACE - Authentication using PACE and F.CA - Chip Authentication that provide PACE and Chip Authentication.

It is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization for manufacturer and personalization agent authentication

FIA_UAU.4/PACE is met by F.CLR_INFO - Clear Residual Information that ensures all authentication data is securely erased to prevent reuse.

FIA_UAU.5/PACE is met by F.PACE - Authentication using PACE that provides PACE Authentication.

It is also met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that provides symmetric authentication.

It is also met by F.SM - Secure Messaging that provides a secure messaging channel.

FIA_UAU.6/PACE is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after PACE authentication

FIA_UAU.6/CA is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after CA authentication

FIA_AFL.1/MP is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that ensures that after 3 unsuccessful symmetric authentication attempts the TOE increases the time taken to respond to a terminal challenge

FIA_UAU.6/MP is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after GP authentication

FIA_API.1/CA is met by F.CA - Chip Authentication that provides Chip Authentication.

FIA_API.1/CAM is met by F.PACE - Authentication using PACE that provides PACE-CAM functionality to prove authenticity of the chip.

Class FDP User Data Protection

FDP_ACC.1/TRM is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided by F.PACE - Authentication using PACE

FDP_ACF.1/TRM is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided by F.PACE - Authentication using PACE

FDP_RIP.1 is met by F.CLR_INFO - Clear Residual Information that ensures keys are erased securely.

FDP_UCT.1/TRM is met by F.SM - Secure Messaging that ensures all user data is transmitted and received via a secure communication channel.

FDP_UIT.1/TRM is met by F.SM - Secure Messaging that ensures all user data is transmitted and received via a secure communication channel.

FDP_ACC.1/UPD_FILE is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.PACE - Authentication using PACE and F.PERS - MRTD Personalization

FDP_ACF.1/UPD_FILE is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.PACE - Authentication using PACE and F.PERS - MRTD Personalization

FDP_UCT.1/CA is met by F.SM - Secure Messaging that ensures all user data is transmitted and received via a secure communication channel.

FDP_UIT.1/CA is met by F.SM - Secure Messaging that ensures all user data is transmitted and received via a secure communication channel.

FDP_ACC.1/CA is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided by F.CA - Chip Authentication

FDP_ACF.1/CA is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanism provided by F.CA - Chip Authentication

Class FTP Trusted Path/Channels

FTP_ITC.1/PACE is met by F.SM - Secure Messaging that establishes a secure communication channel after a successful authentication using PACE protocol as defined in F.PACE - Authentication using PACE.

FTP_ITC.1/MP is met by F.SM - Secure Messaging that establishes a secure channel for communication for loading of keys as defined in F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization.

Class FAU Security Audit

FAU_SAS.1 is met by F.PREP - MRTD Pre-personalization

Class FMT Security Management

FMT_SMF.1 is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that provide the required management functions and F.SM - Secure Messaging that ensures protection of incoming and outgoing user data via secure communication.

FMT_SMR.1/PACE is met by F.PACE - Authentication using PACE, F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization. These roles are maintained by means of the authentication states during the authentication mechanisms provided by the 3 security functions.

FMT_LIM.1 is met by F.PHY - Physical Protection and F.SS - Safe State Management that ensure that no data can be manipulated or revealed and the TSF assumes a safe state in case any illegal attempts to do so are detected.

FMT_LIM.2 is met by F.PHY - Physical Protection and F.SS - Safe State Management that ensure that no data can be manipulated or revealed and the TSF assumes a safe state in case any illegal attempts to do so are detected.

FMT_MTD.1/INI_ENA is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalization

FMT_MTD.1/INI_DIS is met by F.ACR - Access Control in Reading that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalization

FMT_MTD.1/KEY_READ is met by F.ACR - Access Control in Reading that ensures the secret keys are never readable

FMT_MTD.1/PA is met by F.PERS - MRTD Personalization.

