



# **ComblCAO Applet v2.2 in EAC with PACE configuration for French ID on Cosmo V9.1**

## **Public Security Target**

Reference: FQR 550 0087 Ed 7

## DOCUMENT MANAGEMENT

<b>Business Unit – Department</b>	<b>INSI – R&amp;D</b>
<b>Document Title</b>	CombICAO Applet v2.2 in EAC with PACE configuration for French ID on Cosmo V9.1 Public Security Target
<b>FQR No</b>	550 0087
<b>FQR Issue</b>	7

## DOCUMENT EVOLUTION

Date	Revision	Modification
2020/03/17	1	Creation of the document
2020/04/13	2	Updated Platform version
2020/06/17	3	Updated reference of guidance documents
2021/01/14	4	Update following IAR FQR 220 1607 Ed2
2021/01/26	5	Update following Anssi Remark: Guidance edition update
2021/01/26	6	Update following IAR FQR 220 1607 Ed2
2023/03/20	6	Updates for surveillance
2025/12/08	7	Updates for reevaluation

## Table des matières

<b>TABLE OF TABLES.....</b>	<b>7</b>
<b>1 GENERAL.....</b>	<b>8</b>
1.1 INTRODUCTION.....	8
1.2 PRODUCT OVERVIEW .....	8
<b>2 ST INTRODUCTION.....</b>	<b>9</b>
2.1 ST REFERENCE AND TOE REFERENCE.....	9
2.1.1 <i>ST reference.....</i>	9
<i>EAL5 augmented with: .....</i>	9
• <i>ALC_DVS.2 .....</i>	9
2.1.2 <i>TOE reference.....</i>	9
2.2 TOE OVERVIEW .....	10
2.2.1 <i>Usage and major security features of the TOE .....</i>	10
2.2.2 <i>TOE type .....</i>	13
2.2.3 <i>Required non-TOE hardware/Software/firmware .....</i>	13
2.3 TOE DESCRIPTION .....	14
2.3.1 <i>Physical scope of the TOE.....</i>	14
2.3.2 <i>TOE delivery.....</i>	14
2.3.3 <i>Logical scope of the TOE .....</i>	16
2.3.4 <i>Authentication Protocols .....</i>	17
2.3.5 <i>Other features .....</i>	18
2.3.6 <i>TOE life cycle.....</i>	20
2.3.7 <i>Development Environment.....</i>	21
2.3.8 <i>Production Environment .....</i>	21
2.3.9 <i>Preparation Environment .....</i>	22
2.3.10 <i>Operational Environment.....</i>	22
<b>3 CONFORMANCE CLAIMS.....</b>	<b>24</b>
3.1 COMMON CRITERIA CONFORMANCE .....	24
3.2 PROTECTION PROFILE CONFORMANCE .....	24
3.2.1 <i>Overview.....</i>	24
3.2.2 <i>Assumptions .....</i>	25
3.2.3 <i>Threats .....</i>	25
3.2.4 <i>Organisational Security Policies.....</i>	25
3.2.5 <i>Security Objectives.....</i>	26
3.3 CC CONFORMANCE AND USAGE IN REAL LIFE .....	27
<b>4 SECURITY PROBLEM DEFINITION .....</b>	<b>28</b>
4.1 ASSETS.....	28
4.1.1 <i>Biometric Data .....</i>	28
4.1.2 <i>Authenticity of the MRTDs chip .....</i>	29
4.1.3 <i>User data stored on the TOE.....</i>	29
4.1.4 <i>User data transferred between the TOE and the terminal connected .....</i>	29
4.1.5 <i>MRTD tracing data .....</i>	29
4.1.6 <i>Accessibility to the TOE functions and data only for authorised subjects .....</i>	29
4.1.7 <i>Genuineness of the TOE.....</i>	30
4.1.8 <i>TOE intrinsic secret cryptographic keys.....</i>	30
4.1.9 <i>MRTD communication establishment authorisation data .....</i>	30
4.1.10 <i>Additional Assets as per Addendum.....</i>	31
4.2 SUBJECTS.....	31
4.2.1 <i>Subjects from PP.....</i>	32

4.2.2	<i>Additional Subjects as per Addendum</i> .....	35
4.3	THREATS.....	36
4.3.1	<i>Threats from PP</i> .....	36
4.3.2	<i>Additional Threats as per Addendum</i> .....	41
4.4	ORGANISATIONAL SECURITY POLICIES .....	41
4.5	ASSUMPTIONS .....	43
<b>5</b>	<b>SECURITY OBJECTIVES .....</b>	<b>45</b>
5.1	SECURITY OBJECTIVES FOR THE TOE .....	45
5.1.1	<i>Security Objectives from the PP</i> .....	45
5.1.2	<i>Additional Objectives as per Addendum</i> .....	48
5.1.3	<i>Additional Objectives for Active Authentication</i> .....	49
5.2	SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT .....	49
5.2.1	<i>Issuing State or Organisation</i> .....	49
5.2.2	<i>Receiving State or Organisation</i> .....	50
5.2.3	<i>eDigitalIdentity document Issuer as the general responsible</i> .....	51
5.2.4	<i>eDigitalIdentity document Issuer and CVCA: eDigitalIdentity document's PKI (issuing branch</i> <i>51</i>	51
5.2.5	<i>Terminal operator: Terminal's receiving branch</i> .....	52
5.2.6	<i>eDigitalIdentity document holder Obligations</i> .....	52
5.2.7	<i>Additional Security Objectives for the Operational Environment</i> .....	53
5.3	SECURITY OBJECTIVES RATIONALE.....	53
5.3.1	<i>Threats</i> .....	53
5.3.2	<i>Organisational Security Policies</i> .....	56
5.3.3	<i>Assumptions</i> .....	58
5.3.4	<i>SPD and Security Objectives</i> .....	59
<b>6</b>	<b>EXTENDED REQUIREMENTS .....</b>	<b>64</b>
6.1	EXTENDED FAMILIES .....	64
6.1.1	<i>Extended Family FPT_EMS - TOE Emanation</i> .....	64
6.1.2	<i>Extended Family FIA_API - Authentication Proof of Identity</i> .....	65
6.1.3	<i>Extended Family FMT_LIM - Limited capabilities</i> .....	66
6.1.4	<i>Extended Family FAU_SAS - Audit data storage</i> .....	67
6.1.5	<i>Extended Family FCS_RND - Generation of random numbers</i> .....	68
<b>7</b>	<b>SECURITY REQUIREMENTS .....</b>	<b>69</b>
7.1	SECURITY FUNCTIONAL REQUIREMENTS .....	69
7.1.1	<i>Class FCS Cryptographic Support</i> .....	69
7.1.2	<i>Class FIA Identification and Authentication</i> .....	74
7.1.3	<i>Class FDP User Data Protection</i> .....	78
7.1.4	<i>Class FTP Trusted Path/Channels</i> .....	82
7.1.5	<i>Class FAU Security Audit</i> .....	82
7.1.6	<i>Class FMT Security Management</i> .....	83
7.1.7	<i>Class FPT Protection of the Security Functions</i> .....	88
7.1.8	<i>Additional SFRs as per Addendum</i> .....	90
7.2	SECURITY ASSURANCE REQUIREMENTS.....	91
7.2.1	<i>ADV Development</i> .....	91
7.2.2	<i>AGD Guidance documents</i> .....	96
7.2.3	<i>ALC Life-cycle support</i> .....	98
7.2.4	<i>ASE Security Target evaluation</i> .....	102
7.2.5	<i>ATE Tests</i> .....	108
7.2.6	<i>AVA Vulnerability assessment</i> .....	111
7.3	SECURITY REQUIREMENTS RATIONALE .....	112
7.3.1	<i>Objectives</i> .....	112
7.3.2	<i>Rationale tables of Security Objectives and SFRs</i> .....	118

7.3.3	<i>Dependencies</i> .....	125
7.3.4	<i>Rationale for the Security Assurance Requirements</i> .....	131
7.3.5	<i>AVA_VAN.5 Advanced methodical vulnerability analysis</i> .....	131
7.3.6	<i>ALC_DVS.2 Sufficiency of security measures</i> .....	131
<b>8</b>	<b>TOE SUMMARY SPECIFICATION</b> .....	<b>132</b>
8.1	TOE SUMMARY SPECIFICATION .....	132
8.2	SFRs AND TSS .....	138
8.2.1	<i>SFRs and TSS - Rationale</i> .....	138
8.2.2	<i>Association tables of SFRs and TSS</i> .....	144
<b>9</b>	<b>GLOSSARY AND ACRONYMS</b> .....	<b>150</b>
9.1	GLOSSARY .....	150
1.1.1	<i>The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [ICAO_9303]</i> .....	153
9.2	ACRONYMS .....	160
<b>10</b>	<b>REFERENCES</b> .....	<b>162</b>

#### Table of figures

Figure 1	Physical Form of the Module .....	14
Figure 2	TOE Boundaries .....	16
Figure 3	Life cycle Overview .....	20

## Table of tables

Table 1 ST reference .....	9
Table 2 TOE reference.....	9
Table 3 PACE configuration .....	18
Table 4 Roles identification on the life cycle .....	20
Table 5 Image containing both Java Card platform and applet is loaded at IC manufacturer (Option 1) .....	22
Table 6 Cap file of CombICAO Applet v2.2 is loaded (using GP) (Option 2) .....	22
Table 7 Image containing both platform and applet is loaded through the loader of the IC (Option 3) .....	22
Table 8 Common Criteria conformance claim.....	24
Table 9 Protection Profile conformance .....	24
Table 10 Remote Inspection Procedure.....	36
Table 11 Threats and Security Objectives - Coverage .....	60
Table 12 Security Objectives and Threats - Coverage .....	61
Table 13 OSPs and Security Objectives - Coverage .....	61
Table 14 Security Objectives and OSPs - Coverage .....	62
Table 15 Assumptions and Security Objectives for the Operational Environment - Coverage.....	63
Table 16 Security Objectives for the Operational Environment and Assumptions - Coverage.....	63
Table 17 Security Objectives and SFRs - Coverage .....	121
Table 18 SFRs and Security Objectives .....	125
Table 19 SFRs Dependencies .....	129
Table 20 SARs Dependencies .....	130
Table 21 SFRs and TSS - Coverage.....	148
Table 22 TSS and SFRs - Coverage.....	149

# 1 GENERAL

## 1.1 Introduction

This security target describes the security needs induced by the CombICAO Applet v2.2 product in EAC with PACE configuration for French ID on IDEMIA underlying Java Card *ID-ONE Cosmo V9.1 Platform*, 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 within the security environment, and that the TOE summary specification addresses the requirements.

## 1.2 Product overview

The product is designed to support the following usages:

1. **eMRTD as per [ICAO\_9303] and European provisions [TR\_03110]; 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] and European provisions [TR\_03110].

The TOE can be configured in five configurations.

However, The current ST addresses CombICAO Applet v2.2 in configuration 4) below.

- 1) CombICAO Applet v2.2 product in **BAC** configuration with **CA**,
- 2) CombICAO Applet v2.2 product in **EAC** configuration,
- 3) CombICAO Applet v2.2 product in **EAC** with **PACE** configuration,
- 4) CombICAO Applet v2.2 product in **EAC** with **PACE** configuration for French ID
- 5) CombICAO Applet v2.2 product in **SSCD** configuration

## 2 ST INTRODUCTION

### 2.1 ST reference and TOE reference

#### 2.1.1 ST reference

<b>Title</b>	CombICAO Applet v2.2 in EAC with PACE configuration for French ID on Cosmo v9.1 Public Security Target
<b>ST Identification</b>	FQR 550 0087 Ed 7
<b>CC Version</b>	3.1 revision 5
<b>Authors</b>	INSI
<b>ITSEF</b>	CEA-LETI
<b>Certification Body</b>	ANSSI
<b>EAL</b>	EAL5 augmented with: <ul style="list-style-type: none"> <li>• ALC_DVS.2</li> <li>• AVA_VAN.5</li> </ul>
<b>PP</b>	[PP_EACwPACE]

**Table 1 ST reference**

#### 2.1.2 TOE reference

<b>Product Name</b>	CombICAO Applet v2.2
<b>TOE Name</b>	CombICAO Applet v2.2 in EAC with PACE configuration for French ID on ID-ONE Cosmo V9.1
<b>Developer Name</b>	INSI
<b>TOE Identification</b>	203731
<b>Platform Name</b>	ID-One Cosmo V9.1 Platform
<b>Platform Identification</b>	092915
<b>Platform Certificate</b>	[PTF_CERT]
<b>Guidance Documents</b>	[Applet_Perso_Guide], [Applet_User_Guide] [PTF_AGD_OPE], [PTF_AGD_PRE], [PTF_AGD1], [PTF_AGD2], [PTF_AGD3], [PTF_AGD4], [PTF_AGD5] and [PTF_AGD_SEC_AC]

**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 eDigitalIdentity document presenter 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 eDigitalIdentity document presenter 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 eDigitalIdentity 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, Extended Access Control to 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.

This Security Target addresses the protection of the logical eDigitalIdentity document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access

Control Mechanism. Also it addresses the Chip Authentication Version 1 described in [TR\_03110] as an alternative to the Active Authentication stated in [ICAO\_9303].

If BAC is supported by the TOE, the eDigitalIdentity document has to be evaluated and certified separately. This is due to the fact that [PP\_BAC] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA\_VAN.3).

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)
EDigitalIdentity document presenter	Holder

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

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The eDigitalIdentity document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable EDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity document's chip provide private communication (secure messaging) [TR\_03110], [ICAO\_TR\_SAC].

The Security Target requires the TOE to implement the Extended Access Control as defined in [TR\_03110]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1). The Chip Authentication Protocol v.1 (i) authenticates the eDigitalIdentity document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

### **2.2.2 TOE type**

The TOE is a composite product made up of an Embedded Software developed using Java Card technology, developed by INSI, composed on a Java Card open platform 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 eDigitalIdentity documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing :

- Password Authenticated Connection Establishment (PACE)
- Extended Access Control (EAC)
- Chip Authentication Mapping (CAM)
- Terminal Authentication (TA)

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

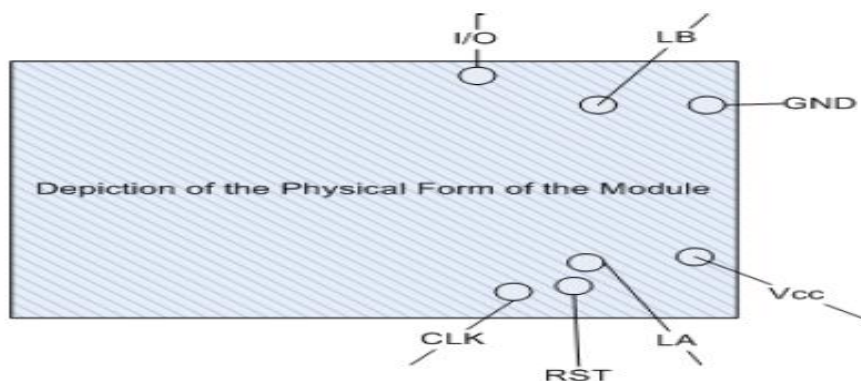
The TOE is physically made up of several components hardware and software.

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 V9.1 Platform: see [ST\_PTF] and [PTF\_CERT]
- CombICAO v2.2 application
- Associated guidance documentation (delivered in electronic version)

An ST Lite version of this Security Target will also be provided as a guidance document along with above-mentioned documents.

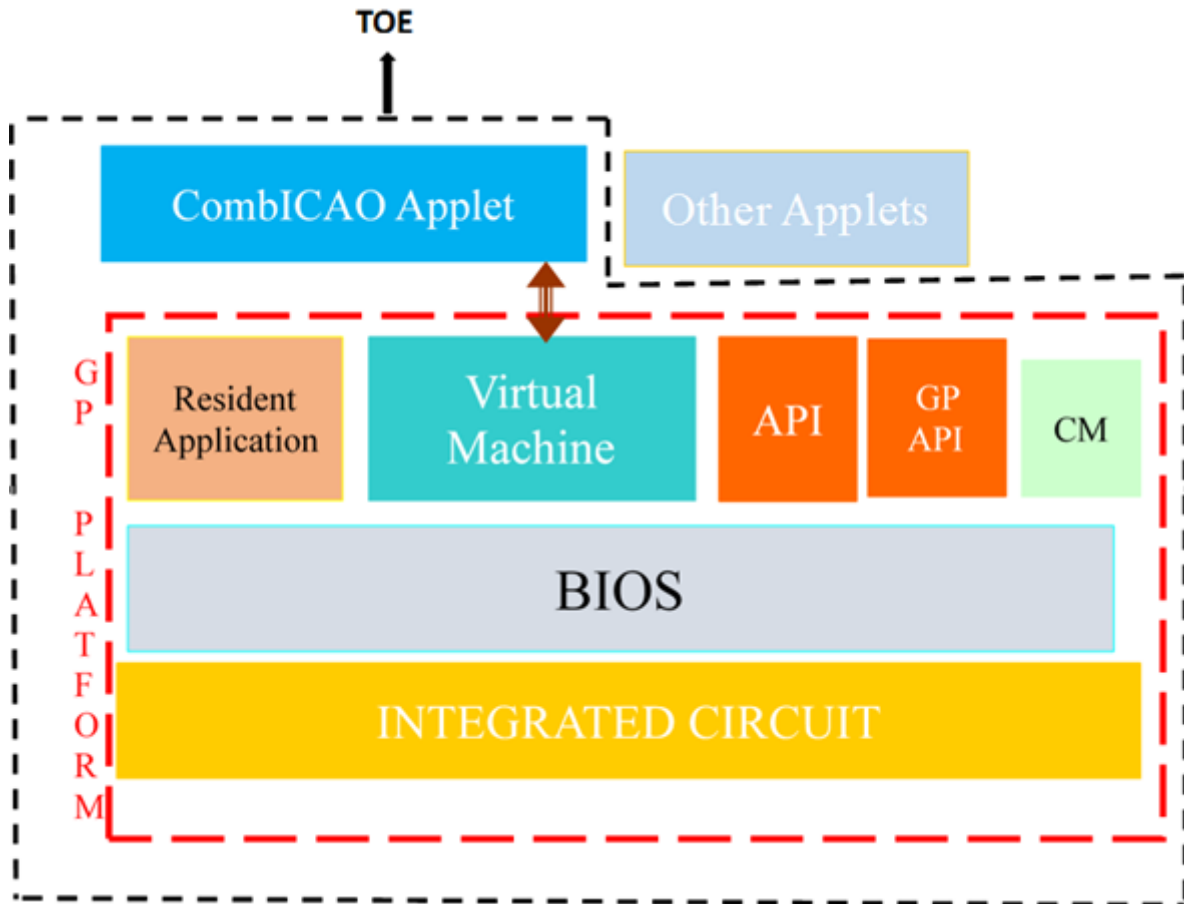
TOE Component	Identification	Form Factor of Delivery	Delivery method
CombICAO Applet v2.2 for MRTD	203731	ID1 or ID3 Passport booklets ID1 cards or ID3 holder pages Antenna <sup>1</sup> inlays Chip in modules on a reel	CPS tool is used in the case of an Image delivery. Otherwise, trusted courier is used.
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_AGD4] [PTF_AGD5] [PTF_AGD_SEC_AC] [PTF_AGD_PRE]		

Form factor and Delivery Preparation:

1. As per the Software Development Process of INSI, 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 INSI 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.

---

<sup>1</sup> The inlay production including the application of the antenna is not part of the TOE



**Figure 2 TOE Boundaries**

### 2.3.3 Logical scope of the TOE

The TOE is a smartcard, composed of :

- IC,
- Java Card Open Platform (OS) and
- CombICAO v2.2 application (data storage file structure)

The TOE scope encompasses the following features:

- Chip Authentication
- Terminal Authentication
- Password Authentication Connection Establishment (PACE v2) including the Chip Authentication Mapping
- Active 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 Terminal Authentication (TA)

This protocol enables the MRTD chip to verify that the terminal is entitled to access sensitive data. As the terminal may access sensitive data afterwards, all further communication MUST be protected appropriately. Terminal Authentication therefore also authenticates an ephemeral public key chosen by the terminal that was used to set up Secure Messaging with Chip Authentication. The MRTD chip MUST bind the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key of the terminal.

Terminal Authentication v1 is part of the EACv1 procedure defined in [TR\_03110].

### 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, 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.

Chip Authentication v1 is part of the EACv1 procedure defined in [TR\_03110].

### 2.3.4.3 Password Authenticated Connection Establishment (PACE v2)

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	Secure Messaging	Auth. Token	Hash Algo
---------------	---------	----------	------------	------------------	-------------	-----------

			(in bytes)			
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 Authenticatio n	AES	16	CBC / CMAC	CMAC	SHA- 1
PACE-ECDH-CAM-AES-192	Chip Authenticatio n	AES	24	CBC / CMAC	CMAC	SHA- 256
PACE-ECDH-CAM-AES-256	Chip Authenticatio n	AES	32	CBC / CMAC	CMAC	SHA- 256

**Table 3 PACE configuration**

#### 2.3.4.4 Active Authentication (AA)

Active Authentication is an authentication mechanism ensuring the chip is genuine. It uses a challenge-response protocol between the IS and the chip.

Active Authentication is realized with the INTERNAL AUTHENTICATE command.

The key and algorithms supported are the following:

RSA ISO/IEC 9796-2 with a key length of 1024 bits, 1536 bits or 2048 bits and hashing algorithm of SHA1 or SHA2.

ECDSA over prime field curves with hashing algorithm of SHA1 or SHA2 and the key sizes 192 to 512.

#### 2.3.5 Other features

##### 2.3.5.1 Automatic BAC phasing out

The TOE also supports a mechanism allowing the automatic deactivation of the BAC protocol after the current date (of the TOE) has reached a reference date - chosen by the issuer and configured by the personalization Agent. The current date is the internal date updated through the EAC protocol. Thanks to this feature, it is possible to issue MRTD supporting both PACE and BAC as needed for interoperability reasons, and perform smooth phasing out of the BAC protocol in the medium term (due

to its cryptographic weaknesses) during the life time of the issued MRTD, without having to wait for the complete renewal of issued MRTD (> 10 years).

*The automatic BAC phasing out is part of the TOE.*

### **2.3.5.2 Enhanced protection over Sensitive biometric data reading**

The access to sensitive biometric data: the fingerprint and iris stored in DG3 and DG4 are protected in accordance with the requirements of the protection profile and specification. Beyond that, the TOE also provides a feature able to ensure a high level of confidentiality when reading these data. The TOE supports a mechanism enforcing to use a minimum cryptographic strength for the confidentiality, integrity and authenticity protection of these sensitive biometric data when being read. This may be useful for issuing authority that do not consider DES algorithm strong enough to ensure a sufficient level of confidentiality. This mechanism allows the TOE to enforce the terminal using a stronger algorithm such as AES 128, or 192 bits, or 256 bits when reading the sensitive biometric data, and deny access to them if this condition is not met (algorithm not strong enough).