FMT_MTD.1/CAPK is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PERS - MRTD Personalization

FMT_MTD.1/UPD_FILE is met by F.PERS - MRTD Personalization that controls access conditions in F.ACW - Access Control in Writing to allow only the name set by the personalization agent to be able to edit files in operational phase.

FMT_MTD.1/LCS_PERS is met by F.PERS - MRTD Personalization that allows the personalization agent after successful authentication to switch the lifecycle state from phase 6 to phase 7

Class FPT Protection of the Security Functions

FPT_EMS.1 is met by F.PHY - Physical Protection that prevents emanations beyond permissible limits to prevent any accidental revelation of data.

FPT_FLS.1 is met by F.SS - Safe State Management that ensures a safe state is maintained.

FPT_PHP.3 is met by F.PHY - Physical Protection that protects the TOE against any physical probing or tampering by using F.SS - Safe State Management in case any physical manipulation is detected.

FPT_TST.1 is met by F.STST - Self Test that performs self tests to ensure integrity of the TSF

8.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FCS_CKM.1/DH_PACE	F.PACE - Authentication using PACE , F.CRYPTO - Cryptographic Support
FCS_CKM.1/CA	F.CA - Chip Authentication , F.CRYPTO - Cryptographic Support
FCS_CKM.1/CAM	F.CA - Chip Authentication , F.CRYPTO - Cryptographic Support
FCS_CKM.1/CA_DATA_GEN	F.CRYPTO - Cryptographic Support
FCS_CKM.1/GP	F.PERS - MRTD Personalization , F.PREP - MRTD Pre-personalization , F.CRYPTO - Cryptographic Support
FCS_CKM.4	F.SM - Secure Messaging , F.CLR_INFO - Clear Residual

	Information
FCS COP.1/PACE_ENC	F.SM - Secure Messaging , F.CRYPTO - Cryptographic Support
FCS COP.1/PACE_MAC	F.SM - Secure Messaging , F.CRYPTO - Cryptographic Support
FCS COP.1/CAM	F.CRYPTO - Cryptographic Support , F.PACE - Authentication using PACE
FCS COP.1/CA_ENC	F.SM - Secure Messaging , F.CRYPTO - Cryptographic Support
FCS COP.1/CA_MAC	F.CRYPTO - Cryptographic Support , F.SM - Secure Messaging
FCS COP.1/GP_ENC	F.SM - Secure Messaging , F.CRYPTO - Cryptographic Support
FCS COP.1/GP_AUTH	F.CRYPTO - Cryptographic Support , F.PERS - MRTD Personalization , F.PREP - MRTD Pre-personalization
FCS COP.1/GP_MAC	F.CRYPTO - Cryptographic Support , F.SM - Secure Messaging
FCS COP.1/GP_KEY_DEC	F.CRYPTO - Cryptographic Support
FCS RND.1	F.CRYPTO - Cryptographic Support
FIA AFL.1/PACE	F.PACE - Authentication using PACE
FIA UID.1/PACE	F.ACR - Access Control in Reading , F.PACE - Authentication using PACE , F.CA - Chip Authentication
FIA UAU.1/PACE	F.ACR - Access Control in Reading , F.PACE - Authentication using PACE , F.CA - Chip Authentication , F.PERS - MRTD Personalization , F.PREP - MRTD Pre-personalization
FIA UAU.4/PACE	F.CLR_INFO - Clear Residual Information
FIA UAU.5/PACE	F.PACE - Authentication using PACE , F.PERS - MRTD Personalization , F.PREP - MRTD Pre-personalization , F.SM - Secure Messaging
FIA UAU.6/PACE	F.SM - Secure Messaging
FIA UAU.6/CA	F.SM - Secure Messaging
FIA AFL.1/MP	F.PERS - MRTD Personalization , F.PREP - MRTD Pre-personalization
FIA UAU.6/MP	F.SM - Secure Messaging
FIA API.1/CA	F.CA - Chip Authentication
FIA API.1/CAM	F.PACE - Authentication using PACE
FDP ACC.1/TRM	F.ACR - Access Control in Reading , F.ACW - Access Control in Writing , F.PACE - Authentication using PACE
FDP ACF.1/TRM	F.ACR - Access Control in Reading , F.ACW - Access Control in Writing , F.PACE - Authentication using PACE
FDP RIP.1	F.CLR_INFO - Clear Residual Information
FDP UCT.1/TRM	F.SM - Secure Messaging
FDP UIT.1/TRM	F.SM - Secure Messaging
FDP ACC.1/UPD_FILE	F.ACR - Access Control in Reading , F.ACW - Access Control in Writing , F.PACE - Authentication using PACE , F.PERS - MRTD Personalization
FDP ACF.1/UPD_FILE	F.ACR - Access Control in Reading , F.ACW - Access Control in Writing , F.PACE - Authentication using PACE , F.PERS - MRTD