*The enhanced protection over sensitive biometric data reading is part of the TOE.*

## 2.3.6 TOE life cycle

### 2.3.6.1 Life cycle overview

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

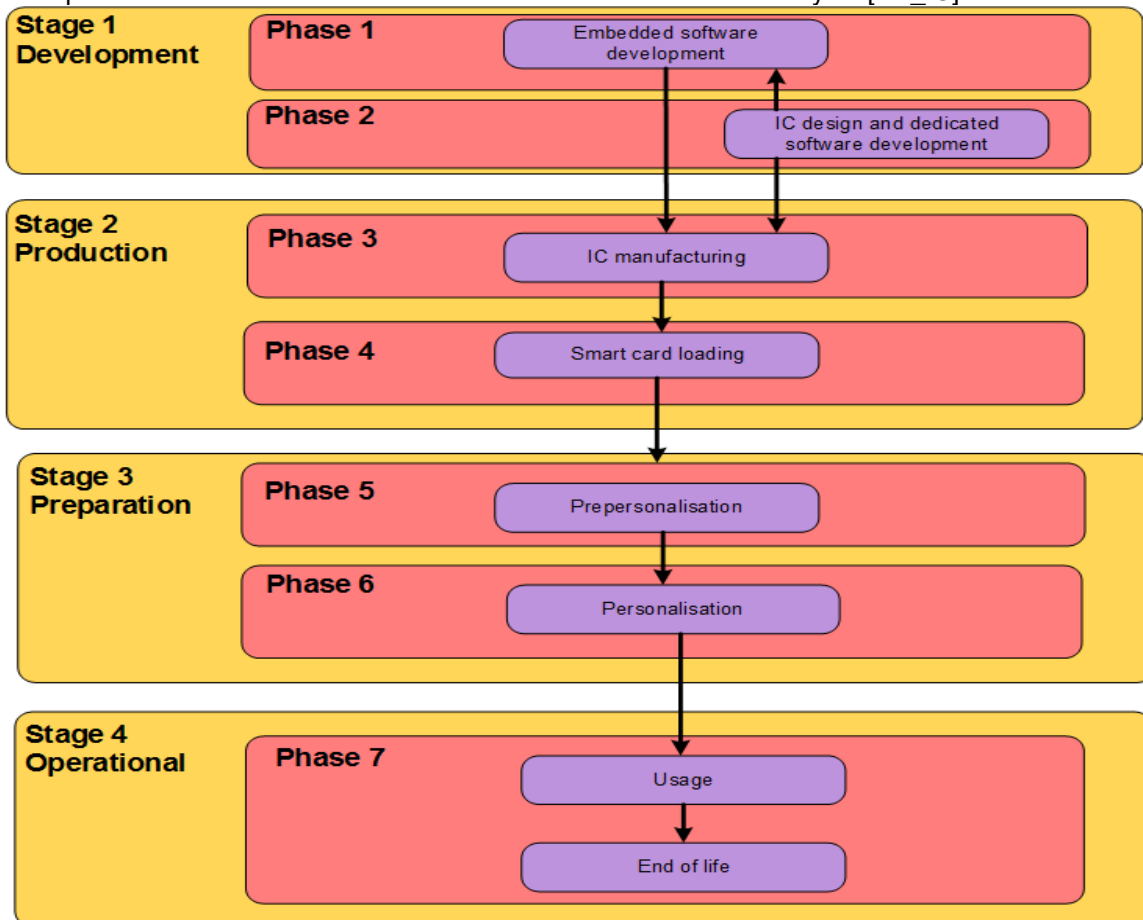
Roles		Subject
IC developer		IC Manufacturer
TOE developer		INSI
Manufacturer	IC manufacturer	IC Manufacturer
	MRTD packaging responsible	INSI or another agent
	Embedded software loading responsible	INSI
	Pre-personalization Agent (Manufacturer Role)	INSI or another agent
Personalization Agent		INSI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

**Table 4 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**

### 2.3.7 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 v2.2)
- 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 v2.2).

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 v2.2 Developer	INSI	MANILA, COURBEVOIE R&D sites	ALC
Redaction and Review of Documents	INSI		ALC
Platform Developer	IDEMIA	IDEMIA R&D sites Refer to [PTF_CERT]	ALC
IC Developer	IC Manufacturer	IC Manufacturer Refer to [PTF_CERT]	ALC

### 2.3.8 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 v2.2) 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 v2.2 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 INSI or IDEMIA audited site.

Or

- **(Option 3)** the developer sends the image (containing both the Java Card platform and the CombICAO Applet v2.2) 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	-	-	-	-
<b>TOE Delivery Point</b>				

**Table 5 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	INSI or IDEMAI	INSI or IDEMAI plant (Shenzhen, Haarlem, Vitré, Noida, Ostrava)	ALC
<b>TOE Delivery Point</b>				

**Table 6 Cap file of CombICAO Applet v2.2 is loaded (using GP) (Option 2)**

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

**Table 7 Image containing both platform and applet is loaded through the loader of the IC (Option 3)**

### 2.3.9 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 v2.2 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].

### 2.3.10 Operational Environment

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



CombICAO Applet v2.2  
in EAC with PACE configuration  
for French ID on Cosmo V9.1

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 Security Target claims conformance to [CC\_2], [CC\_3] and [CC\_EM].

The conformance to the CC is claimed as follows:

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

**Table 8 Common Criteria conformance claim**

### 3.2 Protection Profile conformance

#### 3.2.1 Overview

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

<b>Title</b>	Common Criteria Protection Profile — Machine Readable EDigitalIdentity document with “ICAO Application”, Extended Access Control with PACE (EAC PP)
<b>CC Version</b>	3.1 (Revision 3)
<b>Assurance Level</b>	The minimum assurance level for this PP is EAL4 augmented
<b>Version Number</b>	Version 1.3.2, 05 <sup>th</sup> December 2012
<b>Registration</b>	BSI-CC-PP-0056-V2-2012

**Table 9 Protection Profile conformance**

This ST also addresses the Manufacturing and Personalization phases at TOE level (cf. § 2.3.6). This ST also addresses Active Authentication as an additional authentication protocol.

Since the Chip Authentication protocol is an alternative to the Active Authentication defined in [ICO\_9303], the additional assumptions and security objectives for the operational environment counter the same threats as the ones for chip authentication. They however do not mitigate the threat, and instead provide an additional functionality to the ones defined in the PP.

The additions do not contradict any of the threats, assumptions, organisational policies, objectives or SFRs stated in the [PP\_EACwPACE] that covers the advanced security methods PACE and EAC in operational use phase.

Even though the ST claims conformance to [PP\_EACwPACE], certain terminology has been updated in the ST and Assets, Threats, Objectives and SFRs added according to the [ADDENDUM].

<b>This ST</b>	<b>[PACE/EACPP]</b>
eDigitalIdentity document	travel document
eDigitalIdentity document holder	travel document holder
eDigitalIdentity document presenter	traveler
Identification user data	user data
PACE terminal	BIS-PACE

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

### 3.2.2 Assumptions

The following Assumptions are assumed for this TOE:

- **A.Insp\_Sys** “*Inspection Systems for global interoperability*” defined in [PP\_EACwPACE],
- **A.Auth\_PKI** “*PKI for Inspection Systems*” defined in [PP\_EACwPACE],
- **A.Passive\_Auth** “*PKI for Passive Authentication*” defined in [PP\_EACwPACE],
- **A.Insp\_Sys\_AA** “*Inspection Systems with Active Authentication*” defined in this ST.

### 3.2.3 Threats

The following threats are averted by this TOE:

- **T.Read\_Sensitive\_Data** “*Read the sensitive biometric reference data*” defined in [PP\_EACwPACE],
- **T.Counterfeit** “*Counterfeit of eDigitalIdentity document chip data*” defined in [PP\_EACwPACE],
- **T.Skimming** “*Skimming eDigitalIdentity document / Capturing Card-Terminal Communication*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **T.Eavesdropping** “*Eavesdropping on the communication between the TOE and the PACE terminal*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **T.Tracing** “*Tracing eDigitalIdentity document*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **T.Forgery** “*Forgery of Data*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **T.Abuse-Func** “*Abuse of Functionality*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **T.Information\_Leakage** “*Information Leakage from eDigitalIdentity document*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **T.Phys-Tamper** “*Physical Tampering*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **T.Malfunction** “*Malfunction due to Environmental Stress*” referenced in [PP\_EACwPACE] and 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,
- **T.BAC\_breaking** “*BAC protocol is broken*” defined in this ST.

### 3.2.4 Organisational Security Policies

This TOE complies with the following OSP:

- **P.Sensitive\_Data** “Privacy of sensitive biometric reference data” defined in [PP\_EACwPACE],
- **P.Personalisation** “Personalisation of the eDigitalIdentity document by issuing State or Organisation only” defined in [PP\_EACwPACE],
- **P.Pre-Operational** “Pre-operational handling of the eDigitalIdentity document” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **P.Card\_PKI** “PKI for Passive Authentication (issuing branch)” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **P.Trustworthy\_PKI** “Trustworthiness of PKI” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **P.Manufact** “Manufacturing of the eDigitalIdentity document’s chip” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **P.Terminal** “Abilities and trustworthiness of terminals” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **P.Activ\_Auth** “Active Authentication” defined in this ST.

### 3.2.5 Security Objectives

The Security Objectives for this TOE are the following:

- **OT.Sens\_Data\_Conf** “Confidentiality of sensitive biometric reference data” defined in [PP\_EACwPACE],
- **OT.Chip\_Auth\_Proof** “Proof of the eDigitalIdentity document’s chip authenticity” defined in [PP\_EACwPACE],
- **OT.Data\_Integrity** “Integrity of Data” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.Data\_Authenticity** “Authenticity of Data” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.Data\_Confidentiality** “Confidentiality of Data” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.Tracing** “Tracing eDigitalIdentity document” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.Prot\_Abuse-Func** “Protection against Abuse of Functionality” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.Prot\_Inf\_Leak** “Protection against Information Leakage” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.Prot\_Phys-Tamper** “Protection against Physical Tampering” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.Prot\_Malfunction** “Protection against Malfunctions” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.Identification** “Identification of the TOE” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OT.AC\_Pers** “Access Control for Personalisation of logical MRTD” referenced in [PP\_EACwPACE] and 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.BAC\_Expiration** “Automatic deactivation of BAC protocol” defined in this ST,
- **OT.AC\_SM\_Level** “Access control to sensitive biometric reference data according to SM level” defined in this ST,
- **OT.AA\_Proof** “Proof of MRTD using Active Authentication” defined in this ST,
- **OT.Data\_Int\_AA** “Data Integrity using Active Authentication” defined in this ST.

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

- **OE.Auth\_Key\_Travel\_Document** “*EDigitalIdentity document Authentication Key*” defined in [PP\_EACwPACE],
- **OE.Authoriz\_Sens\_Data** “*Authorization for Use of Sensitive Biometric Reference Data*” defined in [PP\_EACwPACE],
- **OE.Exam\_Travel\_Document** “*Examination of the physical part of the eDigitalIdentity document*” defined in [PP\_EACwPACE],
- **OE.Prot\_Logical\_Travel\_Document** “*Protection of data from the logical eDigitalIdentity document*” defined in [PP\_EACwPACE],
- **OE.Ext\_Insp\_Systems** “*Authorization of Extended Inspection Systems*” defined in [PP\_EACwPACE],
- **OE.Legislative\_Compliance** “*Issuing of the eDigitalIdentity document*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OE.Passive\_Auth\_Sign** “*Authentication of eDigitalIdentity document by Signature*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OE.Personalisation** “*Personalisation of eDigitalIdentity document*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OE.Terminal** “*Terminal operating*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE]
- **OE.Travel\_Document\_Holder** “*EDigitalIdentity document holder Obligations*” referenced in [PP\_EACwPACE] and defined in [PP\_PACE],
- **OE.Exam\_MRTD\_AA** “*Examination of the MRTD using Active Authentication*” defined in this ST,
- **OE.Prot\_Logical\_MRTD\_AA** “*Protection of MRTD after Active Authentication*” defined in this ST,
- **OE.Activ\_Auth\_Verif** “*Verification using Active Authentication*” defined in this ST,
- **OE.Activ\_Auth\_Sign** “*Infrastructure for Active Authentication Key Generation*” defined in this ST.

### 3.3 CC conformance and usage in real life

In the real life, for interoperability purposes, the MRTD will most likely support BAC, PACE and EAC.

- If the terminal reads the content of the MRTD by performing BAC then EAC, the security of the MRTD will be covered by the security evaluation of (1) the TOE described by the ST claiming compliance to [PP\_BAC] and (2) the TOE described by the ST claiming compliance to [PP\_EAC], assuming PACE is not supported (as not used for the inspection procedure)
- If the terminal reads the content of the MRTD by performing PACE then EAC, the security of the MRTD will be covered by the security evaluation of the TOE described by the ST claiming compliance to [PP\_EACwPACE], assuming BAC is not supported (as not used for the inspection procedure).

## 4 Security Problem Definition

### 4.1 Assets

#### Overview

The following table presents the assets of the TOE and their corresponding phase(s) according to §1.3.6 TOE life cycle:

Asset	Step 5	Step 6	Step 7
Biometric Data	No	Yes	Yes
Personal Data	No	Yes	Yes
EF.COM	No	Yes	Yes
CA_SK	No	Yes	Yes
Session_K	Yes	Yes	Yes
PACE_Kmac	No	No	Yes
PACE_Kenc	No	No	Yes
ephem-Skpicc-PACE	No	No	Yes
PACE_PWD	No	Yes	Yes
Perso_K	No	Yes	No
LCS	Yes	Yes	Yes
Updatable data	No	Yes	Yes

Table: Assets of the TOE and their corresponding phase(s)

The assets to be protected by the TOE include the Sensitive Identification User Data on the eDigitalIdentity document's chip, Sensitive Identification user data transferred between the TOE and the terminal, and eDigitalIdentity document tracing data from the claimed [PP\_PACE], chap 3.1.

#### 4.1.1 Biometric Data

##### Biometric Data

The Biometric Data are the Logical MRTD sensitive Identification User Data: sensitive biometric reference data (EF.DG3, EF.DG4).

##### *Application Note:*

(5 in [PP\_EACwPACE]): Due to interoperability reasons the [ICAO\_9303] requires that Basic Inspection Systems may have access to logical eDigitalIdentity document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC [ICAO\_9303]. Note that the BAC mechanism cannot resist attacks with high attack potential (cf.

[PP\_BAC]). If supported, it is therefore recommended to use PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks.

#### **4.1.2 Authenticity of the MRTDs chip**

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

#### **4.1.3 User data stored on the TOE**

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

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

It includes:

##### **Personal Data**

The Personal Data are the logical MRTD standard Identification User Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16).

##### **EF.COM**

The EF.COM is an elementary file containing the list of the existing elementary files (EF) with the Identification user data.

#### **4.1.4 User data transferred between the TOE and the terminal connected**

All data (being not authentication data) being transferred in the context of the ePassport application of the MRTD as defined in [ICAO\_TR\_SAC] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO\_TR\_SAC]).

User data can be received and sent (exchange receive, send).

#### **4.1.5 MRTD tracing data**

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

#### **4.1.6 Accessibility to the 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.

#### **4.1.7 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 [PP\_BAC].

#### **4.1.8 TOE intrinsic secret cryptographic keys**

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

It includes:

##### **Chip Authentication Private Key (CA\_SK)**

The Chip Authentication Private Key is used by the application to process Chip Authentication.

##### **Secure Messaging session keys (Session\_K)**

Session keys are used to secure communication in confidentiality and authenticity.

##### **PACE session keys (PACE-Kmac, PACE-Kenc)**

PACE session keys are secure messaging keys for message authentication and for message encryption agreed between the TOE and a terminal as result of the PACE Protocol.

##### **Ephemeral private key PACE (ephem-Skpicc-PACE)**

The ephemeral PACE Authentication Key Pair is used for Key Agreement Protocol.

#### **4.1.9 MRTD communication establishment authorisation data**

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

It includes:

##### **PACE password (PACE\_PWD)**

Password needed for PACE authentication.

##### **Personalization Agent keys (Perso\_K)**

This key set used for mutual authentication between the Personalization agent and the chip, and secure communication establishment.

##### **TOE Life Cycle State (LCS)**

This is the Life Cycle State of the TOE.

## Updatable Data

Data other than Personal Data, Biometric Data, EF.COM, EF.SOD, CA\_PK, CA\_SK, Pre-Perso\_K, Perso\_K, Session\_K, LCS and Configuration Data which can be modified in Operational Use phase.

### 4.1.10 Additional Assets as per Addendum

#### 4.1.10.1 Primary Assets

#### Sensitive ID User Data

Person identification data, which have been classified as sensitive data by the eDigitalIdentity document issuer. Sensitive identification user data are a subset of all user data. Generic security property to be maintained by the current security policy: Confidentiality, Integrity, Authenticity

#### 4.1.10.2 Secondary Assets

#### eDigitalIdentity document Communication Establishment Authorization Data

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

Generic security property to be maintained by the current security policy: Confidentiality, Integrity

#### Secret eDigitalIdentity document Holder Authentication Data

Secret authentication information for the eDigitalIdentity document holder being used for verification of the authentication attempts as authorized eDigitalIdentity document holder (sent PACE passwords, e.g. PIN or PUK).

Generic security property to be maintained by the current security policy: Confidentiality, Integrity

## 4.2 Subjects

### Overview

The following table presents the assets of the TOE and their corresponding phase(s) according to §1.2.1

Subject	Step 3	Step 4	Step 5	Step 6	Step 7
MRTD Holder	No	No	No	No	Yes
eDigitalIdentity document presenter	No	No	No	No	Yes
Basic Inspection System with PACE	No	No	No	No	Yes
Document Signer	No	No	No	Yes	No
Country Signing Certification Authority	No	No	No	Yes	No

Personalization Agent	No	No	No	Yes	No
IC manufacturer (Manufacturer role)	Yes	No	No	No	No
MRTD packaging responsible (Manufacturer role)	No	Yes	No	No	No
Embedded software loading responsible (Manufacturer role)	No	Yes	No	No	No
Pre-personalization Agent (Manufacturer role)	No	No	Yes	No	No
Country Verifying Certification Authority	No	No	No	No	Yes
Document Verifier	No	No	No	No	Yes
Terminal	No	No	Yes	Yes	Yes
Inspection System	No	No	No	No	Yes
Attacker	Yes	Yes	Yes	Yes	Yes

#### 4.2.1 Subjects from PP

##### MRTD Holder

MRTD holder is the eDigitalIdentity document holder defined in [PP\_PACE]:

A person for whom the eDigitalIdentity document Issuer has personalised the eDigitalIdentity document. This entity is commensurate with 'MRTD Holder' in [PP\_BAC]. Please note that a eDigitalIdentity document holder can also be an attacker.

##### eDigitalIdentity document presenter

A person presenting the eDigitalIdentity document to a terminal and claiming the identity of the eDigitalIdentity document holder. This external entity is commensurate with 'eDigitalIdentity document presenter' in [PP\_BAC]. Please note that a eDigitalIdentity document presenter can also be an attacker.

##### Basic Inspection System with PACE (PACE terminal)

A technical system being used by an inspecting authority and verifying the eDigitalIdentity document presenter as the eDigitalIdentity document holder (for ePassport: by comparing the real biometric data (face) of the eDigitalIdentity document presenter with the stored biometric data (DG2) of the eDigitalIdentity document holder).

PACE terminal implements the terminal's part of the PACE protocol and authenticates itself to the eDigitalIdentity document using a shared password (PACE password) and supports Passive Authentication.

See also par. 1.2.5 in [PP\_PACE].

##### Document Signer (DS)

An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the eDigitalIdentity document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate, see [ICAO\_9303]. This role is usually delegated to a Personalisation Agent.

### **Country Signing Certification Authority (CSCA)**

An organisation enforcing the policy of the eDigitalIdentity document Issuer with respect to confirming correctness of user and TSF data stored in the eDigitalIdentity document. The CSCA represents the country specific root of the PKI for the eDigitalIdentity document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate having to be distributed by strictly secure diplomatic means, see [ICAO\_9303], 5.5.1.

### **Personalisation Agent**

An organisation acting on behalf of the eDigitalIdentity document Issuer to personalise the eDigitalIdentity document for the eDigitalIdentity document holder by some or all of the following activities: (i) establishing the identity of the eDigitalIdentity document holder for the biographic data in the eDigitalIdentity document, (ii) enrolling the biometric reference data of the eDigitalIdentity document holder, (iii) writing a subset of these data on the physical eDigitalIdentity document (optical personalisation) and storing them in the eDigitalIdentity document (electronic personalisation) for the eDigitalIdentity 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 eDigitalIdentity document Issuer. This entity is commensurate with 'Personalisation agent' in [PP\_BAC].

### **IC Manufacturer**

This additional subject is a refinement of the role Manufacturer as described in [PP\_PACE]. It is the manufacturer of the IC.

If scheme 1 is applied (cf. § 1.3.6), this subject is responsible for the embedded software downloading in the IC. This subject does not use Flash loader, even if it is embedded in the IC

### **MRTD packaging responsible**

This additional subject is a refinement of the role Manufacturer as described in [PP\_PACE]. This subject is responsible for the combination of the IC with hardware for the contactless and/or contact interface.

### **Embedded software loading responsible**

This additional subject is a refinement of the role Manufacturer as described in [PP\_PACE]. This subject is responsible for the embedded software loading when scheme 2 is applied (cf. § 1.3.6). This subject does not exist if scheme 1 is applied (cf. § 1.3.6). This subject used the Flash loader embedded in the IC.

### **Pre-personalization Agent**

This additional subject is a refinement of the role Manufacturer as described in [PP\_PACE]. This subject is responsible for the preparation of the card, i.e. creation of the MF and MRTD ADF. He also sets Personalization Agent keys and Configuration data.

### **Country Verifying Certification Authority (CVCA)**

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

### **Document Verifier (DV)**

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

### **Terminal**

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

Note: as the TOE may also be used in contact mode, the terminal may also communicate using the contact interface.

### **Inspection system (IS)**

A technical system used by the border control officer of the receiving State (i) examining an eDigitalIdentity document presented by the eDigitalIdentity document presenter and verifying its authenticity and (ii) verifying the eDigitalIdentity document presenter as eDigitalIdentity document holder.

The Extended Inspection System (EIS) performs the Advanced Inspection Procedure (figure1) and therefore (i) contains a terminal for the communication with the eDigitalIdentity document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical eDigitalIdentity document either under PACE or BAC by optical reading the eDigitalIdentity document providing this information, (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [TR\_03110] and (v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

### **Attacker**

Additionally to the definition from [PP\_PACE], chap 3.1 the definition of an attacker is refined as followed: A threat agent trying (i) to manipulate the logical eDigitalIdentity document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine eDigitalIdentity document, or (iv) to trace a eDigitalIdentity document.

*Application Note:*

(7 in [PP\_EACwPACE]): An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged eDigitalIdentity document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

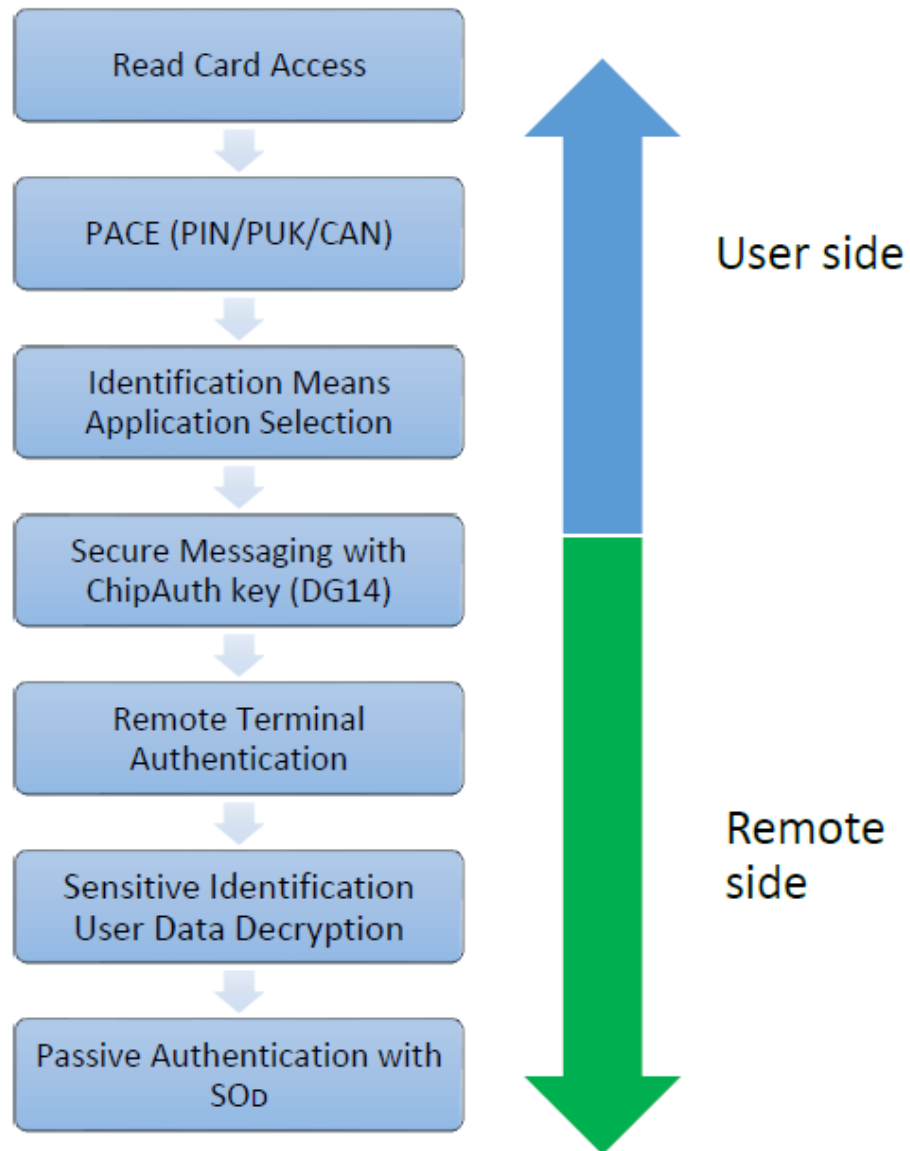
#### **4.2.2 Additional Subjects as per Addendum**

##### **PACE Terminal**

A technical system verifying correspondence between the password stored in the eDigitalIdentity document and the related value presented to the terminal by the eDigitalIdentity document presenter.

A PACE terminal performs the Remote Inspection Procedure (Figure 4) and therefore (i) contains a terminal for the communication with the eDigitalIdentity document's chip, (ii) implements the terminal part of the PACE protocol, (iii) authenticates the eDigitalIdentity holder to the eDigitalIdentity document using a shared password (PIN, PUK or CAN) and (iv) implements the Chip Authentication Protocols Version 1 according to [ICAO9303].

The remote terminal authentication, the decryption of sensitive user data and the passive authentication are performed outside of the TOE.



**Table 10 Remote Inspection Procedure**

## 4.3 Threats

### 4.3.1 Threats from PP

#### T.Read\_Sensitive\_Data

*Adverse action:* An attacker tries to gain the sensitive biometric reference data through the communication interface of the eDigitalIdentity document's chip. The attack T.Read\_Sensitive\_Data is similar to the threat T.Skimming (cf. [PP\_BAC]) in respect of the attack path (communication interface) and the motivation (to get data stored on the eDigitalIdentity document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods.

Note, that the sensitive biometric reference data are stored only on the eDigitalIdentity document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the eDigitalIdentity document as well.

*Threat agent:* having high attack potential, knowing the PACE Password, being in possession of a legitimate eDigitalIdentity document.

*Asset:* confidentiality of logical eDigitalIdentity document sensitive user data (i.e. biometric reference).

## **T.Counterfeit**

*Adverse action:* An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine eDigitalIdentity document's chip to be used as part of a counterfeit eDigitalIdentity document. This violates the authenticity of the eDigitalIdentity document's chip used for authentication of a eDigitalIdentity document presenter by possession of a eDigitalIdentity document. The attacker may generate a new data set or extract completely or partially the data from a genuine eDigitalIdentity document's chip and copy them to another appropriate chip to imitate this genuine eDigitalIdentity document's chip.

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

*Asset:* authenticity of user data stored on the TOE

## **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 eDigitalIdentity document data

*Application Note:*

Application Note (10 in [PP\_PACE]): A product using BIS-BAC cannot avert this threat in the context of the security policy defined in [PP\_PACE].

Application Note (11 in [PP\_PACE]): MRZ is printed and CAN is printed or stuck on the eDigitalIdentity document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel\_Document\_Holder.

## **T.Eavesdropping**

*Adverse action:* An attacker is listening to the communication between the eDigitalIdentity document and the PACE authenticated PACE terminal 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 eDigitalIdentity document data.

*Application Note:*

Application Note (12 in [PP\_PACE]): A product using BIS-BAC cannot avert this threat in the context of the security policy defined in [PP\_PACE]

## T.Tracing

*Adverse action:* An attacker tries to gather TOE tracing data (i.e. to trace the movement of the eDigitalIdentity 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 eDigitalIdentity document holder.

*Application Note:*

Application Note (13 in [PP\_PACE]): This Threat completely covers and extends "T.Chip-ID" from [PP\_BAC].

Application Note (14 in [PP\_PACE]): A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in [PP\_PACE], see also the par. 1.2.5 in [PP\_PACE].

Application Note (15 in [PP\_PACE]): Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the eDigitalIdentity document's chip (no Chip Authentication), a threat like T.Counterfeit (counterfeiting eDigitalIdentity document) cannot be averted by the current TOE.

Application Note: As our TOE supports Chip Authentication in addition to Standard Inspection Procedure, the previous application note extracted from PP does not apply.

## T.Forgery

*Adverse action:* An attacker fraudulently alters the User Data or/and TSF-data stored on the eDigitalIdentity document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated PACE terminal by means of changed eDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity document holder.

*Threat agent:* having high attack potential, being in possession of one or more legitimate eDigitalIdentity documents integrity and authenticity of the eDigitalIdentity document, availability of the functionality of the eDigitalIdentity document

*Asset:* integrity and authenticity of the eDigitalIdentity document, availability of the functionality of the eDigitalIdentity document.

*Application Note:*

Application Note (16 in [PP\_PACE]): Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

## **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 eDigitalIdentity 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 eDigitalIdentity document.

*Application Note:*

Application Note (17 in [PP\_PACE]): Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

## **T.Phys-Tamper**

*Adverse action:* An attacker may perform physical probing of the eDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity document.

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

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

*Application Note:*

Application Note (18 in [PP\_PACE]): Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the eDigitalIdentity document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the eDigitalIdentity document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

## T.Malfunction

*Adverse action:* An attacker may cause a malfunction the eDigitalIdentity 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 eDigitalIdentity document outside the normal operating conditions, exploiting errors in the eDigitalIdentity document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation having information about the functional operation.

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

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

*Application Note:*

Application note (19 in [PP\_PACE]): A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals

## 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 extended inspection system (EIS) 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. BAC\_breaking

*Adverse action:* An attacker manages to break the BAC protocol using cryptanalysis means and powerful computation capacity leading to threaten (1) the non traceability and (2) confidentiality of data. The attacker is able to intercept and record a log of BAC transaction during inspection at a border control. Then using computation capacity, he is able to perform reverse engineering over the logs, to break the protocol within a few minutes or less and get (1) the MRZ value, and (2) the log of plain text exchanged between the MRTD

and the inspection system. This leads the attacker to (1) get the holder information and use it, and (2) trace the holder in real time.

*Threat agent:* having high attack potential, being able to intercept transaction with MRTDs.

*Asset:* confidentiality of data read from the MRTD, traceability of the MRTD

#### **4.3.2 Additional Threats as per Addendum**

##### **T.Sentitive\_ID\_User\_Data**

*Adverse action:* An attacker tries to gain access to identification user data through the communication interface of the eDigitalIdentity document's chip. The threat T.Sentitive\_ID\_User\_Data is similar to the threat T.Skimming from [PACE/EACPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the eDigitalIdentity document's chip) but differs from those in the asset under the attack (identification user data vs. CAN, PIN, PUK and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods.

*Threat agent:* having high attack potential, knowing the PACE passwords, being in possession of one or more legitimate eDigitalIdentity document

*Asset:* confidentiality of identification user data stored on the TOE

### **4.4 Organisational Security Policies**

##### **P.Sensitive\_Data**

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the eDigitalIdentity document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the eDigitalIdentity document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The eDigitalIdentity document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

##### **P.Personalisation**

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

##### **P.Pre-Operational**

1) The eDigitalIdentity document Issuer issues the eDigitalIdentity document and approves it using the terminals complying with all applicable laws and regulations.

2) The eDigitalIdentity document Issuer guarantees correctness of the user data (amongst other of those, concerning the eDigitalIdentity document holder) and of the TSF-data permanently stored in the TOE.

3) The eDigitalIdentity document Issuer uses only such TOE's technical components (IC) which enable traceability of the eDigitalIdentity documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 in [PP\_PACE].

4) If the eDigitalIdentity document Issuer authorises a Personalisation Agent to personalise the eDigitalIdentity document for eDigitalIdentity document holders, the eDigitalIdentity document Issuer has to ensure that the Personalisation Agent acts in accordance with the eDigitalIdentity document Issuer's policy.

### **P.Card\_PKI**

1) The eDigitalIdentity document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the eDigitalIdentity document. For this aim, he runs a Country Signing Certification Authority (CSCA). The eDigitalIdentity 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 (CCSCA) having to be made available to the eDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity documents.

#### *Application Note:*

The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

### **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 eDigitalIdentity document.

### **P.Manufact**

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

### **P.Terminal**

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

1) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by eDigitalIdentity 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 order<sup>28</sup>. 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 eDigitalIdentity 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 [PP\_PACE].

### **P.Activ\_Auth**

The terminal implements the Active Authentication protocol as described in [ICAO\_9303]

## **4.5 Assumptions**

### **A.Insp\_Sys**

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [ICAO\_TR\_SAC] and/or BAC [PP\_BAC]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical eDigitalIdentity document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical eDigitalIdentity document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Justification: The assumption A.Insp\_Sys does not confine the security objectives of the [PP\_PACE] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.

### **A.Auth\_PKI**

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their eDigitalIdentity document's chip.

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [PP\_PACE] be restricted by this

assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

### **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 eDigitalIdentity 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 eDigitalIdentity 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].

### **A.Insp\_Sys\_AA**

The Inspection System implements the Active Authentication Mechanism. The Inspection System verifies the authenticity of the MRTD's chip during inspection using the signature returned by the TOE during Active Authentication.

## 5 Security Objectives

### 5.1 Security Objectives for the TOE

#### 5.1.1 Security Objectives from the PP

##### **OT.Sens\_Data\_Conf**

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organisation. The TOE must ensure the confidentiality of the logical eDigitalIdentity document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

##### **OT.Chip\_Auth\_Proof**

The TOE must support the Inspection Systems to verify the identity and authenticity of the eDigitalIdentity document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in [TR\_03110]. The authenticity proof provided by eDigitalIdentity document's chip shall be protected against attacks with high attack potential.

###### *Application Note:*

The OT.Chip\_Auth\_Proof implies the eDigitalIdentity document's chip to have (i) a unique identity as given by the eDigitalIdentity document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of eDigitalIdentity document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the eDigitalIdentity document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [6] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer

The OT.Chip\_Auth\_Proof implies the eDigitalIdentity document's chip to have (i) a unique identity as given by the eDigitalIdentity document's number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of eDigitalIdentity document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the eDigitalIdentity document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [SPECDI] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

##### **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 PACE terminal) 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 PACE terminal) 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 PACE terminal 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 PACE terminal) after the PACE Authentication.

### **OT.Tracing**

#### ***Tracing eDigitalIdentity document***

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the eDigitalIdentity 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 eDigitalIdentity document's chip (no Chip Authentication), a security objective like OT.Chip\_Auth\_Proof (proof of eDigitalIdentity document authenticity) cannot be achieved by the current TOE.

As our TOE supports Chip Authentication in addition to Standard Inspection Procedure, the previous application note extracted from PP does not apply.

### **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 eDigitalIdentity 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 eDigitalIdentity 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. The following TOE security objectives address the aspects of identified threats to be countered involving TOE's environment.

## **OT.Identification**

### ***IIentification of the TOE***

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

## **OT.AC\_Pers**

### ***Personalization of the Electronic Document***

The TOE must ensure that the logical eDigitalIdentity 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 eDigitalIdentity 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.

#### *Application Note:*

The OT.AC\_Pers implies that the data of the LDS groups written during personalisation for eDigitalIdentity document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

## **OT.Configuration**

### ***Protection of the TOE preparation***

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**

### ***Modification of file in Operational Use Phase***

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.BAC\_Expiration**

### ***Automatic deactivation of BAC protocol***

## **OT.AC\_SM\_Level**

### ***Access control to sensitive biometric reference data according to SM level***

## **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.

## **5.1.2 Additional Objectives as per Addendum**

## **OT.Sens\_Ident\_User\_Data\_Conf**

### ***Confidentiality of sensitive identification user data***

The TOE must ensure the confidentiality of sensitive identification user data by granting read access only to authorized Inspection Systems. The authorization of the inspection system is drawn by the eDigitalIdentity document holder by consciously entering his secret PIN. The identification user data may be decrypted to authorized Inspection Systems by

the eDigitalIdentity document issuer State or Organisation. The TOE must ensure the confidentiality of the identification user data during their transmission to the Inspection System. The confidentiality of the identification user data shall be protected against attacks with high attack potential.

### **5.1.3 Additional Objectives for Active Authentication**

#### **OT.AA\_Proof**

The TOE must support the Inspection Systems to verify the identity and authenticity of MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO\_9303]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

#### **OT.Data\_Int\_AA**

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

## **5.2 Security Objectives for the Operational Environment**

### **5.2.1 Issuing State or Organisation**

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

#### **OE.Auth\_Key\_Travel\_Document**

##### ***eDigitalIdentity document Authentication Key***

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the eDigitalIdentity 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 eDigitalIdentity document's chip used for genuine eDigitalIdentity document by certification of the Chip Authentication Public Key by means of the Document Security Object.

**Justification:** This security objective for the operational environment is needed additionally to those from [PP\_PACE] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in this Protection Profile and not in [PP\_PACE].

#### **OE.Authoriz\_Sens\_Data**

##### ***Authorization for Use of Sensitive Biometric Reference Data***

The issuing State or Organisation has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of eDigitalIdentity document holders to authorized receiving States or Organisations. The Country Verifying

Certification Authority of the issuing State or Organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

**Justification:** This security objective for the operational environment is needed additionally to those from [PP\_PACE] in order to handle the Threat T.Read\_Sensitive\_Data, the Organisational Security Policy P.Sensitive\_Data and the Assumption A.Auth\_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in this Protection Profile and not in [PP\_PACE].

### 5.2.2 Receiving State or Organisation

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

#### OE.Exam\_Travel\_Document

##### ***Examination of the physical part of the eDigitalIdentity document***

The inspection system of the receiving State or Organisation must examine the eDigitalIdentity document presented by the eDigitalIdentity document presenter to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the eDigitalIdentity document. The Basic Inspection System 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] and/or the Basic Access Control [ICAO\_9303]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented eDigitalIdentity document's chip.

**Justification:** This security objective for the operational environment is needed additionally to those from [PP\_PACE] in order to handle the Threat T.Counterfeit and the Assumption A.Insp\_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam\_Travel\_Document also repeats partly the requirements from OE.Terminal in [PP\_PACE] and therefore also counters T.Forgery and A.Passive\_Auth from [PP\_PACE]. This is done because a new type of Inspection System is introduced in [PP\_EACwPACE] as the Extended Inspection System is needed to handle the additional features of a eDigitalIdentity document with Extended Access Control.

#### OE.Prot\_Logical\_Travel\_Document

##### ***Protection of data from the logical eDigitalIdentity document***

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical eDigitalIdentity document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.

**Justification:** This security objective for the operational environment is needed additionally to those from [PP\_PACE] in order to handle the Assumption A.Insp\_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

## **OE.Ext\_Insp\_Systems**

### ***Authorization of Extended Inspection Systems***

The Document Verifier of receiving States or Organisations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical eDigitalIdentity document. The Extended Inspection System authenticates themselves to the eDigitalIdentity document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

**Justification:** This security objective for the operational environment is needed additionally to those from [PP\_PACE] in order to handle the Threat T.Read\_Sensitive\_Data, the Organisational Security Policy P.Sensitive\_Data and the Assumption A.Auth\_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

### **5.2.3 eDigitalIdentity document Issuer as the general responsible**

The eDigitalIdentity 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 eDigitalIdentity document***

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

### **5.2.4 eDigitalIdentity document Issuer and CVCA: eDigitalIdentity document's PKI (issuing) branch**

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

## **OE.Passive\_Auth\_Sign**

### ***Authentication of eDigitalIdentity document by Signature***

The eDigitalIdentity document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the eDigitalIdentity 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 (CCSCA). 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 eDigitalIdentity 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 eDigitalIdentity document.

## **OE.Personalisation**

### ***Personalisation of eDigitalIdentity document***

The eDigitalIdentity document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the eDigitalIdentity document holder and create the biographical data for the eDigitalIdentity document, (ii) enrol the biometric reference data of the eDigitalIdentity document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the eDigitalIdentity document (electronic personalisation) for the eDigitalIdentity 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).

### **5.2.5 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 eDigitalIdentity 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 eDigitalIdentity document (determination of the authenticity of data groups stored in the eDigitalIdentity 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 [PP\_PACE].

*Application Note:*

OE.Terminal completely covers and extends "OE.Exam\_MRTD", "OE.Passive\_Auth\_Verif" and "OE.Prot\_Logical\_MRTD" from [PP\_BAC].

### **5.2.6 eDigitalIdentity document holder Obligations**

## **OE.Travel\_Document\_Holder**

### ***eDigitalIdentity document holder Obligations***

The eDigitalIdentity 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.

## **5.2.7 Additional Security Objectives for the Operational Environment**

### **OE.Exam\_MRTD\_AA**

Additionally to the OE.Exam\_MRTD, the inspection systems perform the Active Authentication protocol to verify the Authenticity of the presented MRTD's chip.

### **OE.Prot\_Logical\_MRTD\_AA**

Additionally to the OE.Prot\_Logical\_Travel\_Document, the inspection system prevents eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Active Authentication Protocol.

### **OE.Activ\_Auth\_Verif**

In addition to the verification by passive authentication, the inspection systems may use the verification by Active Authentication, which offers a stronger guaranty of the authenticity of the MRTD.

### **OE.Activ\_Auth\_Sign**

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) ensure the secrecy of the MRTD's Active Authentication Private Key, sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

## **5.3 Security Objectives Rationale**

### **5.3.1 Threats**

#### **5.3.1.1 Threats from PP**

**T.Read\_Sensitive\_Data** The OSP P.Sensitive\_Data "Privacy of sensitive biometric reference data" is fulfilled and the threat T.Read\_Sensitive\_Data "Read the sensitive biometric reference data" is countered by the TOE-objective OT.Sens\_Data\_Conf "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by OE.Authoriz\_Sens\_Data "Authorization for Use of Sensitive Biometric Reference Data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext\_Insp\_Systems "Authorization of Extended Inspection Systems".

This threat is also covered by OT.AC\_SM\_Level "Access control to sensitive biometric reference data according to SM level" that enhances this protection by allowing the issuing State or Organization to require the usage of a secure messaging with a minimum security

level for accessing the sensitive biometric reference data. The strength of the secure messaging is tightly bound to the underlying block Cipher involved (DES, AES-128/192/256). This objective allows an issuing State or Organization to set a secure messaging level it considers as sufficient to ensure a long term confidentiality of the sensitive biometric data of its citizen when being read.

**T.Counterfeit** The threat T.Counterfeit "Counterfeit of eDigitalIdentity document chip data" addresses the attack of unauthorized copy or reproduction of the genuine eDigitalIdentity document's chip. This attack is thwarted by chip an identification and authenticity proof required by OT.Chip\_Auth\_Proof "Proof of the eDigitalIdentity document's chip authenticity" using an authentication key pair to be generated by the issuing State or Organisation. 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 "eDigitalIdentity document Authentication Key". According to OE.Exam\_Travel\_Document "Examination of the physical part of the eDigitalIdentity document" the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the eDigitalIdentity document's chip. 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.

This threat is also covered by OE.Auth\_Key\_Travel\_Document "eDigitalIdentity document Authentication Key" using a authentication key pair to be generated by the issuing State or Organization.

This attack is also thwarted by Active Authentication proving the authenticity of the chip as required by OT.AA\_Proof and OT.Data\_Int\_AA using a authentication key pair to be generated by the issuing State or Organization.

OE.Activ\_Auth\_Verif and OE.Activ\_Auth\_Sign covers also this threat enabling the possibility of performing an Active Authentication which reinforce the security associated to the communication.

**T.Skimming** The threat T.Skimming "Skimming eDigitalIdentity document / Capturing Card-Terminal Communication" 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 "Integrity of Data", OT.Data\_Authenticity "Authenticity of Data" and OT.Data\_Confidentiality "Confidentiality of Data" through the PACE authentication. The objective OE.Travel\_Document\_Holder "eDigitalIdentity document holder Obligations" ensures that a PACE session can only be established either by the eDigitalIdentity document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

Additionally, the threat is also addressed by OT.Sens\_Ident\_User\_Data\_Conf that demands a trusted channel based on Chip Authentication, and requires that read access to sensitive identification user data is only granted to authorized Inspection Systems.

**T.Eavesdropping** The threat T.Eavesdropping "Eavesdropping on the communication between the TOE and the PACE terminal" 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 "Confidentiality of Data" through a trusted channel based on the PACE authentication.

Additionally, the threat is also addressed by OT.Sens\_Ident\_User\_Data\_Conf that demands a trusted channel based on Chip Authentication.

**T.Tracing** The threat T.Tracing "Tracing eDigitalIdentity document" 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 "Tracing eDigitalIdentity document" (no gathering TOE tracing data) and OE.Travel\_Document\_Holder "eDigitalIdentity document holder Obligations" (the attacker does not a priori know the correct values of the shared passwords).

**T.Forgery** The threat T.Forgery "Forgery of Data" 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 "Access Control for Personalisation of logical MRTD" requires the TOE to limit the write access for the eDigitalIdentity 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 "Integrity of Data" and OT.Data\_Authenticity "Authenticity of Data", respectively. The objectives OT.Prot\_Phys-Tamper "Protection against Physical Tampering" and OT.Prot\_Abuse-Func "Protection against Abuse of Functionality" 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 "Terminal operating" and performing the Passive Authentication using the Document Security Object as aimed by OE.Passive\_Auth\_Sign "Authentication of eDigitalIdentity document by Signature" will be able to effectively verify integrity and authenticity of the data received from the TOE.

Additionally to the security objectives from [PP\_PACE] (see above) which counter this threat, the examination of the presented MRTD passport book according to OE.Exam\_Travel\_Document "Examination of the physical part of the eDigitalIdentity document" and OE.Exam\_MRTD\_AA shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the eDigitalIdentity document.

**T.Abuse-Func** The threat T.Abuse-Func "Abuse of Functionality" 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 "Protection against Abuse of Functionality" 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. BAC\_breaking** The threat T. BAC\_breaking "BAC protocol is broken" addresses the attack aiming at breaking the BAC protocol. The protection of the TOE against this threat is addressed by security objective OT.BAC\_Expiration "Automatic deactivation of BAC protocol" which is directly related to it. It prevents an attacker to perform offline dictionary attacks on transaction log, in order to preserve confidentiality of data and avoid citizen traceability.

### 5.3.1.2 Additional Threats as per Addendum

**T.Sentitive\_ID\_User\_Data** The threat T.Sentitive\_ID\_User\_Data is countered by the TOE-Objective OT.Sens\_Ident\_User\_Data\_Conf that requires that read access to sensitive user data is only granted to authorized Inspection Systems. Furthermore, it is required that the confidentiality of the data is ensured during transmission.

### 5.3.2 Organisational Security Policies

**P.Sensitive\_Data** The OSP P.Sensitive\_Data "Privacy of sensitive biometric reference data" is fulfilled and the threat T.Read\_Sensitive\_Data "Read the sensitive biometric reference data" is countered by the TOE-objective OT.Sens\_Data\_Conf "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's

confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by OE.Authoriz\_Sens\_Data "Authorization for Use of Sensitive Biometric Reference Data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext\_Insp\_Systems "Authorization of Extended Inspection Systems".

This threat is also covered by OT.AC\_SM\_Level "Access control to sensitive biometric reference data according to SM level" that enhances this protection by allowing the issuing State or Organization to require the usage of a secure messaging with a minimum security level for accessing the sensitive biometric reference data. The strength of the secure messaging is tightly bound to the underlying block Cipher involved (DES, AES-128/192/256). This objective allows an issuing State or Organization to set a secure messaging level it considers as sufficient to ensure a long term confidentiality of the sensitive biometric data of its citizen when being read

**P.Personalisation** The OSP P.Personalisation "Personalisation of the eDigitalIdentity document by issuing State or Organisation only" addresses the (i) the enrolment of the logical eDigitalIdentity document by the Personalisation Agent as described in the security objective for the TOE environment OE.Personalisation "Personalisation of eDigitalIdentity document", and (ii) the access control for the user data and TSF data as described by the security objective OT.AC\_Pers "Access Control for Personalisation of logical MRTD" Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to OT.Identification "Identification of the TOE". The security objective OT.AC\_Pers "Access Control for Personalisation of logical MRTD" limits the management of TSF data and the management of TSF to the Personalisation Agent.