	Personalization
FDP UCT.1/CA	F.SM - Secure Messaging
FDP UIT.1/CA	F.SM - Secure Messaging
FDP ACC.1/CA	F.CA - Chip Authentication , F.ACR - Access Control in Reading , F.ACW - Access Control in Writing
FDP ACF.1/CA	F.CA - Chip Authentication , F.ACR - Access Control in Reading , F.ACW - Access Control in Writing
FTP ITC.1/PACE	F.SM - Secure Messaging , F.PACE - Authentication using PACE
FTP ITC.1/MP	F.SM - Secure Messaging , F.PERS - MRTD Personalization , F.PREP - MRTD Pre-personalization
FAU SAS.1	F.PREP - MRTD Pre-personalization
FMT SMF.1	F.PERS - MRTD Personalization , F.PREP - MRTD Pre-personalization , F.SM - Secure Messaging
FMT SMR.1/PACE	F.PACE - Authentication using PACE , F.PERS - MRTD Personalization , F.PREP - MRTD Pre-personalization
FMT LIM.1	F.PHY - Physical Protection , F.SS - Safe State Management
FMT LIM.2	F.PHY - Physical Protection , F.SS - Safe State Management
FMT MTD.1/INI ENA	F.ACW - Access Control in Writing , F.PREP - MRTD Pre-personalization
FMT MTD.1/INI DIS	F.ACR - Access Control in Reading , F.PERS - MRTD Personalization
FMT MTD.1/KEY_READ	F.ACR - Access Control in Reading
FMT MTD.1/PA	F.PERS - MRTD Personalization
FMT MTD.1/CAPK	F.ACW - Access Control in Writing , F.PERS - MRTD Personalization
FMT MTD.1/UPD_FILE	F.ACW - Access Control in Writing , F.PERS - MRTD Personalization
FMT MTD.1/LCS PERS	F.PERS - MRTD Personalization
FPT EMS.1	F.PHY - Physical Protection
FPT FLS.1	F.SS - Safe State Management
FPT PHP.3	F.PHY - Physical Protection , F.SS - Safe State Management
FPT TST.1	F.STST - Self Test

Table 19 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
F.ACR - Access Control in Reading	FIA UID.1/PACE , FIA UAU.1/PACE , FDP ACC.1/TRM , FDP ACF.1/TRM , FDP ACC.1/UPD_FILE , FDP ACF.1/UPD_FILE , FDP ACC.1/CA , FDP ACF.1/CA , FMT MTD.1/INI_DIS , FMT MTD.1/KEY_READ
F.ACW - Access Control in Writing	FDP ACC.1/TRM , FDP ACF.1/TRM , FDP ACC.1/UPD_FILE , FDP ACF.1/UPD_FILE , FDP ACC.1/CA , FDP ACF.1/CA , FMT MTD.1/INI_ENA , FMT MTD.1/CAPK , FMT MTD.1/UPD_FILE
F.CA - Chip Authentication	FCS CKM.1/CA , FCS CKM.1/CAM , FIA UID.1/PACE , FIA UAU.1/PACE , FIA API.1/CA , FDP ACC.1/CA , FDP ACF.1/CA