**P.Pre-Operational** The OSP P.Pre-Operational "Pre-operational handling of the eDigitalIdentity document" is enforced by the following security objectives: OT.Identification "Identification of the TOE" is affine to the OSP's property 'traceability before the operational phase'; OT.AC\_Pers "Access Control for Personalisation of logical MRTD" and OE.Personalisation "Personalisation of eDigitalIdentity document" together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents'; OE.Legislative\_Compliance "Issuing of the eDigitalIdentity document" is affine to the OSP's property 'compliance with laws and regulations'.

**P.Card\_PKI** The OSP P.Card\_PKI "PKI for Passive Authentication (issuing branch)" is enforced by establishing the issuing PKI branch as aimed by the objectives OE.Passive\_Auth\_Sign "Authentication of eDigitalIdentity document by Signature" (for the Document Security Object).

**P.Trustworthy\_PKI** The OSP P.Trustworthy\_PKI "Trustworthiness of PKI" is enforced by OE.Passive\_Auth\_Sign "Authentication of eDigitalIdentity document by Signature" (for CSCA, issuing PKI branch).

**P.Manufact** The OSP P.Manufact "Manufacturing of the eDigitalIdentity 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 "Identification of the TOE".

**P.Terminal** The OSP P.Terminal "Abilities and trustworthiness of terminals" is obviously enforced by the objective OE.Terminal "Terminal operating", whereby the one-to-one mapping between the related properties is applicable.

The OSP P.Terminal "Abilities and trustworthiness of terminals" is countered by the security objective OE.Exam\_Travel\_Document "Examination of the physical part of the eDigitalIdentity document" additionally to the security objectives from [PP\_PACE] (see above). OE.Exam\_Travel\_Document "Examination of the physical part of the eDigitalIdentity document" enforces the terminals to perform the terminal part of the PACE protocol.

**P.Activ\_Auth** The OSP P.Activ\_Auth requires the implementation of the Active Authentication protocol as enforced by OT.AA\_Proof.

### 5.3.3 Assumptions

**A.Insp\_Sys** The examination of the eDigitalIdentity document addressed by the assumption A.Insp\_Sys "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment OE.Exam\_Travel\_Document "Examination of the physical part of the eDigitalIdentity document" which requires the inspection system to examine physically the eDigitalIdentity document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented eDigitalIdentity document's chip. The security objectives for the TOE environment OE.Prot\_Logical\_Travel\_Document "Protection of data from the logical eDigitalIdentity document" require the Inspection System to protect the logical eDigitalIdentity document data during the transmission and the internal handling.

**A.Auth\_PKI** The assumption A.Auth\_PKI "PKI for Inspection Systems" is covered by the security objective for the TOE environment OE.Authoriz\_Sens\_Data "Authorization for Use of Sensitive Biometric Reference Data" requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organisations only. The Document Verifier of the receiving State is required by OE.Ext\_Insp\_Systems "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure

**A.Passive\_Auth** The assumption A.Passive\_Auth "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment OE.Passive\_Auth\_Sign "Authentication of eDigitalIdentity document by Signature" from [PP\_PACE] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by

OE.Exam\_Travel\_Document "Examination of the physical part of the eDigitalIdentity document".

**A.Insp\_Sys\_AA** The examination of the MRTD passport book addressed by the assumption A.Insp\_Sys\_AA "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment OE.Exam\_MRTD\_AA "Examination of the MRTD passport book". The security objectives for the TOE environment OE.Prot\_Logical\_MRTD\_AA "Protection of data from the logical MRTD" will require the Basic Inspection System to implement the Active Authentication Protocol and to protect the logical MRTD data during the transmission and the internal handling.

### 5.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
<a href="#">T.Read Sensitive Data</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OE.Authoriz Sens Data</a> , <a href="#">OE.Ext Insp Systems</a> , <a href="#">OT.AC SM Level</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Counterfeit</a>	<a href="#">OT.Chip Auth Proof</a> , <a href="#">OE.Auth Key Travel Document</a> , <a href="#">OE.Exam Travel Document</a> , <a href="#">OT.Chip Auth Proof PACE CAM</a> , <a href="#">OT.AA Proof</a> , <a href="#">OT.Data Int AA</a> , <a href="#">OE.Activ Auth Verif</a> , <a href="#">OE.Activ Auth Sign</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Skimming</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OE.Travel Document Holder</a> , <a href="#">OT.Sens Ident User Data Conf</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Eavesdropping</a>	<a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Sens Ident User Data Conf</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Tracing</a>	<a href="#">OT.Tracing</a> , <a href="#">OE.Travel Document Holder</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Forgery</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Prot Abuse-Func</a> , <a href="#">OT.Prot Phys-Tamper</a> , <a href="#">OE.Personalisation</a> , <a href="#">OE.Passive Auth Sign</a> , <a href="#">OE.Terminal</a> , <a href="#">OE.Exam Travel Document</a> , <a href="#">OE.Exam MRTD AA</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Abuse-Func</a>	<a href="#">OT.Prot Abuse-Func</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Information Leakage</a>	<a href="#">OT.Prot Inf Leak</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Phys-Tamper</a>	<a href="#">OT.Prot Phys-Tamper</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Malfunction</a>	<a href="#">OT.Prot Malfunction</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Configuration</a>	<a href="#">OT.Configuration</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Forgery Supplemental Data</a>	<a href="#">OT.Update File</a>	<a href="#">Section 5.3.1</a>

<a href="#">T. BAC breaking</a>	<a href="#">OT.BAC Expiration</a>	<a href="#">Section 5.3.1</a>
<a href="#">T.Sentitive ID User Data</a>	<a href="#">OT.Sens Ident User Data Conf</a>	<a href="#">Section 5.3.1</a>

**Table 11 Threats and Security Objectives - Coverage**

Security Objectives	Threats
<a href="#">OT.Sens Data Conf</a>	<a href="#">T.Read Sensitive Data</a>
<a href="#">OT.Chip Auth Proof</a>	<a href="#">T.Counterfeit</a>
<a href="#">OT.Data Integrity</a>	<a href="#">T.Skimming, T.Forgery</a>
<a href="#">OT.Data Authenticity</a>	<a href="#">T.Skimming, T.Forgery</a>
<a href="#">OT.Data Confidentiality</a>	<a href="#">T.Skimming, T.Eavesdropping</a>
<a href="#">OT.Tracing</a>	<a href="#">T.Tracing</a>
<a href="#">OT.Prot Abuse-Func</a>	<a href="#">T.Forgery, T.Abuse-Func</a>
<a href="#">OT.Prot Inf Leak</a>	<a href="#">T.Information Leakage</a>
<a href="#">OT.Prot Phys-Tamper</a>	<a href="#">T.Forgery, T.Phys-Tamper</a>
<a href="#">OT.Prot Malfunction</a>	<a href="#">T.Malfunction</a>
<a href="#">OT.Identification</a>	
<a href="#">OT.AC Pers</a>	<a href="#">T.Forgery</a>
<a href="#">OT.Configuration</a>	<a href="#">T.Configuration</a>
<a href="#">OT.Update File</a>	<a href="#">T. Forgery Supplemental Data</a>
<a href="#">OT.BAC Expiration</a>	<a href="#">T. BAC breaking</a>
<a href="#">OT.AC SM Level</a>	<a href="#">T.Read Sensitive Data</a>
<a href="#">OT.Chip Auth Proof PACE CAM</a>	<a href="#">T.Counterfeit</a>
<a href="#">OT.Sens Ident User Data Conf</a>	<a href="#">T.Skimming, T.Eavesdropping, T.Sentitive ID User Data</a>
<a href="#">OT.AA Proof</a>	<a href="#">T.Counterfeit</a>
<a href="#">OT.Data Int AA</a>	<a href="#">T.Counterfeit</a>
<a href="#">OE.Auth Key Travel Document</a>	<a href="#">T.Counterfeit</a>
<a href="#">OE.Authoriz Sens Data</a>	<a href="#">T.Read Sensitive Data</a>
<a href="#">OE.Exam Travel Document</a>	<a href="#">T.Counterfeit, T.Forgery</a>
<a href="#">OE.Prot Logical Travel Document</a>	
<a href="#">OE.Ext Insp Systems</a>	<a href="#">T.Read Sensitive Data</a>
<a href="#">OE.Legislative Compliance</a>	
<a href="#">OE.Passive Auth Sign</a>	<a href="#">T.Forgery</a>

<a href="#">OE.Personalisation</a>	<a href="#">T.Forgery</a>
<a href="#">OE.Terminal</a>	<a href="#">T.Forgery</a>
<a href="#">OE.Travel Document Holder</a>	<a href="#">T.Skimming, T.Tracing</a>
<a href="#">OE.Exam MRTD AA</a>	<a href="#">T.Forgery</a>
<a href="#">OE.Prot Logical MRTD AA</a>	
<a href="#">OE.Activ Auth Verif</a>	<a href="#">T.Counterfeit</a>
<a href="#">OE.Activ Auth Sign</a>	<a href="#">T.Counterfeit</a>

**Table 12 Security Objectives and Threats - Coverage**

Organisational Security Policies	Security Objectives	Rationale
<a href="#">P.Sensitive Data</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OE.Authoriz Sens Data</a> , <a href="#">OE.Ext Insp Systems</a> , <a href="#">OT.AC SM Level</a>	<a href="#">Section 5.3.2</a>
<a href="#">P.Personalisation</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Identification</a> , <a href="#">OE.Personalisation</a>	<a href="#">Section 5.3.2</a>
<a href="#">P.Pre-Operational</a>	<a href="#">OT.Identification</a> , <a href="#">OT.AC Pers</a> , <a href="#">OE.Personalisation</a> , <a href="#">OE.Legislative Compliance</a>	<a href="#">Section 5.3.2</a>
<a href="#">P.Card PKI</a>	<a href="#">OE.Passive Auth Sign</a>	<a href="#">Section 5.3.2</a>
<a href="#">P.Trustworthy PKI</a>	<a href="#">OE.Passive Auth Sign</a>	<a href="#">Section 5.3.2</a>
<a href="#">P.Manufact</a>	<a href="#">OT.Identification</a>	<a href="#">Section 5.3.2</a>
<a href="#">P.Terminal</a>	<a href="#">OE.Terminal</a> , <a href="#">OE.Exam Travel Document</a>	<a href="#">Section 5.3.2</a>
<a href="#">P.Activ Auth</a>	<a href="#">OT.AA Proof</a>	<a href="#">Section 5.3.2</a>

**Table 13 OSPs and Security Objectives - Coverage**

Security Objectives	Organisational Security Policies
<a href="#">OT.Sens Data Conf</a>	<a href="#">P.Sensitive Data</a>
<a href="#">OT.Chip Auth Proof</a>	
<a href="#">OT.Data Integrity</a>	
<a href="#">OT.Data Authenticity</a>	
<a href="#">OT.Data Confidentiality</a>	
<a href="#">OT.Tracing</a>	
<a href="#">OT.Prot Abuse-Func</a>	
<a href="#">OT.Prot Inf Leak</a>	
<a href="#">OT.Prot Phys-Tamper</a>	
<a href="#">OT.Prot Malfunction</a>	

<a href="#">OT.Identification</a>	<a href="#">P.Personalisation</a> , <a href="#">P.Pre-Operational</a> , <a href="#">P.Manufact</a>
<a href="#">OT.AC Pers</a>	<a href="#">P.Personalisation</a> , <a href="#">P.Pre-Operational</a>
<a href="#">OT.Configuration</a>	
<a href="#">OT.Update File</a>	
<a href="#">OT.BAC Expiration</a>	
<a href="#">OT.AC SM Level</a>	<a href="#">P.Sensitive Data</a>
<a href="#">OT.Chip Auth Proof PACE CAM</a>	
<a href="#">OT.Sens Ident User Data Conf</a>	
<a href="#">OT.AA Proof</a>	<a href="#">P.Activ Auth</a>
<a href="#">OT.Data Int AA</a>	
<a href="#">OE.Auth Key Travel Document</a>	
<a href="#">OE.Authoriz Sens Data</a>	<a href="#">P.Sensitive Data</a>
<a href="#">OE.Exam Travel Document</a>	<a href="#">P.Terminal</a>
<a href="#">OE.Prot Logical Travel Document</a>	
<a href="#">OE.Ext Insp Systems</a>	<a href="#">P.Sensitive Data</a>
<a href="#">OE.Legislative Compliance</a>	<a href="#">P.Pre-Operational</a>
<a href="#">OE.Passive Auth Sign</a>	<a href="#">P.Card PKI</a> , <a href="#">P.Trustworthy PKI</a>
<a href="#">OE.Personalisation</a>	<a href="#">P.Personalisation</a> , <a href="#">P.Pre-Operational</a>
<a href="#">OE.Terminal</a>	<a href="#">P.Terminal</a>
<a href="#">OE.Travel Document Holder</a>	
<a href="#">OE.Exam MRTD AA</a>	
<a href="#">OE.Prot Logical MRTD AA</a>	
<a href="#">OE.Activ Auth Verif</a>	
<a href="#">OE.Activ Auth Sign</a>	

**Table 14 Security Objectives and OSPs - Coverage**

Assumptions	Security Objectives for the Operational Environment	Rationale
<a href="#">A.Insp Sys</a>	<a href="#">OE.Exam Travel Document</a> , <a href="#">OE.Prot Logical Travel Document</a>	<a href="#">Section 5.3.3</a>
<a href="#">A.Auth PKI</a>	<a href="#">OE.Authoriz Sens Data</a> , <a href="#">OE.Ext Insp Systems</a>	<a href="#">Section 5.3.3</a>
<a href="#">A.Passive Auth</a>	<a href="#">OE.Passive Auth Sign</a> , <a href="#">OE.Exam Travel Document</a>	<a href="#">Section 5.3.3</a>
<a href="#">A.Insp Sys AA</a>	<a href="#">OE.Exam MRTD AA</a> , <a href="#">OE.Prot Logical MRTD AA</a>	<a href="#">Section 5.3.3</a>

**Table 15 Assumptions and Security Objectives for the Operational Environment - Coverage**

Security Objectives for the Operational Environment	Assumptions
<a href="#">OE.Auth Key Travel Document</a>	
<a href="#">OE.Authoriz Sens Data</a>	<a href="#">A.Auth PKI</a>
<a href="#">OE.Exam Travel Document</a>	<a href="#">A.Insp Sys,</a> <a href="#">A.Passive Auth</a>
<a href="#">OE.Prot Logical Travel Document</a>	<a href="#">A.Insp Sys</a>
<a href="#">OE.Ext Insp Systems</a>	<a href="#">A.Auth PKI</a>
<a href="#">OE.Legislative Compliance</a>	
<a href="#">OE.Passive Auth Sign</a>	<a href="#">A.Passive Auth</a>
<a href="#">OE.Personalisation</a>	
<a href="#">OE.Terminal</a>	
<a href="#">OE.Travel Document Holder</a>	
<a href="#">OE.Exam MRTD AA</a>	<a href="#">A.Insp Sys AA</a>
<a href="#">OE.Prot Logical MRTD AA</a>	<a href="#">A.Insp Sys AA</a>
<a href="#">OE.Activ Auth Verif</a>	
<a href="#">OE.Activ Auth Sign</a>	

**Table 16 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].

**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].

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: (FMT\_LIM.2)

#### 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: (FMT\_LIM.1)

### 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 [TR\_03111]** and specified cryptographic key sizes **192 to 512 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/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/SIG\_VER Cryptographic operation

**FCS\_COP.1.1/SIG\_VER** 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
-------------------------	-----------	-----------

digital signature verification	ECDSA with SHA-1, SHA-224 and SHA-256 as defined in [FIPS_186_3]	192 to 512
digital signature verification	RSA PKCS#1 v1.5 with SHA-1, SHA-256 and SHA-512	1024, 1536, 2048
digital signature verification	RSA PKCS#1-PSS with SHA-1, SHA-256 and SHA-512	1024, 1536, 2048

### 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/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/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\_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 Sizes	Standard
secure messaging – message authentication code	Retail MAC	112 bit	[ISO_9797_1]
secure messaging – message authentication code	AES CMAC	128, 198 and 256 bits	[NIST_800_38B]

**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]

*Application Note:*

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

**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\_COP.1/AA Cryptographic operation

**FCS\_COP.1.1/AA** The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standard]**

Cryptographic Operation	Cryptographic Algorithm	Cryptographic Key Sizes(bits)	Standard
Digital Signature Creation	ECDSA with SHA1, 256, 384, 512	192 to 512 over prime field curves	[ISO_9796-2], [PKCS#3], [FIPS_180_2] and [X.92]
Digital Signature Creation	RSA signature (CRT) with SHA1, 256, 384, 512	1024, 1536 and 2048	[ISO_9796-2]

### 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 0.994.**

#### 7.1.2 Class FIA Identification and Authentication

### 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 Mapping (PACE-CAM) according to [ICAO\_9303]**

- o **To carry out the Chip Authentication Protocol v.1 according to [TR\_03110]**
- o **To carry out the Terminal Authentication Protocol according to [TR\_03110]**

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 disabled 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 Terminal Authentication Protocol according to [TR\_03110]**
- 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 and AES**
- o **Terminal Authentication Protocol v.1 according to [TR\_03110].**

*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 according to [ICAO\_TR\_SAC] and PACE-CAM Protocol according to [ICAO\_9303],**
- 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 and AES**
- o **Terminal Authentication Protocol v.1 according to [TR\_03110]**

to support user authentication.

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

- o **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.**
- o **The TOE accepts the authentication attempt as Personalisation Agent by the Authentication Mechanism with Personalization Agent Key(s).**
- o **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.**
- o **The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Mechanism v.1 or the terminal uses the public key presented during PACE-CAM and the secure messaging established during PACE.**
- o **The TOE accepts the authentication attempt as Personalisation Agent by the Authentication Mechanism with Personalization Agent Key(s).**

**FIA\_UAU.6/EAC Re-authenticating**

**FIA\_UAU.6.1/EAC** The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System.**

**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/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\_AFL.1/PACE Authentication failure handling**

**FIA\_AFL.1.1/PACE** The TSF shall detect when **[Number]** unsuccessful authentication attempts occur related to **[Authentication events]**.

**FIA\_AFL.1.2/PACE** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **[Actions]**

Password	Number	Authentication events	Actions
CAN, MRZ	Positive integer number set to 0x0A	Authentication attempt involving CAN, MRZ as shared password for PACE	Wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the PACE authentication attempts
PIN & PUK	An administrator configurable positive integer linked to the PIN or PUK (respectively)	Consecutive failed authentication attempts using the PIN or PUK as the shared password for PACE leaving a single authentication attempt	Suspend the PIN or the PUK
PIN & PUK	'1'	On suspend mode, a bad or incorrect value presentation attempts using the PIN or PUK as the shared password for PACE	Suspend the PIN or the PUK
PIN & PUK	'1'	On suspend mode, After a PACE_CAN authentication,	Block the PIN or the PUK

		a bad PIN/PUK value presentation attempt.	
--	--	--	--

#### **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\_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 eDigitalIdentity document**.

#### **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,**
  - **PACE terminal,**

- **Extended Inspection System**
- **Objects:**
  - **data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16,EF.SOD and EF.COM of the logical eDigitalIdentity document,**
  - **data in EF.DG3 of the logical eDigitalIdentity document,**
  - **data in EF.DG4 of the logical eDigitalIdentity document,**
  - **all TOE intrinsic secret cryptographic keys stored in the eDigitalIdentity document**
- **Security attributes:**
  - **PACE Authentication**
  - **Terminal Authentication v.1**
  - **Authorisation of the Terminal**
  - **Chip Authentication v.1.**

**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 PACE terminal is allowed to read data objects from FDP\_ACF.1/TRM according to [ICAO\_TR\_SAC] after at least a successful PACE authentication as required by FIA\_UAU.1/PACE**
- **A PACE Terminal is allowed to read data objects 2a) of FDP\_ACF.1.1/TRM according to [SPECDI] only after a successful PACE authentication followed by Chip Authentication v1 as required by FIA\_UAU.1/PACE. This rule is not applicable for EF.DG14.**
- **A PACE Terminal is allowed to read data objects 2b) and 2c) of FDP\_ACF.1.1/TRM according to [SPECDI] only after a successful PACE authentication followed by Chip Authentication v1 and Terminal Authentication v.1 as required by FIA\_UAU.1/PACE.**

*Refinement:*

The TOE can be configured to restrict access to data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16,EF.SOD and EF.COM of the logical eDigitalIdentity document to a successful PACE Authentication followed by a successful Chip Authentication.

**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:

- **Any terminal being not authenticated at least as PACE authenticated PACE terminal is not allowed to read, to write, to modify, to use any User Data stored on the eDigitalIdentity document.**
- **Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the eDigitalIdentity document.**
- **Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 granted by the relative**

**certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP\_ACF.1.1/TRM.**

- **Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP\_ACF.1.1/TRM.**
- **Nobody is allowed to read the data objects 2d) of FDP\_ACF.1.1/TRM.**
- **Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.**
- **Moreover, the Extended Inspection System shall communicate with at least the minimum secure messaging level identified at the creation of the DG3 and DG4, to be able to read these DGs.**

#### **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:

- **Subjects:**
  - **Personalization Agent,**
  - **Extended Inspection System**
  - **Terminal,**
- **Objects:**
  - **data in the file(s) EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**
- **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:

- **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,**
- **the successfully authenticated Extended Inspection System following FMT\_MTD.1.1/UPD\_FILE is allowed to 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\_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 **PIN and PUK.**

#### **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\_DAU.1/AA Basic Data Authentication**

**FDP\_DAU.1.1/AA** The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the TOE itself**.

**FDP\_DAU.1.2/AA** The TSF shall provide **any users** with the ability to verify evidence of the validity of the indicated information.

### **FDP\_ITC.1/AA Import of user data without security attributes**

**FDP\_ITC.1.1/AA** The TSF shall enforce the **Active Authentication Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

**FDP\_ITC.1.2/AA** The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

**FDP\_ITC.1.3/AA** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **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\_MOF.1/BAC\_EXP Management of security functions behaviour

**FMT\_MOF.1.1/BAC\_EXP** The TSF shall restrict the ability to **enable** the functions

- o **deactivation of BAC protocol**

to **Country Verifying Certification Authority and Domestic Document Verifier once the current date in the TOE has reached or passed the value set by FMT\_MTD.1/BAC\_EXP.**

*Application Note:*

The BAC is automatically deactivated by the TOE once the authenticated subject (CVCA or Domestic Document Verifier) has updated the current date of the TOE with a date that reaches or passes the reference date configured by FMT\_MTD.1/BAC\_EXP

## FMT\_MOF.1/GP Management of security functions behaviour

**FMT\_MOF.1.1/GP** The TSF shall restrict the ability to **enable** the functions

- o **transmission of user data in a manner protected from unauthorized disclosure,**
- o **reception of user data in a manner protected from unauthorized disclosure,**
- o **transmission of user data in a manner protected from modification, deletion, insertion and replay errors,**
- o **reception of user data in a manner protected from modification, deletion, insertion and replay errors,**

to **the manufacturer and personalization agent.**

## FMT\_MOF.1/AA Management of security functions behaviour

**FMT\_MOF.1.1/AA** The TSF shall restrict the ability to **enable and disable** the functions **TSF Active Authentication to Personalization Agent.**

## FMT\_SMF.1 Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions:

- **Initialization,**
- **Pre-personalisation,**
- **Personalisation,**
- **Configuration,**
- **Chip Authentication Protocol,**
- **Protection of incoming user data,**
- **Protection of outgoing user data,**
- **Basic Access Control expiration**
- **Initialize, and resume the PIN or the PUK**
- **Change and unblock the PIN.**

## FMT\_SMR.1/PACE Security roles

**FMT\_SMR.1.1/PACE** The TSF shall maintain the roles

- **Manufacturer,**
- **Personalization Agent,**
- **Terminal,**
- **PACE authenticated PACE terminal**
- **Country Verifying Certificate Authority,**
- **Document Verifier,**
- **Domestic Extended Inspection System,**
- **Foreign Extended Inspection System,**
- **Administrator,**
- **Signatory.**

**FMT\_SMR.1.2/PACE** The TSF shall be able to associate users with roles.

*Application Note:*

This SFR also applies to the refinement of the role Manufacturer.

## 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/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/CVCA\_INI Management of TSF data

**FMT\_MTD.1.1/CVCA\_INI** The TSF shall restrict the ability to **write** the

- o **initial Country Verifying Certification Authority Public Key,**
- o **initial Country Verifying Certification Authority Certificate,**
- o **Initial Current Date**
- o **none**

to **the Personalization Agent**.

#### FMT\_MTD.1/CVCA\_UPD Management of TSF data

**FMT\_MTD.1.1/CVCA\_UPD** The TSF shall restrict the ability to **update** the

- o **Country Verifying Certification Authority Public Key,**
- o **Country Verifying Certification Authority Certificate**

to **Country Verifying Certification Authority**.

#### FMT\_MTD.1/DATE Management of TSF data

**FMT\_MTD.1.1/DATE** The TSF shall restrict the ability to **modify** the **Current Date** to

- o **Country Verifying Certification Authority**
- o **Document Verifier**
- o **Domestic Extended Inspection System.**

**FMT\_MTD.1/CAPK Management of TSF data**

**FMT\_MTD.1.1/CAPK** The TSF shall restrict the ability to **[Operation]** the **[TSF Data]** to **[Role]**

Operation	TSF Date	Role
load or create	Chip Authentication private key	the personalization agent (in phase 6)
create	Chip Authentication private key	admin or admin + signatory (in phase 7)

**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 **Chip Authentication Private Key**

to **none**.

**FMT\_MTD.1/PACE\_PWD Management of TSF data**

**FMT\_MTD.1.1/PACE\_PWD** The TSF shall restrict the ability to **load** the **PACE Password** to **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**.

**FMT\_MTD.1/BAC\_EXP Management of TSF data**

**FMT\_MTD.1.1/BAC\_EXP** The TSF shall restrict the ability to **set** the **BAC expiry date** to **Personalization Agent**.

*Application Note:*

By default, BAC expiration feature is not activated

### 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/SM\_LVL Management of TSF data

**FMT\_MTD.1.1/SM\_LVL** The TSF shall restrict the ability to **set** the **minimum Secure Messaging level required to access DG3 and DG4** to **Personalization Agent**.

*Application Note:*

Possible secure messaging levels are: DES, AES 128, AES 192 or AES 256

### FMT\_MTD.1/AA\_KEY\_READ Management of TSF data

**FMT\_MTD.1.1/AA\_KEY\_READ** The TSF shall restrict the ability to **read** the **AAK** to **none**.

### FMT\_MTD.1/AA\_KEY\_WRITE Management of TSF data

**FMT\_MTD.1.1/AA\_KEY\_WRITE** The TSF shall restrict the ability to **write** the **AAK** to **Personalization Agent**.

### FMT\_MTD.3 Secure TSF data

**FMT\_MTD.3.1 [Editorially Refined]** The TSF shall ensure that only secure values of the certificate chain are accepted for **TSF data of the Terminal Authentication Protocol v.1 and the Access Control**.

*Refinement:*

The certificate chain is valid if and only if

- the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,
- the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country Verifying Certification Authority is not

before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

- the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

### **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**

- **User Data to be manipulated and disclosed,**
- **TSF data to be manipulated or disclosed,**
- **software to be reconstructed,**
- **substantial information about construction of TSF to be gathered which may enable other attacks,**
- **sensitive User Data(EF.DG3 and EF.DG4) to be disclosed**

### **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**

- **User Data to be manipulated and disclosed,**
- **TSF data to be manipulated or disclosed,**
- **software to be reconstructed,**
- **substantial information about construction of TSF to be gathered which may enable other attacks,**
- **sensitive User Data(EF.DG3 and EF.DG4) to be disclosed**

#### **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 **Chip Authentication Session Keys,**
- o **PACE session keys (PACE-K mac, PACE-K enc),**
- o **The ephemeral private key ephem SK picc -PACE,**
- o **The ephemeral private key SK Map,PICC -PACE-CAM,**
- o **Personalization Agent Key(s),**
- o **Chip Authentication Private Key,**
- o **Active Authentication Private Key(AAK).**

**FPT\_EMS.1.2** The TSF shall ensure **users** are unable to use the following interface **smart card circuit contacts** to gain access to

- o **Chip Authentication Session Keys,**
- 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 **Active Authentication Private Key(AAK).**

**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**.

#### **7.1.8 Additional SFRs as per Addendum**

##### **FIA\_API.1/TOE Authentication Proof of Identity**

**FIA\_API.1.1/TOE** The TSF shall provide a **an authentication mechanism** to prove the identity of the **the eDigitalIdentity document holder**.

*Application Note:*

The TOE acts as a substitute for the eDigitalIdentity document holder, to authenticate digitally on its behalf. The authentication mechanism is triggered by the eDigitalIdentity Document holder itself by presenting its PIN to the TOE.

##### **FMT\_MTD.1/Initialize\_PIN Management of TSF data**

**FMT\_MTD.1.1/Initialize\_PIN** The TSF shall restrict the ability to **write** the **PIN and PUK** to **the Personalization Agent**.

##### **FMT\_MTD.1/Resume\_PIN Management of TSF data**

**FMT\_MTD.1.1/Resume\_PIN** The TSF shall restrict the ability to **resume** the **suspended PIN or the PUK** to **the eDigitalIdentity document holder**.

##### **FMT\_MTD.1/Change\_PIN Management of TSF data**

**FMT\_MTD.1.1/Change\_PIN** The TSF shall restrict the ability to **change** the **PIN** to **eDigitalIdentity document holder**.

<b>FMT_MTD.1/Unblock_PIN Management of TSF data</b>
---

**FMT\_MTD.1.1/Unblock\_PIN** The TSF shall restrict the ability to **unblock** the **blocked PIN** to the **eDigitalIdentity document holder (using the PUK for unblocking)**.

## **7.2 Security Assurance Requirements**

The Evaluation Assurance Level is EAL5 augmented with AVA\_VAN.5 and ALC\_DVS.2.

### **7.2.1 ADV Development**

#### **7.2.1.1 ADV\_ARC Security Architecture**

## **ADV\_ARC.1 Security architecture description**

**ADV\_ARC.1.1D** The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

**ADV\_ARC.1.2D** The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

**ADV\_ARC.1.3D** The developer shall provide a security architecture description of the TSF.

**ADV\_ARC.1.1C** The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

**ADV\_ARC.1.2C** The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

**ADV\_ARC.1.3C** The security architecture description shall describe how the TSF initialisation process is secure.

**ADV\_ARC.1.4C** The security architecture description shall demonstrate that the TSF protects itself from tampering.

**ADV\_ARC.1.5C** The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

**ADV\_ARC.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.1.2 ADV\_FSP Functional specification**

<b>ADV_FSP.5 Complete semi-formal functional specification with additional error information</b>
--

**ADV\_FSP.5.1D** The developer shall provide a functional specification.

**ADV\_FSP.5.2D** The developer shall provide a tracing from the functional specification to the SFRs.

**ADV\_FSP.5.1C** The functional specification shall completely represent the TSF.

**ADV\_FSP.5.2C** The functional specification shall describe the TSFI using a semi-formal style.

**ADV\_FSP.5.3C** The functional specification shall describe the purpose and method of use for all TSFI.

**ADV\_FSP.5.4C** The functional specification shall identify and describe all parameters associated with each TSFI.

**ADV\_FSP.5.5C** The functional specification shall describe all actions associated with each TSFI.

**ADV\_FSP.5.6C** The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

**ADV\_FSP.5.7C** The functional specification shall describe all error messages that do not result from an invocation of a TSFI.

**ADV\_FSP.5.8C** The functional specification shall provide a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.

**ADV\_FSP.5.9C** The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

**ADV\_FSP.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV\_FSP.5.2E** The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

### 7.2.1.3 ADV\_IMP Implementation representation

## **ADV\_IMP.1 Implementation representation of the TSF**

**ADV\_IMP.1.1D** The developer shall make available the implementation representation for the entire TSF.

**ADV\_IMP.1.2D** The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

**ADV\_IMP.1.1C** The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

**ADV\_IMP.1.2C** The implementation representation shall be in the form used by the development personnel.

**ADV\_IMP.1.3C** The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

**ADV\_IMP.1.1E** The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

### **7.2.1.4 ADV\_TDS TOE design**

## **ADV\_TDS.4 Semiformal modular design**

**ADV\_TDS.4.1D** The developer shall provide the design of the TOE.

**ADV\_TDS.4.2D** The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

**ADV\_TDS.4.1C** The design shall describe the structure of the TOE in terms of subsystems.

**ADV\_TDS.4.2C** The design shall describe the TSF in terms of modules, designating each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering.

**ADV\_TDS.4.3C** The design shall identify all subsystems of the TSF.

**ADV\_TDS.4.4C** The design shall provide a semiformal description of each subsystem of the TSF, supported by informal, explanatory text where appropriate.

**ADV\_TDS.4.5C** The design shall provide a description of the interactions among all subsystems of the TSF.

**ADV\_TDS.4.6C** The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

**ADV\_TDS.4.7C** The design shall describe each SFR-enforcing and SFR-supporting module in terms of its purpose and relationship with other modules.

**ADV\_TDS.4.8C** The design shall describe each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with

other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.

**ADV\_TDS.4.9C** The design shall describe each SFR-non-interfering module in terms of its purpose and interaction with other modules.

**ADV\_TDS.4.10C** The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

**ADV\_TDS.4.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV\_TDS.4.2E** The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

#### 7.2.1.5 ADV\_INT TSF internals

### **ADV\_INT.2 Well-structured internals**

**ADV\_INT.2.1D** The developer shall design and implement the entire TSF such that it has well-structured internals.

**ADV\_INT.2.2D** The developer shall provide an internals description and justification.

**ADV\_INT.2.1C** The justification shall describe the characteristics used to judge the meaning of "well-structured".

**ADV\_INT.2.2C** The TSF internals description shall demonstrate that the entire TSF is well-structured.

**ADV\_INT.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV\_INT.2.2E** The evaluator shall perform an internals analysis on the TSF.

## 7.2.2 AGD Guidance documents

### 7.2.2.1 AGD\_OPE Operational user guidance

## **AGD\_OPE.1 Operational user guidance**

**AGD\_OPE.1.1D** The developer shall provide operational user guidance.

**AGD\_OPE.1.1C** The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

**AGD\_OPE.1.2C** The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

**AGD\_OPE.1.3C** The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

**AGD\_OPE.1.4C** The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

**AGD\_OPE.1.5C** The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

**AGD\_OPE.1.6C** The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

**AGD\_OPE.1.7C** The operational user guidance shall be clear and reasonable.

**AGD\_OPE.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.2.2 AGD\_PRE Preparative procedures**

## **AGD\_PRE.1 Preparative procedures**

**AGD\_PRE.1.1D** The developer shall provide the TOE including its preparative procedures.

**AGD\_PRE.1.1C** The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

**AGD\_PRE.1.2C** The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

**AGD\_PRE.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AGD\_PRE.1.2E** The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

### **7.2.3 ALC Life-cycle support**

#### **7.2.3.1 ALC\_CMC CM capabilities**

## **ALC\_CMC.4 Production support, acceptance procedures and automation**

**ALC\_CMC.4.1D** The developer shall provide the TOE and a reference for the TOE.

**ALC\_CMC.4.2D** The developer shall provide the CM documentation.

**ALC\_CMC.4.3D** The developer shall use a CM system.

**ALC\_CMC.4.1C** The TOE shall be labelled with its unique reference.

**ALC\_CMC.4.2C** The CM documentation shall describe the method used to uniquely identify the configuration items.

**ALC\_CMC.4.3C** The CM system shall uniquely identify all configuration items.

**ALC\_CMC.4.4C** The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

**ALC\_CMC.4.5C** The CM system shall support the production of the TOE by automated means.

**ALC\_CMC.4.6C** The CM documentation shall include a CM plan.

**ALC\_CMC.4.7C** The CM plan shall describe how the CM system is used for the development of the TOE.

**ALC\_CMC.4.8C** The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

**ALC\_CMC.4.9C** The evidence shall demonstrate that all configuration items are being maintained under the CM system.

**ALC\_CMC.4.10C** The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

**ALC\_CMC.4.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.3.2 ALC\_CMS CM scope**

### **ALC\_CMS.5 Development tools CM coverage**

**ALC\_CMS.5.1D** The developer shall provide a configuration list for the TOE.

**ALC\_CMS.5.1C** The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

**ALC\_CMS.5.2C** The configuration list shall uniquely identify the configuration items.

**ALC\_CMS.5.3C** For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

**ALC\_CMS.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### **7.2.3.3 ALC\_DEL Delivery**

### **ALC\_DEL.1 Delivery procedures**

**ALC\_DEL.1.1D** The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

**ALC\_DEL.1.2D** The developer shall use the delivery procedures.

**ALC\_DEL.1.1C** The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

**ALC\_DEL.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### **7.2.3.4 ALC\_DVS Development security**

### **ALC\_DVS.2 Sufficiency of security measures**

**ALC\_DVS.2.1D** The developer shall produce and provide development security documentation.

**ALC\_DVS.2.1C** The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the

confidentiality and integrity of the TOE design and implementation in its development environment.

**ALC\_DVS.2.2C** The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

**ALC\_DVS.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ALC\_DVS.2.2E** The evaluator shall confirm that the security measures are being applied.

#### 7.2.3.5 ALC\_LCD Life-cycle definition

##### **ALC\_LCD.1 Developer defined life-cycle model**

**ALC\_LCD.1.1D** The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

**ALC\_LCD.1.2D** The developer shall provide life-cycle definition documentation.

**ALC\_LCD.1.1C** The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

**ALC\_LCD.1.2C** The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

**ALC\_LCD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 7.2.3.6 ALC\_TAT Tools and techniques

## **ALC\_TAT.2 Compliance with implementation standards**

**ALC\_TAT.2.1D** The developer shall provide the documentation identifying each development tool being used for the TOE.

**ALC\_TAT.2.2D** The developer shall document and provide the selected implementation-dependent options of each development tool.

**ALC\_TAT.2.3D** The developer shall describe and provide the implementation standards that are being applied by the developer.

**ALC\_TAT.2.1C** Each development tool used for implementation shall be well-defined.

**ALC\_TAT.2.2C** The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

**ALC\_TAT.2.3C** The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

**ALC\_TAT.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ALC\_TAT.2.2E** The evaluator shall confirm that the implementation standards have been applied.

### **7.2.4 ASE Security Target evaluation**

#### **7.2.4.1 ASE\_CCL Conformance claims**

## **ASE\_CCL.1 Conformance claims**

**ASE\_CCL.1.1D** The developer shall provide a conformance claim.

**ASE\_CCL.1.2D** The developer shall provide a conformance claim rationale.

**ASE\_CCL.1.1C** The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

**ASE\_CCL.1.2C** The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

**ASE\_CCL.1.3C** The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

**ASE\_CCL.1.4C** The CC conformance claim shall be consistent with the extended components definition.

**ASE\_CCL.1.5C** The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

**ASE\_CCL.1.6C** The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

**ASE\_CCL.1.7C** The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

**ASE\_CCL.1.8C** The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

**ASE\_CCL.1.9C** The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

**ASE\_CCL.1.10C** The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

**ASE\_CCL.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.4.2 ASE\_ECD Extended components definition**

## **ASE\_ECD.1 Extended components definition**

**ASE\_ECD.1.1D** The developer shall provide a statement of security requirements.

**ASE\_ECD.1.2D** The developer shall provide an extended components definition.

**ASE\_ECD.1.1C** The statement of security requirements shall identify all extended security requirements.

**ASE\_ECD.1.2C** The extended components definition shall define an extended component for each extended security requirement.

**ASE\_ECD.1.3C** The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

**ASE\_ECD.1.4C** The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

**ASE\_ECD.1.5C** The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

**ASE\_ECD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE\_ECD.1.2E** The evaluator shall confirm that no extended component can be clearly expressed using existing components.

### **7.2.4.3 ASE\_INT ST introduction**

## **ASE\_INT.1 ST introduction**

**ASE\_INT.1.1D** The developer shall provide an ST introduction.

**ASE\_INT.1.1C** The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

**ASE\_INT.1.2C** The ST reference shall uniquely identify the ST.

**ASE\_INT.1.3C** The TOE reference shall identify the TOE.

**ASE\_INT.1.4C** The TOE overview shall summarise the usage and major security features of the TOE.

**ASE\_INT.1.5C** The TOE overview shall identify the TOE type.

**ASE\_INT.1.6C** The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

**ASE\_INT.1.7C** The TOE description shall describe the physical scope of the TOE.

**ASE\_INT.1.8C** The TOE description shall describe the logical scope of the TOE.

**ASE\_INT.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE\_INT.1.2E** The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

### **7.2.4.4 ASE\_OBJ Security objectives**

## **ASE\_OBJ.2 Security objectives**

**ASE\_OBJ.2.1D** The developer shall provide a statement of security objectives.

**ASE\_OBJ.2.2D** The developer shall provide a security objectives rationale.

**ASE\_OBJ.2.1C** The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

**ASE\_OBJ.2.2C** The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

**ASE\_OBJ.2.3C** The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

**ASE\_OBJ.2.4C** The security objectives rationale shall demonstrate that the security objectives counter all threats.

**ASE\_OBJ.2.5C** The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

**ASE\_OBJ.2.6C** The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

**ASE\_OBJ.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.4.5 ASE\_REQ Security requirements**

## **ASE\_REQ.2 Derived security requirements**

**ASE\_REQ.2.1D** The developer shall provide a statement of security requirements.

**ASE\_REQ.2.2D** The developer shall provide a security requirements rationale.

**ASE\_REQ.2.1C** The statement of security requirements shall describe the SFRs and the SARs.

**ASE\_REQ.2.2C** All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

**ASE\_REQ.2.3C** The statement of security requirements shall identify all operations on the security requirements.

**ASE\_REQ.2.4C** All operations shall be performed correctly.

**ASE\_REQ.2.5C** Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

**ASE\_REQ.2.6C** The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

**ASE\_REQ.2.7C** The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

**ASE\_REQ.2.8C** The security requirements rationale shall explain why the SARs were chosen.

**ASE\_REQ.2.9C** The statement of security requirements shall be internally consistent.

**ASE\_REQ.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.4.6 ASE\_SPD Security problem definition**

## **ASE\_SPD.1 Security problem definition**

**ASE\_APD.1.1D** The developer shall provide a security problem definition.

**ASE\_SPD.1.1C** The security problem definition shall describe the threats.

**ASE\_SPD.1.2C** All threats shall be described in terms of a threat agent, an asset, and an adverse action.

**ASE\_SPD.1.3C** The security problem definition shall describe the OSPs.

**ASE\_SPD.1.4C** The security problem definition shall describe the assumptions about the operational environment of the TOE.

**ASE\_SPD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.4.7 ASE\_TSS TOE summary specification**

## **ASE\_TSS.1 TOE summary specification**

**ASE\_TSS.1.1D** The developer shall provide a TOE summary specification.

**ASE\_TSS.1.1C** The TOE summary specification shall describe how the TOE meets each SFR.

**ASE\_TSS.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE\_TSS.1.2E** The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

### **7.2.5 ATE Tests**

#### **7.2.5.1 ATE\_COV Coverage**

## **ATE\_COV.2 Analysis of coverage**

**ATE\_COV.2.1D** The developer shall provide an analysis of the test coverage.

**ATE\_COV.2.1C** The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

**ATE\_COV.2.2C** The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

**ATE\_COV.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.5.2 ATE\_DPT Depth**

## **ATE\_DPT.3 Testing: modular design**

**ATE\_DPT.3.1D** The developer shall provide the analysis of the depth of testing.

**ATE\_DPT.3.1C** The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

**ATE\_DPT.3.2C** The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

**ATE\_DPT.3.3C** The analysis of the depth of testing shall demonstrate that all TSF modules in the TOE design have been tested.

**ATE\_DPT.3.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.5.3 ATE\_FUN Functional tests**

## **ATE\_FUN.1 Functional testing**

**ATE\_FUN.1.1D** The developer shall test the TSF and document the results.

**ATE\_FUN.1.2D** The developer shall provide test documentation.

**ATE\_FUN.1.1C** The test documentation shall consist of test plans, expected test results and actual test results.

**ATE\_FUN.1.2C** The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

**ATE\_FUN.1.3C** The expected test results shall show the anticipated outputs from a successful execution of the tests.

**ATE\_FUN.1.4C** The actual test results shall be consistent with the expected test results.

**ATE\_FUN.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### **7.2.5.4 ATE\_IND Independent testing**

## **ATE\_IND.2 Independent testing - sample**

**ATE\_IND.2.1D** The developer shall provide the TOE for testing.

**ATE\_IND.2.1C** The TOE shall be suitable for testing.

**ATE\_IND.2.2C** The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

**ATE\_IND.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ATE\_IND.2.2E** The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

**ATE\_IND.2.3E** The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

### **7.2.6 AVA Vulnerability assessment**

#### **7.2.6.1 AVA\_VAN Vulnerability analysis**

## **AVA\_VAN.5 Advanced methodical vulnerability analysis**

**AVA\_VAN.5.1D** The developer shall provide the TOE for testing.

**AVA\_VAN.5.1C** The TOE shall be suitable for testing.

**AVA\_VAN.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AVA\_VAN.5.2E** The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

**AVA\_VAN.5.3E** The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security

architecture description and implementation representation to identify potential vulnerabilities in the TOE.

**AVA\_VAN.5.4E** The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

## 7.3 Security Requirements Rationale

### 7.3.1 Objectives

#### 7.3.1.1 Security Objectives for the TOE

##### Security Objectives from the PP

**OT.Sens\_Data\_Conf** The security objective OT.Sense\_Data\_Conf "Confidentiality of sensitive biometric reference data" is enforced by the Access Control SFP defined in FDP\_ACC.1/TRM and FDP\_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS\_COP.1/SIG\_VER. The SFRs FIA\_UID.1/PACE and FIA\_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA\_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA\_UAU.4/PACE. The SFR FIA\_UAU.6/EAC and FDP\_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS\_RND.1 (for the generation of the terminal authentication challenge), FCS\_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), FCS\_CKM.1/CA\_DATA\_GEN for generation of Chip Authentication Data in personalization phase, and FCS\_COP.1/CA\_ENC and FCS\_COP.1/CA\_MAC for the ENC\_MAC\_Mode secure messaging. The session keys are destroyed according to FCS\_CKM.4 after use. The SFR FMT\_MTD.1/CAPK and FMT\_MTD.1/KEY\_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. FIA\_UAU.6/MP requires that the sensitive data is sent via Secure Messaging during personalization phase. To allow a verification of the certificate chain as in FMT\_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as of FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. FMT\_MOF.1/GP ensures all data is transmitted and received via secure messaging to ensure confidentiality

**OT.Chip\_Auth\_Proof** The security objective OT.Chip\_Auth\_Proof "Proof of eDigitalIdentity 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.Data\_Integrity** The security objective OT.Data\_Integrity "Integrity of personal data" requires the TOE to protect the integrity of the logical eDigitalIdentity document stored on the eDigitalIdentity document's chip against physical manipulation and unauthorized writing. 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): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical eDigitalIdentity document (FDP\_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical eDigitalIdentity document (cf. FDP\_ACF.1.4/TRM). 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 Personalisation Agent must identify and authenticate themselves according to FIA\_UID.1/PACE and FIA\_UAU.1/PACE before accessing these data. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE and FCS\_CKM.4 represent some required specific properties of the protocols used. The SFR FMT\_SMR.1/PACE lists the roles and the SFR FMT\_SMF.1 lists the TSF management functions.

Unauthorized modifying of the exchanged data is addressed, in the first line, by FTP\_ITC.1/PACE using FCS\_COP.1/PACE\_MAC. For PACE secured data exchange, 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 resp. FIA\_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP\_RIP.1 requires erasing the values of session keys (here: for KMAC).

The TOE supports the inspection system detect any modification of the transmitted logical eDigitalIdentity document data after Chip Authentication v.1. The SFR FIA\_UAU.6/EAC and FDP\_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS\_CKM.1/CA and FCS\_CKM.1/CAM(for the generation of shared secret and for the derivation of the new session keys), and FCS\_COP.1/CA\_ENC and FCS\_COP.1/CA\_MAC for the ENC\_MAC\_Mode secure messaging. The session keys are destroyed according to FCS\_CKM.4 after use.