F.CLR_INFO - Clear Residual Information	FCS_CKM.4 , FIA_UAU.4/PACE , FDP_RIP.1
F.CRYPTO - Cryptographic Support	FCS_CKM.1/DH_PACE , FCS_CKM.1/CA , FCS_CKM.1/CAM , FCS_CKM.1/CA_DATA_GEN , FCS_CKM.1/GP , FCS_COP.1/PACE_ENC , FCS_COP.1/PACE_MAC , FCS_COP.1/CAM , FCS_COP.1/CA_ENC , FCS_COP.1/CA_MAC , FCS_COP.1/GP_ENC , FCS_COP.1/GP_AUTH , FCS_COP.1/GP_MAC , FCS_COP.1/GP_KEY_DEC , FCS_RND.1
F.PACE - Authentication using PACE	FCS_CKM.1/DH_PACE , FCS_COP.1/CAM , FIA_AFL.1/PACE , FIA_UID.1/PACE , FIA_UAU.1/PACE , FIA_UAU.5/PACE , FIA_API.1/CAM , FDP_ACC.1/TRM , FDP_ACF.1/TRM , FDP_ACC.1/UPD_FILE , FDP_ACF.1/UPD_FILE , FTP_ITC.1/PACE , FMT_SMR.1/PACE
F.PERS - MRTD Personalization	FCS_CKM.1/GP , FCS_COP.1/GP_AUTH , FIA_UAU.1/PACE , FIA_UAU.5/PACE , FIA_AFL.1/MP , FDP_ACC.1/UPD_FILE , FDP_ACF.1/UPD_FILE , FTP_ITC.1/MP , FMT_SMF.1 , FMT_SMR.1/PACE , FMT_MTD.1/INI_DIS , FMT_MTD.1/PA , FMT_MTD.1/CAPK , FMT_MTD.1/UPD_FILE , FMT_MTD.1/LCS_PERS
F.PHY - Physical Protection	FMT_LIM.1 , FMT_LIM.2 , FPT_EMS.1 , FPT_PHP.3
F.PREP - MRTD Pre-personalization	FCS_CKM.1/GP , FCS_COP.1/GP_AUTH , FIA_UAU.1/PACE , FIA_UAU.5/PACE , FIA_AFL.1/MP , FTP_ITC.1/MP , FAU_SAS.1 , FMT_SMF.1 , FMT_SMR.1/PACE , FMT_MTD.1/INI_ENA
F.SM - Secure Messaging	FCS_CKM.4 , FCS_COP.1/PACE_ENC , FCS_COP.1/PACE_MAC , FCS_COP.1/CA_ENC , FCS_COP.1/CA_MAC , FCS_COP.1/GP_ENC , FCS_COP.1/GP_MAC , FIA_UAU.5/PACE , FIA_UAU.6/PACE , FIA_UAU.6/CA , FIA_UAU.6/MP , FDP_UCT.1/TRM , FDP_UIT.1/TRM , FDP_UCT.1/CA , FDP_UIT.1/CA , FTP_ITC.1/PACE , FTP_ITC.1/MP , FMT_SMF.1
F.SS - Safe State Management	FMT_LIM.1 , FMT_LIM.2 , FPT_FLS.1 , FPT_PHP.3
F.STST - Self Test	FPT_TST.1

Table 20 TSS and SFRs - Coverage

9 GLOSSARY AND ACRONYMS

9.1 Glossary

Term	Definition
Agreement	This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [ICAO_9303] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organisation.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the travel document's chip to store the Initialization Data and Pre-personalisation Data.
Authenticity	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organisation
Basic Access Control (BAC)	Security mechanism defined in [ICAO_9303] by which means the travel document's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System with PACE protocol (BIS-PACE)	<p>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).</p> <p>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.</p>
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.
Biographical data (biodata)	The personalised details of the travel document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document. [ICAO_9303]
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.
Certificate chain	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.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_9303]
Country Signing CA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPUCCSCA) issued by Country Signing Certification Authority stored in the inspection system.