The SFR FMT\_MTD.1/CAPK and FMT\_MTD.1/KEY\_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FCS\_RND.1 represents a general support for cryptographic operations needed.

The SFRs FDP\_ACC.1/UPD\_FILE and FDP\_ACF.1/UPD\_FILE ensure that no terminal is allowed to modify the user data.

FIA\_UAU.6/MP and FMT\_MOF.1/GP makes sure that the data is transmitted via secure messaging to maintain integrity.

Additionally to the SFRs from [PACE/EACPP] which cover these objectives, these security objectives are achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFRs FIA\_API.1/TOE. Since PACE can use the PIN as the shared secret, using and management of PIN, the SFRs FIA\_AFL.1/PACE, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN support also the achievement of these objectives. The SFR FMT\_SMF.1 support the related functions. The SFR FDP\_RIP.1 requires erasing the temporal values PIN and PUK.

**OT.Data\_Authenticity** The security objective OT.Data\_Authenticity aims ensuring authenticity of the User- and TSF data (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 or Chip and Terminal Authentication v.1 (FIA\_UID.1/PACE, FIA\_UAU.1/PACE) using FCS\_CKM.1/DH\_PACE resp. FCS\_CKM.1/CA or FCS\_CKM.1/CAM and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE resp. FIA\_UAU.6/EAC. FIA\_UAU.6/MP ensures the data that is reaching the TOE is coming from the personalization agent by maintaining secure messaging for all commands. FDP\_RIP.1 requires erasing the values of session keys (here: for KMAC). FIA\_UAU.4/PACE, FIA\_UAU.5/PACE and FCS\_CKM.4 represent some required specific properties of the protocols used. The SFR FMT\_MTD.1/KEY\_READ restricts the access to the PACE passwords and the Chip Authentication Private 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.

Additionally to the SFRs from [PACE/EACPP] which cover these objectives, these security objectives are achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFR FIA\_API.1/TOE. Since PACE can use the PIN as the shared secret, using and management of PIN, the SFRs FIA\_AFL.1/PACE, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN support also the achievement of these objectives. The SFR FMT\_SMF.1 support the related functions. The SFR FDP\_RIP.1 requires erasing the temporal values PIN and PUK.

**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 resp. Chip 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, FTP\_ITC.1/PACE using FCS\_COP.1/PACE\_ENC resp. FCS\_COP.1/CA\_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA\_UID.1/PACE, FIA\_UAU.1/PACE) using FCS\_CKM.1/DH\_PACE resp. FCS\_CKM.1/CA or FCS\_CKM.1/CAM and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE resp. FIA\_UAU.6/EAC and FIA\_UAU.6/MP for Manufacture and Personalization Agent authentication. 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 and the Chip Authentication Private 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 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.

Additionally to the SFRs from [PACE/EACPP] which cover these objectives, these security objectives are achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFR FIA\_API.1/TOE. Since PACE can use the PIN as the shared

secret, using and management of PIN, the SFRs FIA\_AFL.1/PACE, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN support also the achievement of these objectives. The SFR FMT\_SMF.1 support the related functions. The SFR FDP\_RIP.1 requires erasing the temporal values PIN and PUK.

**OT.Tracing** The security objective OT.Tracing aims that the TOE prevents gathering TOE tracing data by means of unambiguously identifying the eDigitalIdentity document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ). This objective is achieved as follows: (i) while establishing PACE communication with PIN, PUK, CAN or MRZ (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 card-individual) – FTP\_ITC.1/PACE.

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

**OT.Prot\_Inf\_Leak** The security objective OT.Prot\_Inf\_Leak “Protection against Information Leakage” requires the TOE to protect confidential TSF data stored and/or processed in the eDigitalIdentity document’s chip against disclosure

- 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 which is addressed by the SFR FPT\_EMS.1,
- o by forcing a malfunction of the TOE which is addressed by the SFR FPT\_FLS.1 and FPT\_TST.1, and/or
- o by a physical manipulation of the TOE which is addressed by the SFR FPT\_PHP.3.

**OT.Prot\_Phys-Tamper** The security objective OT.Prot\_Phys-Tamper “Protection against Physical Tampering” is covered by the SFR FPT\_PHP.3.

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

**OT.Identification** The security objective OT.Identification “Identification of the TOE” addresses the storage of Initialisation and Pre-Personalisation 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 Pre-personalisation 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 "Access Control for Personalisation of logical eDigitalIdentity document" addresses the access control of the writing the logical eDigitalIdentity document. 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. The write access to the logical eDigitalIdentity document data are defined by the SFR FIA\_UID.1/PACE, FIA\_UAU.1/PACE, FDP\_ACC.1/TRM and FDP\_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical eDigitalIdentity document only once. FMT\_MTD.1/PA covers the related property of OT.AC\_Pers (writing SOD and, in generally, personalisation data). The SFR FMT\_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT\_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT\_MTD.1/KEY\_READ and FMT\_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA\_UAU.4/PACE and FIA\_UAU.5/PACE. If the Personalisation Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalisation Agent Keys the TOE will use TSF according to the FCS\_RND.1 (for the generation of the challenge), FCS\_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), FCS\_CKM.1/CA\_DATA\_GEN for generation of CA Data in phase 6, and FCS\_COP.1/CA\_ENC and FCS\_COP.1/CA\_MAC (for the ENC\_MAC\_Mode secure messaging), FCS\_COP.1/SIG\_VER (as part of the Terminal Authentication Protocol v.1) and FIA\_UAU.6/EAC (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS\_RND.1 (for the generation of the challenge) and FCS\_COP.1/CA\_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS\_CKM.4 after use.

The Personalisation Agent can load the PACE password according to FMT\_MTD.1/PACE\_PWD.

FMT\_MTD.1/LCS\_PERS ensures only personalization agent can transfer the TOE from life cycle phase 6 to phase 7.

FIA\_UAU.6/MP ensures all commands in personalization phase are sent via secure messaging. FIA\_AFL.1/MP helps block the Authentication in Phase 6 if too many failed authentication attempts occur to prevent attacks.

FDP\_ACC.1/UPD\_FILE and FDP\_ACF.1/UPD\_FILE restrict write access to files to personalization agent.

Additionally to the SFRs from [PACE/EACPP] which cover this objective, the security objective OT.AC\_Pers is achieved by terminal identification/authentication using and managing the PIN/PUK as required by the SFRs FIA\_AFL.1/PACE. The SFR FMT\_SMF.1 support the related functions. The SFR FDP\_RIP.1 requires erasing the temporal values PIN and PUK.

**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/PACE and FIA\_UAU.5/PACE. 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 read access to the Pre-personalization keys is prevented by SFRs 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/PACE and FIA\_UAU.5/PACE. 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 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 FCS\_CKM.4, FPT\_EMS.1, FPT\_FLS.1 and FPT\_PHP.3 the confidentiality of Personalization Agent 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 Extended Inspection System is allowed to modify Updatable Data, only if with the name corresponding to the one (or beginning of the one) set following FMT\_MTD.1/UPD\_FILE by the Personalization Agent during Pre-Personalisation and Personalisation phases.

**OT.BAC\_Expiration** The security objective OT.BAC\_Expiration “Automatic deactivation of BAC protocol” is ensured by the SFR FMT\_SMF.1 and detailed in FMT\_MOF.1/BAC\_EXP

regarding mechanism activation and FMT\_MTD.1/BAC\_EXP regarding mechanism configuration.

**OT.AC\_SM\_Level** The security objective OT.AC\_SM\_Level "Access control to sensitive biometric reference data according to SM level" is covered by FMT\_MTD.1/SM\_LVL.

**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.

**Additional Objectives as per Addendum**

**OT.Sens\_Ident\_User\_Data\_Conf** The security objective of OT.Sens\_Ident\_User\_Data\_Conf aims to explicitly protect sensitive identification user and TSF-Data during their exchange. It is enforcing by the Access Control SFP defined in FDP\_ACC.1/TRM and FDP\_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS\_COP.1/SIG\_VER. A prerequisite for establishing a trusted channel is a successful Chip Authentication thanks to the SFRs FIA\_API.1/TOE. Since PACE can use the PIN as the shared secret, the SFRs FIA\_AFL.1/PACE, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN support the achievement of this objective. The SFR FMT\_SMF.1 support the related functions. The SFR FDP\_RIP.1 requires erasing the temporal values PIN and PUK.

**Additional Objectives for Active Authentication**

**OT.AA\_Proof** The security objective OT.AA\_Proof is ensured by the Active Authentication Protocol activated by FMT\_MOF.1/AA and provided by FDP\_DAU.1/AA, FDP\_ITC.1/AA proving the identity and authenticity of the TOE. The Active Authentication relies on FCS\_COP.1/AA and FCS\_RND.1. It is performed using a TOE internally stored confidential private key as required by FMT\_MTD.1/AA\_KEY\_WRITE and FMT\_MTD.1/AA\_KEY\_READ.

**OT.Data\_Int\_AA** The security objective OT.AA\_Proof is ensured by the Active Authentication Protocol activated by FMT\_MOF.1/AA and provided by FDP\_DAU.1/AA and FDP\_ITC.1/AA proving the identity and authenticity of the TOE.

**7.3.2 Rationale tables of Security Objectives and SFRs**

Security Objectives	Security Functional Requirements	Rationale
<a href="#">OT.Sens_Data_Conf</a>	<a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/CA_ENC</a> , <a href="#">FCS_COP.1/SIG_VER</a> , <a href="#">FCS_COP.1/CA_MAC</a> , <a href="#">FCS_RND.1</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_UAU.4/PACE</a> , <a href="#">FIA_UAU.5/PACE</a> ,	<a href="#">Section 7.3.1</a>

	<a href="#">FIA UAU.6/EAC</a> , <a href="#">FIA UAU.6/MP</a> , <a href="#">FDP ACC.1/TRM</a> , <a href="#">FDP ACF.1/TRM</a> , <a href="#">FDP UCT.1/TRM</a> , <a href="#">FMT MOF.1/GP</a> , <a href="#">FMT MTD.1/CVCA INI</a> , <a href="#">FMT MTD.1/CVCA UPD</a> , <a href="#">FMT MTD.1/DATE</a> , <a href="#">FMT MTD.1/CAPK</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FMT MTD.3</a> , <a href="#">FCS CKM.1/CA DATA GEN</a>	
<a href="#">OT.Chip Auth Proof</a>	<a href="#">FCS CKM.1/CA</a> , <a href="#">FCS COP.1/CA ENC</a> , <a href="#">FCS COP.1/CA MAC</a> , <a href="#">FIA API.1/CA</a> , <a href="#">FMT SMF.1</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FMT MTD.1/CAPK</a> , <a href="#">FCS CKM.1/CA DATA GEN</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Data Integrity</a>	<a href="#">FCS CKM.1/DH PACE</a> , <a href="#">FCS COP.1/PACE MAC</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA UAU.6/EAC</a> , <a href="#">FIA UID.1/PACE</a> , <a href="#">FIA UAU.4/PACE</a> , <a href="#">FIA UAU.6/PACE</a> , <a href="#">FDP ACF.1/TRM</a> , <a href="#">FDP ACC.1/TRM</a> , <a href="#">FDP UIT.1/TRM</a> , <a href="#">FTP ITC.1/PACE</a> , <a href="#">FMT MTD.1/PA</a> , <a href="#">FMT MTD.1/CAPK</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FCS COP.1/CA MAC</a> , <a href="#">FCS CKM.1/CA</a> , <a href="#">FCS CKM.4</a> , <a href="#">FCS COP.1/CA ENC</a> , <a href="#">FDP RIP.1</a> , <a href="#">FMT SMF.1</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FPT PHP.3</a> , <a href="#">FIA UAU.6/MP</a> , <a href="#">FDP ACC.1/UPD FILE</a> , <a href="#">FDP ACF.1/UPD FILE</a> , <a href="#">FCS RND.1</a> , <a href="#">FMT MOF.1/GP</a> , <a href="#">FCS CKM.1/CAM</a> , <a href="#">FIA AFL.1/PACE</a> , <a href="#">FIA API.1/TOE</a> , <a href="#">FMT MTD.1/Initialize PIN</a> , <a href="#">FMT MTD.1/Resume PIN</a> , <a href="#">FMT MTD.1/Change PIN</a> , <a href="#">FMT MTD.1/Unblock PIN</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Data Authenticity</a>	<a href="#">FCS CKM.1/DH PACE</a> , <a href="#">FCS COP.1/PACE MAC</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA UAU.6/EAC</a> , <a href="#">FIA UID.1/PACE</a> , <a href="#">FIA UAU.4/PACE</a> , <a href="#">FIA UAU.6/PACE</a> , <a href="#">FTP ITC.1/PACE</a> , <a href="#">FMT MTD.1/PA</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FCS CKM.1/CA</a> , <a href="#">FCS CKM.4</a> , <a href="#">FDP RIP.1</a> , <a href="#">FMT SMF.1</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FIA UAU.6/MP</a> , <a href="#">FCS RND.1</a> , <a href="#">FCS CKM.1/CAM</a> , <a href="#">FIA AFL.1/PACE</a> , <a href="#">FIA API.1/TOE</a> , <a href="#">FMT MTD.1/Initialize PIN</a> , <a href="#">FMT MTD.1/Resume PIN</a> ,	<a href="#">Section 7.3.1</a>

	<a href="#">FMT_MTD.1/Change_PIN</a> , <a href="#">FMT_MTD.1/Unblock_PIN</a>	
<a href="#">OT.Data Confidentiality</a>	<a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_COP.1/PACE_ENC</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_UAU.5/PACE</a> , <a href="#">FIA_UAU.6/EAC</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.4/PACE</a> , <a href="#">FIA_UAU.6/PACE</a> , <a href="#">FDP_ACF.1/TRM</a> , <a href="#">FDP_ACC.1/TRM</a> , <a href="#">FDP_UCT.1/TRM</a> , <a href="#">FDP_UIT.1/TRM</a> , <a href="#">FTP_ITC.1/PACE</a> , <a href="#">FMT_MTD.1/PA</a> , <a href="#">FMT_MTD.1/KEY_READ</a> , <a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/CA_ENC</a> , <a href="#">FDP_RIP.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a> , <a href="#">FIA_UAU.6/MP</a> , <a href="#">FCS_RND.1</a> , <a href="#">FCS_CKM.1/CAM</a> , <a href="#">FIA_AFL.1/PACE</a> , <a href="#">FIA_API.1/TOE</a> , <a href="#">FMT_MTD.1/Initialize_PIN</a> , <a href="#">FMT_MTD.1/Resume_PIN</a> , <a href="#">FMT_MTD.1/Change_PIN</a> , <a href="#">FMT_MTD.1/Unblock_PIN</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Tracing</a>	<a href="#">FTP_ITC.1/PACE</a> , <a href="#">FIA_AFL.1/PACE</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Prot Abuse-Func</a>	<a href="#">FMT_LIM.2</a> , <a href="#">FMT_LIM.1</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Prot Inf Leak</a>	<a href="#">FPT_FLS.1</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_TST.1</a> , <a href="#">FPT_EMS.1</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Prot Phys-Tamper</a>	<a href="#">FPT_PHP.3</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Prot Malfunction</a>	<a href="#">FPT_FLS.1</a> , <a href="#">FPT_TST.1</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Identification</a>	<a href="#">FMT_MTD.1/INI_ENA</a> , <a href="#">FMT_MTD.1/INI_DIS</a> , <a href="#">FAU_SAS.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.AC Pers</a>	<a href="#">FMT_MTD.1/PA</a> , <a href="#">FMT_MTD.1/KEY_READ</a> , <a href="#">FMT_MTD.1/INI_ENA</a> , <a href="#">FMT_MTD.1/INI_DIS</a> , <a href="#">FAU_SAS.1</a> , <a href="#">FIA_UAU.5/PACE</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a> , <a href="#">FIA_UAU.6/MP</a> , <a href="#">FIA_AFL.1/MP</a> , <a href="#">FDP_ACC.1/UPD_FILE</a> , <a href="#">FDP_ACF.1/UPD_FILE</a> , <a href="#">FMT_MTD.1/LCS_PERS</a> , <a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/CA_ENC</a> , <a href="#">FCS_COP.1/SIG_VER</a> , <a href="#">FCS_RND.1</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_UAU.4/PACE</a> , <a href="#">FIA_UAU.6/EAC</a> , <a href="#">FDP_ACC.1/TRM</a> , <a href="#">FDP_ACF.1/TRM</a> , <a href="#">FMT_MTD.1/PACE_PWD</a> , <a href="#">FPT_EMS.1</a> , <a href="#">FCS_CKM.1/CA_DATA_GEN</a> ,	<a href="#">Section 7.3.1</a>

	<a href="#">FCS COP.1/CA MAC</a> , <a href="#">FIA AFL.1/PACE</a> , <a href="#">FDP RIP.1</a>	
<a href="#">OT.Configuration</a>	<a href="#">FCS CKM.1/GP</a> , <a href="#">FCS COP.1/GP ENC</a> , <a href="#">FCS COP.1/GP MAC</a> , <a href="#">FCS COP.1/GP AUTH</a> , <a href="#">FCS COP.1/GP KEY DEC</a> , <a href="#">FTP ITC.1/MP</a> , <a href="#">FIA AFL.1/MP</a> , <a href="#">FIA UAU.6/MP</a> , <a href="#">FCS CKM.4</a> , <a href="#">FCS RND.1</a> , <a href="#">FPT EMS.1</a> , <a href="#">FPT FLS.1</a> , <a href="#">FPT PHP.3</a> , <a href="#">FIA UAU.4/PACE</a> , <a href="#">FIA UAU.5/PACE</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Update File</a>	<a href="#">FDP ACC.1/UPD FILE</a> , <a href="#">FDP ACF.1/UPD FILE</a> , <a href="#">FMT MTD.1/UPD FILE</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.BAC Expiration</a>	<a href="#">FMT MOF.1/BAC EXP</a> , <a href="#">FMT SMF.1</a> , <a href="#">FMT MTD.1/BAC EXP</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.AC SM Level</a>	<a href="#">FMT MTD.1/SM LVL</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Chip Auth Proof PACE CAM</a>	<a href="#">FCS COP.1/CAM</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA API.1/CAM</a> , <a href="#">FIA UID.1/PACE</a> , <a href="#">FCS CKM.1/CAM</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Sens Ident User Data Conf</a>	<a href="#">FIA AFL.1/PACE</a> , <a href="#">FIA API.1/TOE</a> , <a href="#">FMT MTD.1/Initialize PIN</a> , <a href="#">FMT MTD.1/Resume PIN</a> , <a href="#">FMT MTD.1/Change PIN</a> , <a href="#">FMT MTD.1/Unblock PIN</a> , <a href="#">FMT SMF.1</a> , <a href="#">FDP RIP.1</a> , <a href="#">FDP ACC.1/TRM</a> , <a href="#">FDP ACF.1/TRM</a> , <a href="#">FCS COP.1/SIG VER</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.AA Proof</a>	<a href="#">FCS COP.1/AA</a> , <a href="#">FCS RND.1</a> , <a href="#">FDP ITC.1/AA</a> , <a href="#">FDP DAU.1/AA</a> , <a href="#">FMT MOF.1/AA</a> , <a href="#">FMT MTD.1/AA KEY READ</a> , <a href="#">FMT MTD.1/AA KEY WRITE</a>	<a href="#">Section 7.3.1</a>
<a href="#">OT.Data Int AA</a>	<a href="#">FDP DAU.1/AA</a> , <a href="#">FDP ITC.1/AA</a> , <a href="#">FMT MOF.1/AA</a>	<a href="#">Section 7.3.1</a>

**Table 17 Security Objectives and SFRs - Coverage**

Security Functional Requirements	Security Objectives
<a href="#">FCS CKM.1/DH PACE</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a>
<a href="#">FCS CKM.1/CA</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Chip Auth Proof</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a>

<a href="#">FCS_CKM.1/CAM</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Chip Auth Proof PACE CAM</a>
<a href="#">FCS_CKM.1/CA_DATA_GEN</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Chip Auth Proof</a> , <a href="#">OT.AC Pers</a>
<a href="#">FCS_CKM.1/GP</a>	<a href="#">OT.Configuration</a>
<a href="#">FCS_CKM.4</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Configuration</a>
<a href="#">FCS_COP.1/PACE_ENC</a>	<a href="#">OT.Data Confidentiality</a>
<a href="#">FCS_COP.1/PACE_MAC</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a>
<a href="#">FCS_COP.1/CA_ENC</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Chip Auth Proof</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a>
<a href="#">FCS_COP.1/SIG_VER</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FCS_COP.1/CA_MAC</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Chip Auth Proof</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.AC Pers</a>
<a href="#">FCS_COP.1/CAM</a>	<a href="#">OT.Chip Auth Proof PACE CAM</a>
<a href="#">FCS_COP.1/GP_ENC</a>	<a href="#">OT.Configuration</a>
<a href="#">FCS_COP.1/GP_MAC</a>	<a href="#">OT.Configuration</a>
<a href="#">FCS_COP.1/GP_AUTH</a>	<a href="#">OT.Configuration</a>
<a href="#">FCS_COP.1/GP_KEY_DEC</a>	<a href="#">OT.Configuration</a>
<a href="#">FCS_COP.1/AA</a>	<a href="#">OT.AA Proof</a>
<a href="#">FCS_RND.1</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Configuration</a> , <a href="#">OT.AA Proof</a>
<a href="#">FIA_UID.1/PACE</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Chip Auth Proof PACE CAM</a>
<a href="#">FIA_UAU.1/PACE</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a>
<a href="#">FIA_UAU.4/PACE</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Configuration</a>
<a href="#">FIA_UAU.5/PACE</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Configuration</a> , <a href="#">OT.Chip Auth Proof PACE CAM</a>

<a href="#">FIA UAU.6/EAC</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a>
<a href="#">FIA UAU.6/PACE</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a>
<a href="#">FIA UAU.6/MP</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Configuration</a>
<a href="#">FIA AFL.1/PACE</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Tracing</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FIA AFL.1/MP</a>	<a href="#">OT.AC Pers</a> , <a href="#">OT.Configuration</a>
<a href="#">FIA API.1/CA</a>	<a href="#">OT.Chip Auth Proof</a>
<a href="#">FIA API.1/CAM</a>	<a href="#">OT.Chip Auth Proof PACE CAM</a>
<a href="#">FDP ACC.1/TRM</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FDP ACF.1/TRM</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FDP ACC.1/UPD FILE</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Update File</a>
<a href="#">FDP ACF.1/UPD FILE</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Update File</a>
<a href="#">FDP RIP.1</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FDP UCT.1/TRM</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Confidentiality</a>
<a href="#">FDP UIT.1/TRM</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Confidentiality</a>
<a href="#">FDP DAU.1/AA</a>	<a href="#">OT.AA Proof</a> , <a href="#">OT.Data Int AA</a>
<a href="#">FDP ITC.1/AA</a>	<a href="#">OT.AA Proof</a> , <a href="#">OT.Data Int AA</a>
<a href="#">FTP ITC.1/PACE</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Tracing</a>
<a href="#">FTP ITC.1/MP</a>	<a href="#">OT.Configuration</a>
<a href="#">FAU SAS.1</a>	<a href="#">OT.Identification</a> , <a href="#">OT.AC Pers</a>
<a href="#">FMT MOF.1/BAC EXP</a>	<a href="#">OT.BAC Expiration</a>
<a href="#">FMT MOF.1/GP</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Data Integrity</a>
<a href="#">FMT MOF.1/AA</a>	<a href="#">OT.AA Proof</a> , <a href="#">OT.Data Int AA</a>
<a href="#">FMT SMF.1</a>	<a href="#">OT.Chip Auth Proof</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> ,

	<a href="#">OT.Identification</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.BAC Expiration</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FMT SMR.1/PACE</a>	<a href="#">OT.Chip Auth Proof</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Identification</a> , <a href="#">OT.AC Pers</a>
<a href="#">FMT MTD.1/INI ENA</a>	<a href="#">OT.Identification</a> , <a href="#">OT.AC Pers</a>
<a href="#">FMT MTD.1/INI DIS</a>	<a href="#">OT.Identification</a> , <a href="#">OT.AC Pers</a>
<a href="#">FMT MTD.1/PA</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a>
<a href="#">FMT MTD.1/CVCA INI</a>	<a href="#">OT.Sens Data Conf</a>
<a href="#">FMT MTD.1/CVCA UPD</a>	<a href="#">OT.Sens Data Conf</a>
<a href="#">FMT MTD.1/DATE</a>	<a href="#">OT.Sens Data Conf</a>
<a href="#">FMT MTD.1/CAPK</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Chip Auth Proof</a> , <a href="#">OT.Data Integrity</a>
<a href="#">FMT MTD.1/KEY READ</a>	<a href="#">OT.Sens Data Conf</a> , <a href="#">OT.Chip Auth Proof</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.AC Pers</a>
<a href="#">FMT MTD.1/PACE PWD</a>	<a href="#">OT.AC Pers</a>
<a href="#">FMT MTD.1/LCS PERS</a>	<a href="#">OT.AC Pers</a>
<a href="#">FMT MTD.1/BAC EXP</a>	<a href="#">OT.BAC Expiration</a>
<a href="#">FMT MTD.1/UPD FILE</a>	<a href="#">OT.Update File</a>
<a href="#">FMT MTD.1/SM LVL</a>	<a href="#">OT.AC SM Level</a>
<a href="#">FMT MTD.1/AA KEY READ</a>	<a href="#">OT.AA Proof</a>
<a href="#">FMT MTD.1/AA KEY WRITE</a>	<a href="#">OT.AA Proof</a>
<a href="#">FMT MTD.3</a>	<a href="#">OT.Sens Data Conf</a>
<a href="#">FMT LIM.1</a>	<a href="#">OT.Prot Abuse-Func</a>
<a href="#">FMT LIM.2</a>	<a href="#">OT.Prot Abuse-Func</a>
<a href="#">FPT EMS.1</a>	<a href="#">OT.Prot Inf Leak</a> , <a href="#">OT.AC Pers</a> , <a href="#">OT.Configuration</a>
<a href="#">FPT FLS.1</a>	<a href="#">OT.Prot Inf Leak</a> , <a href="#">OT.Prot Malfunction</a> , <a href="#">OT.Configuration</a>
<a href="#">FPT PHP.3</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Prot Inf Leak</a> , <a href="#">OT.Prot Phys-Tamper</a> , <a href="#">OT.Configuration</a>
<a href="#">FPT TST.1</a>	<a href="#">OT.Prot Inf Leak</a> , <a href="#">OT.Prot Malfunction</a>

<a href="#">FIA_API.1/TOE</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FMT_MTD.1/Initialize PIN</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FMT_MTD.1/Resume PIN</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FMT_MTD.1/Change PIN</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Sens Ident User Data Conf</a>
<a href="#">FMT_MTD.1/Unlock PIN</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Sens Ident User Data Conf</a>

**Table 18 SFRs and Security Objectives**

### 7.3.3 Dependencies

#### 7.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">FCS_CKM.1/DH_PACE</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/PACE_ENC</a> , <a href="#">FCS_COP.1/PACE_MAC</a>
<a href="#">FCS_CKM.1/CA</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/CA_ENC</a> , <a href="#">FCS_COP.1/CA_MAC</a>
<a href="#">FCS_CKM.1/CAM</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/CAM</a>
<a href="#">FCS_CKM.1/CA_DATA_GEN</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/SIG_VER</a>
<a href="#">FCS_CKM.1/GP</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_COP.1/GP_ENC</a> , <a href="#">FCS_COP.1/GP_MAC</a>
<a href="#">FCS_CKM.4</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	<a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_CKM.1/CA_DATA_GEN</a> , <a href="#">FCS_CKM.1/GP</a>

<a href="#">FCS COP.1/PACE_ENC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/PACE_MAC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/CA_ENC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/SIG_VER</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/CA_MAC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/CAM</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/CAM</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/GP_ENC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/GP</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/GP_MAC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/GP</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/GP_AUTH</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/GP</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/GP_KEY_DEC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/GP</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS COP.1/AA</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FDP_ITC.1/AA</a>

<a href="#">FCS_RND.1</a>	No Dependencies	
<a href="#">FIA_UID.1/PACE</a>	No Dependencies	
<a href="#">FIA_UAU.1/PACE</a>	(FIA_UID.1)	<a href="#">FIA_UID.1/PACE</a>
<a href="#">FIA_UAU.4/PACE</a>	No Dependencies	
<a href="#">FIA_UAU.5/PACE</a>	No Dependencies	
<a href="#">FIA_UAU.6/EAC</a>	No Dependencies	
<a href="#">FIA_UAU.6/PACE</a>	No Dependencies	
<a href="#">FIA_UAU.6/MP</a>	No Dependencies	
<a href="#">FIA_AFL.1/PACE</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1/PACE</a>
<a href="#">FIA_AFL.1/MP</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1/PACE</a>
<a href="#">FIA_API.1/CA</a>	No Dependencies	
<a href="#">FIA_API.1/CAM</a>	No Dependencies	
<a href="#">FDP_ACC.1/TRM</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/TRM</a>
<a href="#">FDP_ACF.1/TRM</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1/TRM</a>
<a href="#">FDP_ACC.1/UPD_FILE</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/UPD_FILE</a>
<a href="#">FDP_ACF.1/UPD_FILE</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1/UPD_FILE</a>
<a href="#">FDP_RIP.1</a>	No Dependencies	
<a href="#">FDP_UCT.1/TRM</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FTP_ITC.1/PACE</a>
<a href="#">FDP_UIT.1/TRM</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FTP_ITC.1/PACE</a>
<a href="#">FDP_DAU.1/AA</a>	No Dependencies	
<a href="#">FDP_ITC.1/AA</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1/TRM</a>
<a href="#">FTP_ITC.1/PACE</a>	No Dependencies	
<a href="#">FTP_ITC.1/MP</a>	No Dependencies	
<a href="#">FAU_SAS.1</a>	No Dependencies	
<a href="#">FMT_MOF.1/BAC_EXP</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>

<a href="#">FMT_MOF.1/GP</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MOF.1/AA</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_SMF.1</a>	No Dependencies	
<a href="#">FMT_SMR.1/PACE</a>	(FIA_UID.1)	<a href="#">FIA_UID.1/PACE</a>
<a href="#">FMT_MTD.1/INI_ENA</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/INI_DIS</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/PA</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/CVCA_INI</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/CVCA_UPD</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/DATE</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/CAPK</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/KEY_READ</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/PACE_PWD</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/LCS_PERS</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/BAC_EXP</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/UPD_FILE</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/SM_LVL</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/AA_KEY_READ</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/AA_KEY_WRITE</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.3</a>	(FMT_MTD.1)	<a href="#">FMT_MTD.1/CVCA_INI</a> , <a href="#">FMT_MTD.1/CVCA_UPD</a>
<a href="#">FMT_LIM.1</a>	(FMT_LIM.2)	<a href="#">FMT_LIM.2</a>

<a href="#">FMT_LIM.2</a>	(FMT_LIM.1)	<a href="#">FMT_LIM.1</a>
<a href="#">FPT_EMS.1</a>	No Dependencies	
<a href="#">FPT_FLS.1</a>	No Dependencies	
<a href="#">FPT_PHP.3</a>	No Dependencies	
<a href="#">FPT_TST.1</a>	No Dependencies	
<a href="#">FIA_API.1/TOE</a>	No Dependencies	
<a href="#">FMT_MTD.1/Initialize PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/Resume PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/Change PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>
<a href="#">FMT_MTD.1/Unblock PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a>

**Table 19 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 which are defined during the personalisation and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT\_MSA.1 and FMT\_MSA.3) is necessary here.

**The dependency FMT\_MSA.3 of FDP\_ITC.1/AA is discarded.** The access control TSF according to FDP\_ACF.1/TRM uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT\_MSA.1 and FMT\_MSA.3) is necessary here.

**7.3.3.2 SARs Dependencies**

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">ADV_ARC.1</a>	(ADV_FSP.1) and (ADV_TDS.1)	<a href="#">ADV_FSP.5</a> , <a href="#">ADV_TDS.4</a>
<a href="#">ADV_FSP.5</a>	(ADV_IMP.1) and (ADV_TDS.1)	<a href="#">ADV_IMP.1</a> , <a href="#">ADV_TDS.4</a>
<a href="#">ADV_IMP.1</a>	(ADV_TDS.3) and (ALC_TAT.1)	<a href="#">ADV_TDS.4</a> , <a href="#">ALC_TAT.2</a>

<a href="#">ADV_TDS.4</a>	(ADV_FSP.5)	<a href="#">ADV_FSP.5</a>
<a href="#">ADV_INT.2</a>	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	<a href="#">ADV_IMP.1</a> , <a href="#">ADV_TDS.4</a> , <a href="#">ALC_TAT.2</a>
<a href="#">AGD_OPE.1</a>	(ADV_FSP.1)	<a href="#">ADV_FSP.5</a>
<a href="#">AGD_PRE.1</a>	No Dependencies	
<a href="#">ALC_CMC.4</a>	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	<a href="#">ALC_CMS.5</a> , <a href="#">ALC_DVS.2</a> , <a href="#">ALC_LCD.1</a>
<a href="#">ALC_CMS.5</a>	No Dependencies	
<a href="#">ALC_DEL.1</a>	No Dependencies	
<a href="#">ALC_DVS.2</a>	No Dependencies	
<a href="#">ALC_LCD.1</a>	No Dependencies	
<a href="#">ALC_TAT.2</a>	(ADV_IMP.1)	<a href="#">ADV_IMP.1</a>
<a href="#">ASE_CCL.1</a>	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	<a href="#">ASE_ECD.1</a> , <a href="#">ASE_INT.1</a> , <a href="#">ASE_REQ.2</a>
<a href="#">ASE_ECD.1</a>	No Dependencies	
<a href="#">ASE_INT.1</a>	No Dependencies	
<a href="#">ASE_OBJ.2</a>	(ASE_SPD.1)	<a href="#">ASE_SPD.1</a>
<a href="#">ASE_REQ.2</a>	(ASE_ECD.1) and (ASE_OBJ.2)	<a href="#">ASE_ECD.1</a> , <a href="#">ASE_OBJ.2</a>
<a href="#">ASE_SPD.1</a>	No Dependencies	
<a href="#">ASE_TSS.1</a>	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	<a href="#">ADV_FSP.5</a> , <a href="#">ASE_INT.1</a> , <a href="#">ASE_REQ.2</a>
<a href="#">ATE_COV.2</a>	(ADV_FSP.2) and (ATE_FUN.1)	<a href="#">ADV_FSP.5</a> , <a href="#">ATE_FUN.1</a>
<a href="#">ATE_DPT.3</a>	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	<a href="#">ADV_ARC.1</a> , <a href="#">ADV_TDS.4</a> , <a href="#">ATE_FUN.1</a>
<a href="#">ATE_FUN.1</a>	(ATE_COV.1)	<a href="#">ATE_COV.2</a>
<a href="#">ATE_IND.2</a>	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	<a href="#">ADV_FSP.5</a> , <a href="#">AGD_OPE.1</a> , <a href="#">AGD_PRE.1</a> , <a href="#">ATE_COV.2</a> , <a href="#">ATE_FUN.1</a>
<a href="#">AVA_VAN.5</a>	(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)	<a href="#">ADV_ARC.1</a> , <a href="#">ADV_FSP.5</a> , <a href="#">ADV_IMP.1</a> , <a href="#">ADV_TDS.4</a> , <a href="#">AGD_OPE.1</a> , <a href="#">AGD_PRE.1</a> , <a href="#">ATE_DPT.3</a>

**Table 20 SARs Dependencies**

### **7.3.4 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.

### **7.3.5 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

### **7.3.6 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

The TOE provides the following Security Functions (TSF):

TSF	Acronym	Step 5	Step 6	Step 7
Access Control in Reading	F.ACR	Yes	Yes	Yes
Access Control in Writing	F.ACW	Yes	Yes	Yes
Clear Residual Information	F.CLR_INFO	Yes	Yes	Yes
Cryptographic Support	F.CRYPTO	Yes	Yes	Yes
Extended Access Control	F.EAC	No	No	Yes
PACE	F.PACE	No	No	Yes
MRTD Personalisation	F.PERS	No	Yes	No
Physical Protection	F.PHY	Yes	Yes	Yes
MRTD Pre-Personalisation	F.PREP	Yes	No	No
Safe State Management	F.SS	Yes	Yes	Yes
Secure Messaging	F.SM	Yes	Yes	Yes
Self Test	F.STST	No	No	Yes

#### 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 CA private key,
- o PACE passwords,
- o Active Authentication Keys.

It controls access to the Initialization and Pre-Personalization data by allowing read access without authentication prior to delivery. After delivery, only the personalization agent after authentication has read access to it.

Regarding the file structure:

In the Operational Use phase:

- o The terminal can read user data, the Document Security Object, (EF.COM, EF.SOD, EF.DG1 to EF.DG16) only after PACE or EAC 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), except for the current date, the CVCA public key and the CVCA certificate which can be updated if the access conditions is verified by the subjects defined in FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE.

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, Chip Authentication Private Key, Active Authentication Keys and Country Verifying Certification Authority Public 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.AA - Active Authentication**

This security functionality ensures the Active Authentication is performed as described in [ICAO\_9303] (if it is activated by the personalizer).

### **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, PACE authentication and EAC is securely cleared to prevent reuse
- o Session keys is securely erased in case an error is detected or the secure communication session is closed

- o ephem-SK picc -PACE is securely erased
- o PIN and PUK

## **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).
  - AES in CBC mode (key sizes 128,192,256 bits).
- o Secure messaging (message authentication code) using:
  - Retail MAC with key size 112 bits.
  - AES CMAC with key sizes 128,192 and 256 bits.
- 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 Digital signature creation using:
  - ECDSA with SHA-1, 224, 256, 384 and 512 with key sizes 192 to 512 bits over prime field curves
  - RSA signature (CRT) with SHA-1, 224, 256, 384 and 512 with key sizes 1024, 1536, 2048.
- o Digital signature verification using:
  - ECDSA with SHA-1, SHA-224 and SHA-256 with key sizes 192 to 512 bits.
  - RSA PKCS#1v1.5 with SHA-1, SHA-256 and SHA-512 with key sizes 1024, 1536, 2048
  - RSA PKCS#1-PSS with SHA-1, SHA-256 and SHA-512 with key sizes 1024, 1536, 2048
- 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 0.994.
- 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.EAC - Extended Access Control**

This TSF provides the Extended Access Control, authentication and session keys generation to be used by F.SM, as described in [TR\_03110]. It also provides the following management functions:

- o Maintain the roles: Document Verifier, CVCA, Domestic EIS, Foreign EIS
- o Limit the ability to update the CVCA Public key and CVCA Certificate to the Country Verifying Certification Authority
- o Limit the ability to update the date to CVCA, Document Verifier and Domestic Extended Inspection System.

### **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 the administrator defined number defined in FIA\_AFL.1/PACE the TSF will slow down further authentication attempts.

Only the eDigitalIdentity document holder after successful authentication can

- o resume the suspended PIN or PUK,
- o change the PIN,
- o unblock the blocked PIN using the PUK.

### **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 security function is also responsible for management operations during personalization phase. 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 Configure SM level for biometrical data access,
- o Load Chip Authentication keys in encrypted form,
- o Chip Authentication Key Generation,
- o Write Active Authentication Keys,
- o Enable and disable TSF Active Authentication,
- o Load of key data PACE in encrypted form,
- o Configure BAC deactivation mechanism,
- o Set TOE life cycle to Operational Use phase,
- o Write the PIN and PUK,

- o set the files that are allowed to be modified in phase 7,
- o Write the Document Security Object (SO d),
- o Write the initial CVCA Public Key, CVCA Certificate and Current Date.

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 transmission of user data in 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 keys after a successful authentication using F.CRYPTO - Cryptographic Support

**FCS\_CKM.1/CA** is met by F.EAC - Extended Access Control, EAC that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support

**FCS\_CKM.1/CAM** is met by F.PACE - Authentication using PACE that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support

**FCS\_CKM.1/CA\_DATA\_GEN** is met by F.PERS - MRTD Personalization that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support

**FCS\_CKM.1/GP** is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support

**FCS\_CKM.4** is met by F.CLR\_INFO - Clear Residual Information and F.SM - Secure Messaging that destroys the session keys upon closure of a secure messaging session.

**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/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/SIG\_VER** is met by F.EAC - Extended Access Control that uses F.CRYPTO - Cryptographic Support to provide digital signature verification.

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

**FCS\_COP.1/GP\_ENC** is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

**FCS\_COP.1/GP\_MAC** is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support 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\_KEY\_DEC** is met by F.PREP - MRTD Pre-personalization and F.PERS - MRTD Personalization that use F.CRYPTO - Cryptographic Support to perform key decryption.

**FCS\_COP.1/AA** is covered by F.AA - Active Authentication in association with F.CRYPTO - Cryptographic Support

**FCS\_RND.1** is met by F.CRYPTO - Cryptographic Support

#### **Class FIA Identification and Authentication**

**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.EAC - Extended Access Control 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.EAC - Extended Access Control that provide PACE and Extended Access Control.

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.EAC - Extended Access Control that provides Chip Authentication and Terminal Authentication as part of Extended Access Control.

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/EAC** is met by F.SM - Secure Messaging that ensures all messages are sent through secure messaging after chip and terminal authentication

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

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

**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\_API.1/CA** is met by F.EAC - Extended Access Control 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\_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.EAC - Extended Access Control and F.PACE - Authentication using PACE 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 and F.EAC - Extended Access Control using PACE and F.PERS - MRTD Personalization

**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\_DAU.1/AA** is met by F.AA - Active Authentication.

**FDP\_ITC.1/AA** is met by F.ACW - Access Control in Writing that verifies the write access based on authentication provided by F.AA - Active Authentication.

#### Class FTP Trusted Path/Channels

**FTP\_ITC.1/PACE** is met by F.SM - Secure Messaging that establishes a secure channel for communication as defined in F.EAC - Extended Access Control and 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\_MOF.1/BAC\_EXP** is met by F.EAC - Extended Access Control that implements date change to automatically deactivate BAC protocol

**FMT\_MOF.1/GP** is met by F.SM - Secure Messaging that provides secure messaging after authentication through F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization

**FMT\_MOF.1/AA** is met by F.PERS - MRTD Personalization

**FMT\_SMF.1** is met by F.EAC - Extended Access Control, F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that provide the required management functions and

CombICAO Applet v2.2  
in EAC with PACE configuration  
for French ID on Cosmo V9.1

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.EAC - Extended Access Control, 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\_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/PA** is met by F.PERS - MRTD Personalization.

**FMT\_MTD.1/CVCA\_INI** is met by F.ACW - Access Control in Writing that controls write access based on authentication provided by F.PERS - MRTD Personalization

**FMT\_MTD.1/CVCA\_UPD** is met by F.ACW - Access Control in Writing that controls write access based on authentication provided by F.EAC - Extended Access Control

**FMT\_MTD.1/DATE** is met by F.ACW - Access Control in Writing that controls write access based on authentication provided by F.EAC - Extended Access Control

**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/KEY\_READ** is met by F.ACR - Access Control in Reading that ensures the secret keys are never readable

**FMT\_MTD.1/PACE\_PWD** is met by F.PERS - MRTD Personalization

**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

**FMT\_MTD.1/BAC\_EXP** is met by 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/SM\_LVL** is met by F.PERS - MRTD Personalization that allows the personalization agent to provide configure the secure messaging level required to access DG.3 and DG.4

**FMT\_MTD.1/AA\_KEY\_READ** is met by F.ACR - Access Control in Reading that ensures the secret keys are never readable

**FMT\_MTD.1/AA\_KEY\_WRITE** is met by F.ACW - Access Control in Writing that controls write access for Active Authentication based on authentication provided by F.PERS - MRTD Personalization.

**FMT\_MTD.3** is met by F.EAC - Extended Access Control that implements terminal authentication.

**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.

#### 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

#### Additional SFRs as per Addendum

**FIA\_API.1/TOE** is met by F.PACE - Authentication using PACE that provides a means to identify the document holder via PACE Authentication

**FMT\_MTD.1/Initialize\_PIN** is met by F.PERS - MRTD Personalization.

**FMT\_MTD.1/Resume\_PIN** is met by F.PACE - Authentication using PACE.

**FMT\_MTD.1/Change\_PIN** is met by F.PACE - Authentication using PACE.

**FMT\_MTD.1/Unblock\_PIN** is met by F.PACE - Authentication using PACE.

### **8.2.2 Association tables of SFRs and TSS**

Security Functional Requirements	TOE Summary Specification
----------------------------------	---------------------------

<a href="#">FCS_CKM.1/DH_PACE</a>	<a href="#">F.PACE - Authentication using PACE, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_CKM.1/CA</a>	<a href="#">F.EAC - Extended Access Control, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_CKM.1/CAM</a>	<a href="#">F.CRYPTO - Cryptographic Support, F.PACE - Authentication using PACE</a>
<a href="#">FCS_CKM.1/CA_DATA_GEN</a>	<a href="#">F.PERS - MRTD Personalization, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_CKM.1/GP</a>	<a href="#">F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_CKM.4</a>	<a href="#">F.SM - Secure Messaging, F.CLR_INFO - Clear Residual Information</a>
<a href="#">FCS_COP.1/PACE_ENC</a>	<a href="#">F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_COP.1/PACE_MAC</a>	<a href="#">F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_COP.1/CA_ENC</a>	<a href="#">F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_COP.1/SIG_VER</a>	<a href="#">F.EAC - Extended Access Control, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_COP.1/CA_MAC</a>	<a href="#">F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_COP.1/CAM</a>	<a href="#">F.CRYPTO - Cryptographic Support, F.PACE - Authentication using PACE</a>
<a href="#">FCS_COP.1/GP_ENC</a>	<a href="#">F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_COP.1/GP_MAC</a>	<a href="#">F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_COP.1/GP_AUTH</a>	<a href="#">F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_COP.1/GP_KEY_DEC</a>	<a href="#">F.PERS - MRTD Personalization, F.CRYPTO - Cryptographic Support, F.PREP - MRTD Pre-personalization</a>
<a href="#">FCS_COP.1/AA</a>	<a href="#">F.AA - Active Authentication, F.CRYPTO - Cryptographic Support</a>
<a href="#">FCS_RND.1</a>	<a href="#">F.CRYPTO - Cryptographic Support</a>
<a href="#">FIA_UID.1/PACE</a>	<a href="#">F.EAC - Extended Access Control, F.PACE - Authentication using PACE, F.ACR - Access Control in Reading</a>
<a href="#">FIA_UAU.1/PACE</a>	<a href="#">F.ACR - Access Control in Reading, F.EAC - Extended Access Control, F.PACE - Authentication using PACE,</a>

	<a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.PREP - MRTD Pre-personalization</a>
<a href="#">FIA_UAU.4/PACE</a>	<a href="#">F.CLR INFO - Clear Residual Information</a>
<a href="#">FIA_UAU.5/PACE</a>	<a href="#">F.EAC - Extended Access Control</a> , <a href="#">F.PACE - Authentication using PACE</a> , <a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.PREP - MRTD Pre-personalization</a> , <a href="#">F.SM - Secure Messaging</a>
<a href="#">FIA_UAU.6/EAC</a>	<a href="#">F.SM - Secure Messaging</a>
<a href="#">FIA_UAU.6/PACE</a>	<a href="#">F.SM - Secure Messaging</a>
<a href="#">FIA_UAU.6/MP</a>	<a href="#">F.SM - Secure Messaging</a>
<a href="#">FIA_AFL.1/PACE</a>	<a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FIA_AFL.1/MP</a>	<a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.PREP - MRTD Pre-personalization</a>
<a href="#">FIA_API.1/CA</a>	<a href="#">F.EAC - Extended Access Control</a>
<a href="#">FIA_API.1/CAM</a>	<a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FDP_ACC.1/TRM</a>	<a href="#">F.ACR - Access Control in Reading</a> , <a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FDP_ACF.1/TRM</a>	<a href="#">F.ACR - Access Control in Reading</a> , <a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FDP_ACC.1/UPD_FILE</a>	<a href="#">F.ACR - Access Control in Reading</a> , <a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.EAC - Extended Access Control</a> , <a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FDP_ACF.1/UPD_FILE</a>	<a href="#">F.ACR - Access Control in Reading</a> , <a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.EAC - Extended Access Control</a> , <a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FDP_RIP.1</a>	<a href="#">F.CLR INFO - Clear Residual Information</a>
<a href="#">FDP_UCT.1/TRM</a>	<a href="#">F.SM - Secure Messaging</a>
<a href="#">FDP_UIT.1/TRM</a>	<a href="#">F.SM - Secure Messaging</a>
<a href="#">FDP_DAU.1/AA</a>	<a href="#">F.AA - Active Authentication</a>
<a href="#">FDP_ITC.1/AA</a>	<a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.AA - Active Authentication</a>
<a href="#">FTP_ITC.1/PACE</a>	<a href="#">F.SM - Secure Messaging</a> , <a href="#">F.PACE - Authentication using PACE</a> , <a href="#">F.EAC - Extended Access Control</a>
<a href="#">FTP_ITC.1/MP</a>	<a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.PREP - MRTD Pre-personalization</a> , <a href="#">F.SM - Secure Messaging</a>
<a href="#">FAU_SAS.1</a>	<a href="#">F.PREP - MRTD Pre-personalization</a>
<a href="#">FMT_MOF.1/BAC_EXP</a>	<a href="#">F.EAC - Extended Access Control</a>