Term	Definition
Country Signing Certification Authority (CSCA)	<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. [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 pairs must be used for different roles, see [TR_03110].</p>
Country Verifying Certification Authority (CVCA)	<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].</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 PP.</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 pairs must be used for different roles, see [TR_03110].</p>
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used to validate card verifiable certificates.
CV Certificate	Card Verifiable Certificate according to [TR_03110].
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [ICAO_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.
PACE passwords	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_TR_SAC]
Document Details Data	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.
Document Security Object (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS). [ICAO_9303]
Document Signer (DS)	<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] and [ICAO_9303].</p> <p>This role is usually delegated to a Personalisation Agent.</p>



Term	Definition
Document Verifier (DV)	<p>An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing 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].</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 PP.</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).55 56</p>
Eavesdropper	A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]
Travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [TR_03110].
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO_9303]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO_9303]
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
IC Identification Data	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.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_9303]



Term	Definition
Improperly document person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_9303]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document's material (IC identification data).
Inspection	The act of a State examining an travel document presented to it by a traveller (the travel document holder) and verifying its authenticity. [ICAO_9303]
Inspection System (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organisation
Issuing Organisation	Organisation authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]
Issuing State	The Country issuing the travel document. [ICAO_9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the travel document's chip.
Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) <ul 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
Machine Readable Travel Document (MRTD)	Official document issued by a State or Organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_9303]
Machine Readable Zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_9303]



Term	Definition
Manufacturer	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.
Metadata of a CV Certificate	<p>Data within the certificate body (excepting Public Key) as described in [TR_03110].</p> <p>The metadata of a CV certificate comprise the following elements:</p> <ul style="list-style-type: none"> - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
ePassport application	<p>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.
Optional biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
PACE Password	A password needed for PACE authentication, e.g. CAN or MRZ.
Personalization	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. sec. 1.2, TOE life-cycle, Phase 3, Step 6).



Term	Definition
Personalization Agent	<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], (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>
Personalisation Data	<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>
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalisation Agent.
Personalization Agent Key	Cryptographic authentication key used (i) by the Personalisation Agent to prove his identity and to get access to the logical travel document and (ii) by the travel document's chip to verify the authentication attempt of a terminal as Personalisation Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/PACE.
Physical travel document	<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.
Pre-Personalisation	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalised travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalisation Agent Key Pair.
Pre-personalized travel document's chip	travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the traveller is applying for entry. [ICAO_9303]



Term	Definition
reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443.
secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO_9303]
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Service Provider	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.
Skimming	Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [ICAO_TR_SAC], namely (i) PACE or BAC and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.
Terminal	<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 PP the role 'Terminal' corresponds to any terminal being authenticated by the TOE.</p> <p>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).</p>
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Terminal Authorisation Level	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.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	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").
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
Travel document's Chip	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO, [ICAO_9303], sec III.
Travel document's Chip Embedded Software	Software embedded in a travel document's chip and not being developed by the IC Designer. The travel document's chip Embedded Software is designed in Phase 1 and embedded into the travel document's chip in Phase 2 of the TOE life-cycle.
Traveller	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.



Term	Definition
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC_1]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialization Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
User data	<p>All data (being not authentication data)</p> <p>(i) stored in the context of the ePassport application of the travel document as defined in [TR_03110] and</p> <p>(ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE .</p> <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_1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning ([CC_2]).</p>
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO_9303]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

9.2 Acronyms

Acronym	Term
<i>BIS</i>	Basic Inspection System
<i>BIS-PACE</i>	Basic Inspection System with PACE
<i>CA</i>	Chip Authentication
<i>CAN</i>	Card Access Number
<i>CC</i>	Common Criteria
<i>CPS</i>	Common Personalization System
<i>EF</i>	Elementary File
<i>GIS</i>	General Inspection System
<i>ICCSN</i>	Integrated Circuit Card Serial Number.
<i>LCS</i>	Life Cycle State
<i>MF</i>	Master File
<i>MRZ</i>	Machine readable zone
<i>n.a.</i>	Not applicable
<i>OSP</i>	Organisational security policy
<i>PACE</i>	Password Authenticated Connection Establishment
<i>PCD</i>	Proximity Coupling Device
<i>PICC</i>	Proximity Integrated Circuit Chip
<i>PP</i>	Protection Profile
<i>PT</i>	Personalisation Terminal
<i>RF</i>	Radio Frequency
<i>SAR</i>	Security assurance requirements
<i>SFR</i>	Security functional requirement
<i>SIP</i>	Standard Inspection Procedure
<i>TA</i>	Terminal Authentication
<i>TOE</i>	Target of Evaluation
<i>TSF</i>	TOE Security Functions
<i>TSP</i>	TOE Security Policy (defined by the current document)

10 REFERENCES

- [CC_1] Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", April 2017, Version 3.1 revision 5.
- [CC_2] "Common Criteria for information Technology Security Evaluation, Part 2: Security Functional component", April 2017, Version 3.1 revision 5.
- [CC_3] "Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance components", April 2017, Version 3.1 revision 5.
- [PP_IC] 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
- [PP_PACE] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) - BSI-CC-PP-0068-V2-2011-MA-01
- [PP_BAC] Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control - BSI-CC-PP-0055 v1.10 25th march 2009
- [PTF_CERT] NSCIB CC-18-200833
- [ST_PTF] FQR 110 8959 Ed 3.0 - ID One Cosmo V9 Essential Public ST
- [PTF_AGD1] ID-One Cosmo V9 Application Loading Protection Guidance, FQR: 110 8798, Issue 2, IDEMIA
- [PTF_AGD2] ID-One Cosmo V9 Applet Security Recommendations, FQR: 110 8794, Issue 4, IDEMIA
- [PTF_AGD3] Secure acceptance and delivery of sensitive element - FQR 110 8921 Ed1, IDEMIA
- [PTF_AGD_PRE] ID One Cosmo V9.0 Essential - Pre-Perso Guide, FQR 110 8797 Ed5 AGD PRE, IDEMIA
- [PTF_AGD_OPE] ID One Cosmo V9.0 Essential Reference Guide, 22 October 2018, FQR 110 8823 Ed5, IDEMIA
- [Applet_Perso_Guide] FQR 220 1306– CombICAO Applet – Perso Guide Ed 8, IDEMIA
- [Applet_User_Guide] FQR 220 1307– CombICAO Applet – User Guide Ed 9, IDEMIA
- [ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, 7th Edition, 2015 – Security Mechanisms for MRTDs
- [ICAO_TR_SAC] ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010
- [ISO_9797_1] ISO/IEC 9797-1 Information technology – Security techniques – Message Authentication codes (MACs) – part 1: Mechanisms using a block cipher, Second edition 2011-03-01
- [TR_03110] 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.
- [TR_03111] BSI, Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009
- [FIPS_46_3] FIPS 46-3, Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard (DES), 1999 October 25
- [FIPS_197] FIPS 197, Federal Information Processing Standards Publication (FIPS PUB 197), Advanced Encryption Standard (AES)
- [NIST_800_38B] NIST Special Publication 800-38B: 2005, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005
- [NIST_800_38A] NIST Special Publication 800-38A: 2001, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001
- [GPC_SPE_014] GlobalPlatform Card Technology - Secure Channel Protocol '03', Card Specification v2.2 – Amendment D Version 1.1.1 - Public Release July 2014
- [GPC_SPE_034] "GlobalPlatform Card Specification" Version 2.3 Public Release - October 2015 Document Reference: GPC_SPE_034