<a href="#">FMT_MOF.1/GP</a>	<a href="#">F.SM - Secure Messaging</a> , <a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.PREP - MRTD Pre-personalization</a>
<a href="#">FMT_MOF.1/AA</a>	<a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_SMF.1</a>	<a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.PREP - MRTD Pre-personalization</a> , <a href="#">F.EAC - Extended Access Control</a> , <a href="#">F.SM - Secure Messaging</a>
<a href="#">FMT_SMR.1/PACE</a>	<a href="#">F.PACE - Authentication using PACE</a> , <a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.PREP - MRTD Pre-personalization</a> , <a href="#">F.EAC - Extended Access Control</a>
<a href="#">FMT_MTD.1/INI_ENA</a>	<a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.PREP - MRTD Pre-personalization</a>
<a href="#">FMT_MTD.1/INI_DIS</a>	<a href="#">F.ACR - Access Control in Reading</a> , <a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/PA</a>	<a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/CVCA_INI</a>	<a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/CVCA_UPD</a>	<a href="#">F.EAC - Extended Access Control</a> , <a href="#">F.ACW - Access Control in Writing</a>
<a href="#">FMT_MTD.1/DATE</a>	<a href="#">F.EAC - Extended Access Control</a> , <a href="#">F.ACW - Access Control in Writing</a>
<a href="#">FMT_MTD.1/CAPK</a>	<a href="#">F.PERS - MRTD Personalization</a> , <a href="#">F.ACW - Access Control in Writing</a>
<a href="#">FMT_MTD.1/KEY_READ</a>	<a href="#">F.ACR - Access Control in Reading</a>
<a href="#">FMT_MTD.1/PACE_PWD</a>	<a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/LCS_PERS</a>	<a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/BAC_EXP</a>	<a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/UPD_FILE</a>	<a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/SM_LVL</a>	<a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/AA_KEY_READ</a>	<a href="#">F.ACR - Access Control in Reading</a>
<a href="#">FMT_MTD.1/AA_KEY_WRITE</a>	<a href="#">F.ACW - Access Control in Writing</a> , <a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.3</a>	<a href="#">F.EAC - Extended Access Control</a>
<a href="#">FMT_LIM.1</a>	<a href="#">F.PHY - Physical Protection</a> , <a href="#">F.SS - Safe State Management</a>
<a href="#">FMT_LIM.2</a>	<a href="#">F.PHY - Physical Protection</a> , <a href="#">F.SS - Safe State Management</a>
<a href="#">FPT_EMS.1</a>	<a href="#">F.PHY - Physical Protection</a>
<a href="#">FPT_FLS.1</a>	<a href="#">F.SS - Safe State Management</a>

<a href="#">FPT_PHP.3</a>	<a href="#">F.PHY - Physical Protection</a> , <a href="#">F.SS - Safe State Management</a>
<a href="#">FPT_TST.1</a>	<a href="#">F.STST - Self Test</a>
<a href="#">FIA_API.1/TOE</a>	<a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FMT_MTD.1/Initialize PIN</a>	<a href="#">F.PERS - MRTD Personalization</a>
<a href="#">FMT_MTD.1/Resume PIN</a>	<a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FMT_MTD.1/Change PIN</a>	<a href="#">F.PACE - Authentication using PACE</a>
<a href="#">FMT_MTD.1/Unblock PIN</a>	<a href="#">F.PACE - Authentication using PACE</a>

**Table 21 SFRs and TSS - Coverage**

<a href="#">TOE Summary Specification</a>	<a href="#">Security Functional Requirements</a>
<a href="#">F.ACR - Access Control in Reading</a>	<a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FDP_ACC.1/TRM</a> , <a href="#">FDP_ACF.1/TRM</a> , <a href="#">FDP_ACC.1/UPD_FILE</a> , <a href="#">FDP_ACF.1/UPD_FILE</a> , <a href="#">FMT_MTD.1/INI_DIS</a> , <a href="#">FMT_MTD.1/KEY_READ</a> , <a href="#">FMT_MTD.1/AA_KEY_READ</a>
<a href="#">F.ACW - Access Control in Writing</a>	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FDP_ACF.1/TRM</a> , <a href="#">FDP_ACC.1/UPD_FILE</a> , <a href="#">FDP_ACF.1/UPD_FILE</a> , <a href="#">FDP_ITC.1/AA</a> , <a href="#">FMT_MTD.1/INI_ENA</a> , <a href="#">FMT_MTD.1/CVCA_INI</a> , <a href="#">FMT_MTD.1/CVCA_UPD</a> , <a href="#">FMT_MTD.1/DATE</a> , <a href="#">FMT_MTD.1/CAPK</a> , <a href="#">FMT_MTD.1/UPD_FILE</a> , <a href="#">FMT_MTD.1/AA_KEY_WRITE</a>
<a href="#">F.AA - Active Authentication</a>	<a href="#">FCS_COP.1/AA</a> , <a href="#">FDP_DAU.1/AA</a> , <a href="#">FDP_ITC.1/AA</a>
<a href="#">F.CLR_INFO - Clear Residual Information</a>	<a href="#">FCS_CKM.4</a> , <a href="#">FIA_UAU.4/PACE</a> , <a href="#">FDP_RIP.1</a>
<a href="#">F.CRYPTO - Cryptographic Support</a>	<a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_CKM.1/CAM</a> , <a href="#">FCS_CKM.1/CA_DATA_GEN</a> , <a href="#">FCS_CKM.1/GP</a> , <a href="#">FCS_COP.1/PACE_ENC</a> , <a href="#">FCS_COP.1/PACE_MAC</a> , <a href="#">FCS_COP.1/CA_ENC</a> , <a href="#">FCS_COP.1/SIG_VER</a> , <a href="#">FCS_COP.1/CA_MAC</a> , <a href="#">FCS_COP.1/CAM</a> , <a href="#">FCS_COP.1/GP_ENC</a> , <a href="#">FCS_COP.1/GP_MAC</a> , <a href="#">FCS_COP.1/GP_AUTH</a> , <a href="#">FCS_COP.1/GP_KEY_DEC</a> , <a href="#">FCS_COP.1/AA</a> , <a href="#">FCS_RND.1</a>
<a href="#">F.EAC - Extended Access Control</a>	<a href="#">FCS_CKM.1/CA</a> , <a href="#">FCS_COP.1/SIG_VER</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_UAU.5/PACE</a> , <a href="#">FIA_API.1/CA</a> , <a href="#">FDP_ACC.1/UPD_FILE</a> , <a href="#">FDP_ACF.1/UPD_FILE</a> , <a href="#">FDP_ITC.1/PACE</a> , <a href="#">FMT_MOF.1/BAC_EXP</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_MTD.1/CVCA_UPD</a> , <a href="#">FMT_MTD.1/DATE</a> , <a href="#">FMT_MTD.3</a>
<a href="#">F.PACE - Authentication using PACE</a>	<a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_CKM.1/CAM</a> , <a href="#">FCS_COP.1/CAM</a> , <a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UAU.1/PACE</a> , <a href="#">FIA_UAU.5/PACE</a> , <a href="#">FIA_AFL.1/PACE</a> , <a href="#">FIA_API.1/CAM</a> , <a href="#">FDP_ACC.1/TRM</a> , <a href="#">FDP_ACF.1/TRM</a> , <a href="#">FDP_ACC.1/UPD_FILE</a> , <a href="#">FDP_ACF.1/UPD_FILE</a> , <a href="#">FDP_ITC.1/PACE</a> , <a href="#">FMT_SMR.1/PACE</a> , <a href="#">FIA_API.1/TOE</a> , <a href="#">FMT_MTD.1/Resume_PIN</a> , <a href="#">FMT_MTD.1/Change_PIN</a> , <a href="#">FMT_MTD.1/Unblock_PIN</a>

<a href="#">F.PERS - MRTD Personalization</a>	<a href="#">FCS CKM.1/CA DATA GEN</a> , <a href="#">FCS CKM.1/GP</a> , <a href="#">FCS COP.1/GP AUTH</a> , <a href="#">FCS COP.1/GP KEY DEC</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA AFL.1/MP</a> , <a href="#">FDP ACC.1/UPD FILE</a> , <a href="#">FDP ACF.1/UPD FILE</a> , <a href="#">FTP ITC.1/MP</a> , <a href="#">FMT MOF.1/GP</a> , <a href="#">FMT MOF.1/AA</a> , <a href="#">FMT SMF.1</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/INI DIS</a> , <a href="#">FMT MTD.1/PA</a> , <a href="#">FMT MTD.1/CVCA INI</a> , <a href="#">FMT MTD.1/CAPK</a> , <a href="#">FMT MTD.1/PACE PWD</a> , <a href="#">FMT MTD.1/LCS PERS</a> , <a href="#">FMT MTD.1/BAC EXP</a> , <a href="#">FMT MTD.1/UPD FILE</a> , <a href="#">FMT MTD.1/SM LVL</a> , <a href="#">FMT MTD.1/AA KEY WRITE</a> , <a href="#">FMT MTD.1/Initialize PIN</a>
<a href="#">F.PHY - Physical Protection</a>	<a href="#">FMT LIM.1</a> , <a href="#">FMT LIM.2</a> , <a href="#">FPT EMS.1</a> , <a href="#">FPT PHP.3</a>
<a href="#">F.PREP - MRTD Pre-personalization</a>	<a href="#">FCS CKM.1/GP</a> , <a href="#">FCS COP.1/GP AUTH</a> , <a href="#">FCS COP.1/GP KEY DEC</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA AFL.1/MP</a> , <a href="#">FTP ITC.1/MP</a> , <a href="#">FAU SAS.1</a> , <a href="#">FMT MOF.1/GP</a> , <a href="#">FMT SMF.1</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/INI ENA</a>
<a href="#">F.SM - Secure Messaging</a>	<a href="#">FCS CKM.4</a> , <a href="#">FCS COP.1/PACE ENC</a> , <a href="#">FCS COP.1/PACE MAC</a> , <a href="#">FCS COP.1/CA ENC</a> , <a href="#">FCS COP.1/CA MAC</a> , <a href="#">FCS COP.1/GP ENC</a> , <a href="#">FCS COP.1/GP MAC</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA UAU.6/EAC</a> , <a href="#">FIA UAU.6/PACE</a> , <a href="#">FIA UAU.6/MP</a> , <a href="#">FDP UCT.1/TRM</a> , <a href="#">FDP UIT.1/TRM</a> , <a href="#">FTP ITC.1/PACE</a> , <a href="#">FTP ITC.1/MP</a> , <a href="#">FMT MOF.1/GP</a> , <a href="#">FMT SMF.1</a>
<a href="#">F.SS - Safe State Management</a>	<a href="#">FMT LIM.1</a> , <a href="#">FMT LIM.2</a> , <a href="#">FPT FLS.1</a> , <a href="#">FPT PHP.3</a>
<a href="#">F.STST - Self Test</a>	<a href="#">FPT TST.1</a>

**Table 22 TSS and SFRs - Coverage**

## 9 GLOSSARY AND ACRONYMS

### 9.1 Glossary

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the eDigitalIdentity document's chip to produce Terminal Certificates with the correct certificate effective date, see [TR_03110].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a eDigitalIdentity document and a terminal as required by [ICAO_TR_SAC], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SOD and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
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 eDigitalIdentity document's chip proves and the inspection system verifies the identity and authenticity of the eDigitalIdentity document's chip as part of a genuine eDigitalIdentity 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 eDigitalIdentity document's chip to store the Initialization Data and Pre-personalisation Data.
Authenticity	Ability to confirm the eDigitalIdentity document and its data elements on the eDigitalIdentity 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 eDigitalIdentity 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)	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 eDigitalIdentity document presenter as the eDigitalIdentity document holder (for ePassport: by comparing the real biometric data (face) of the eDigitalIdentity document presenter with the stored biometric data (DG2) of the eDigitalIdentity document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the eDigitalIdentity document Issuer through the Document Verifier of receiving state to read a subset of data stored on the eDigitalIdentity document.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the eDigitalIdentity document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical eDigitalIdentity document.

Term	Definition
Biographical data (biodata)	The personalised details of the eDigitalIdentity document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a eDigitalIdentity document. [ICAO_9303]
Biometric reference data	Data stored for biometric authentication of the eDigitalIdentity document holder in the eDigitalIdentity 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 (KPU CSCA) issued by Country Signing Certification Authority stored in the inspection system.
Country Signing Certification Authority (CSCA)	<p>An organisation enforcing the policy of the eDigitalIdentity document Issuer with respect to confirming correctness of user and TSF data stored in the eDigitalIdentity document. The CSCA represents the country specific root of the PKI for the eDigitalIdentity 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 eDigitalIdentity document Issuer with respect to protection of Identification user data stored in the eDigitalIdentity 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>

Term	Definition
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
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.
Document Details Data	Data printed on and electronically stored in the eDigitalIdentity 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 eDigitalIdentity 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 eDigitalIdentity 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>
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 eDigitalIdentity 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 eDigitalIdentity document Issuer und a foreign CVCA ensuring enforcing the eDigitalIdentity document Issuer's privacy policy).55 56</p>
Eavesdropper	A threat agent with high attack potential reading the communication between the eDigitalIdentity document's chip and the inspection system to gain the data on the eDigitalIdentity 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]

Term	Definition
EDigitalIdentity 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 Identification 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 eDigitalIdentity document (MRTD). See [TR_03110].
Extended Access Control	Security mechanism identified in [ICAO_9303] by which means the eDigitalIdentity document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organisation to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO_9303]
Global Interoperability	1.1.1 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 eDigitalIdentity document material during the IC manufacturing and the delivery process to the eDigitalIdentity document manufacturer.

Term	Definition
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_9303]
Improperly document person	A person who travels, or attempts to travel with: (a) an expired eDigitalIdentity document or an invalid visa; (b) a counterfeit, forged or altered eDigitalIdentity document or visa; (c) someone else's eDigitalIdentity document or visa; or (d) no eDigitalIdentity 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 eDigitalIdentity document's material (IC identification data).
Inspection	The act of a State examining an eDigitalIdentity document presented to it by a traveller (the eDigitalIdentity 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 eDigitalIdentity document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as eDigitalIdentity document holder.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The eDigitalIdentity document's chip is an integrated circuit.
Integrity	Ability to confirm the eDigitalIdentity document and its data elements on the eDigitalIdentity document's chip have not been altered from that created by the issuing State or Organisation
Issuing Organisation	Organisation authorized to issue an official eDigitalIdentity document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]
Issuing State	The Country issuing the eDigitalIdentity 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 eDigitalIdentity document's chip.

Term	Definition
Logical eDigitalIdentity document	<p>Data of the eDigitalIdentity 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)</p> <ol style="list-style-type: none"> <li>1.personal data of the eDigitalIdentity document holder</li> <li>2.the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),</li> <li>3.the digitized portraits (EF.DG2),</li> <li>4.the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and</li> <li>5.the other data according to LDS (EF.DG5 to EF.DG16).</li> <li>6.EF.COM and EF.SOD</li> </ol>
Machine Readable EDigitalIdentity document (MRTD)	<p>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]</p>
Machine Readable Zone (MRZ)	<p>Fixed dimensional area located on the front of the eDigitalIdentity document or MRP Data Page or, in the case of the TD1, the back of the eDigitalIdentity document, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303]</p> <p>The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.</p>
Machine-verifiable biometrics feature	<p>A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a eDigitalIdentity document in a form that can be read and verified by machine. [ICAO_9303]</p>
Manufacturer	<p>Generic term for the IC Manufacturer producing integrated circuit and the eDigitalIdentity document Manufacturer completing the IC to the eDigitalIdentity 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 eDigitalIdentity document Manufacturer using this role Manufacturer.</p>

Term	Definition
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"> <li>- Certificate Profile Identifier,</li> <li>- Certificate Authority Reference,</li> <li>- Certificate Holder Reference,</li> <li>- Certificate Holder Authorisation Template,</li> <li>- Certificate Effective Date,</li> <li>- Certificate Expiration Date.</li> </ul>
ePassport application	<p>Non-executable data defining the functionality of the operating system on the IC as the eDigitalIdentity document's chip. It includes</p> <ul style="list-style-type: none"> <li>•the file structure implementing the LDS [ICAO_9303],</li> <li>•the definition of the Identification user data, but does not include the Identification user data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and</li> <li>•the TSF Data including the definition the authentication data but except the authentication data itself.</li> </ul>
Optional biometric reference data	<p>Data stored for biometric authentication of the eDigitalIdentity document holder in the eDigitalIdentity 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.</p>
Passive authentication	<p>(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.</p>
PACE Password	<p>A password needed for PACE authentication, e.g. CAN or MRZ.</p>
Personalization	<p>The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the eDigitalIdentity document. This may also include the optional biometric data collected during the "Enrolment" (cf. sec. 1.2, TOE life-cycle, Phase 3, Step 6).</p>

Term	Definition
Personalization Agent	<p>An organisation acting on behalf of the eDigitalIdentity document Issuer to personalise the eDigitalIdentity document for the eDigitalIdentity document holder by some or all of the following activities:</p> <ul style="list-style-type: none"> <li>(i) establishing the identity of the eDigitalIdentity document holder for the biographic data in the eDigitalIdentity document,</li> <li>(ii) enrolling the biometric reference data of the eDigitalIdentity document holder,</li> <li>(iii) writing a subset of these data on the physical eDigitalIdentity document (optical personalisation) and storing them in the eDigitalIdentity document (electronic personalisation) for the eDigitalIdentity document holder as defined in [TR_03110],</li> <li>(iv) writing the document details data,</li> <li>(v) writing the initial TSF data,</li> <li>(vi) signing the Document Security Object defined in [ICAO_9303] (in the role of DS).</li> </ul> <p>Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the eDigitalIdentity document Issuer. 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"> <li>(i) individual-related data (biographic and biometric data) of the eDigitalIdentity document holder,</li> <li>(ii) dedicated document details data and</li> <li>(iii) dedicated initial TSF data (incl. the Document Security Object).</li> </ul> <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	<p>TSF data used for authentication proof and verification of the Personalisation Agent.</p>
Personalization Agent Key	<p>Cryptographic authentication key used (i) by the Personalisation Agent to prove his identity and to get access to the logical eDigitalIdentity document and (ii) by the eDigitalIdentity 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/EAC.</p>

Term	Definition
Physical eDigitalIdentity document	<p>EDigitalIdentity 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"> <li>1.biographical data,</li> <li>2.data of the machine-readable zone,</li> <li>3.photographic image and</li> <li>4.other data.</li> </ol>
Pre-Personalisation	<p>Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the eDigitalIdentity document Application (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 5)</p>
Pre-personalization Data	<p>Any data that is injected into the non-volatile memory of the TOE by the eDigitalIdentity document Manufacturer (Phase 2) for traceability of non-personalised eDigitalIdentity 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.</p>
Pre-personalized eDigitalIdentity document's chip	<p>eDigitalIdentity document's chip equipped with a unique identifier.</p>
Receiving State	<p>The Country to which the traveller is applying for entry. [ICAO_9303]</p>
reference data	<p>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.</p>
RF-terminal	<p>A device being able to establish communication with an RF-chip according to ISO/IEC 14443.</p>
secondary image	<p>A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO_9303]</p>
Secure messaging in encrypted/combined mode	<p>Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4</p>
Service Provider	<p>An official organisation (inspection authority) providing inspection service which can be used by the eDigitalIdentity document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.</p>
Skimming	<p>Imitation of the inspection system to read the logical eDigitalIdentity document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.</p>
Standard Inspection Procedure	<p>A specific order of authentication steps between an eDigitalIdentity 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.</p>

Term	Definition
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 eDigitalIdentity document and the related value presented to the terminal by the eDigitalIdentity 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 eDigitalIdentity document using a shared password (CAN or MRZ).</p>
Terminal Authorization	<p>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.</p>
Terminal Authorisation Level	<p>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.</p>
TOE tracing data	<p>Technical information about the current and previous locations of the eDigitalIdentity document gathered by inconspicuous (for the eDigitalIdentity document holder) recognising the eDigitalIdentity document.</p>
EDigitalIdentity document	<p>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 eDigitalIdentity document").</p>
EDigitalIdentity document Holder	<p>The rightful holder of the eDigitalIdentity document for whom the issuing State or Organisation personalised the eDigitalIdentity document.</p>
EDigitalIdentity document's Chip	<p>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.</p>
EDigitalIdentity document's Chip Embedded Software	<p>Software embedded in a eDigitalIdentity document's chip and not being developed by the IC Designer. The eDigitalIdentity document's chip Embedded Software is designed in Phase 1 and embedded into the eDigitalIdentity document's chip in Phase 2 of the TOE life-cycle.</p>
EDigitalIdentity document presenter	<p>Person presenting the eDigitalIdentity document to the inspection system and claiming the identity of the eDigitalIdentity document holder.</p>
TSF data	<p>Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC_1]).</p>

Term	Definition
Unpersonalised eDigitalIdentity document	The eDigitalIdentity document that contains the eDigitalIdentity document chip holding only Initialization Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
Identification user data	<p>All data (being not authentication data)</p> <p>(i) stored in the context of the ePassport application of the eDigitalIdentity 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 Identification 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>EAC</i>	Extended Access Control
<i>CPS</i>	Common Personalization System
<i>EF</i>	Elementary File
<i>ICCSN</i>	Integrated Circuit Card Serial Number.
<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

### Common Criteria

[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.
[CC_EM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

### Protection Profiles

[PP_0002]	PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001  Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002
[PP_IC]	Security IC Platform Protection Profile, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007
[PP_BAC]	Machine readable eDigitalIdentity documents with "ICAO Application", Basic Access control – BSI-PP-0055 v1.10 25th march 2009
[PP_EAC]	Common Criteria Protection Profile Machine Readable EDigitalIdentity document with "ICAO Application", Extended Access Control, BSI-PP-0056, Version 1.10, 25 <sup>th</sup> March 2009
[PP_PACE]	Common Criteria Protection Profile Machine Readable EDigitalIdentity document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, V1.0 2 <sup>nd</sup> November 2011
[PP_EACwPACE]	Common Criteria Protection Profile Machine Readable EDigitalIdentity document with "ICAO Application", Extended Application Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5 <sup>th</sup> December 2012

### Platform

[PTF_CERT]	ANSSI-CC-2020/07-R01
[ST_PTF]	FQR 110 9395 Ed9 Public Security Target Cosmo v9.1
[PTF_AGD1]	ID-One COSMO V9.1 Application Loading Protection Guidance, FQR 110 9238 Ed 1

[PTF_AGD2]	ID-One COSMO V9.1 Security Recommendations, FQR 110 9237 Ed 3
[PTF_AGD3]	ID-One Cosmo V9.1 platform - Javadoc, FQR 110 9242 Ed 1
[PTF_AGD4]	JCVM Patch FQR 110 8805 Ed 2
[PTF_AGD5]	Platform Flash Generation FQR 110 9402 Ed 1– 27/11/2019
[PTF_AGD_OPE]	ID-One COSMO V9.1, Reference Guide FQR 110 9200 Ed 8
[PTF_AGD_PRE]	ID-One COSMO V9.1 Pre-Perso Guide, FQR 110 9208 Ed 9
[PTF_AGD_SEC_AC]	Secure acceptance and delivery of sensitive elements FQR 110 8921 Ed 1 – 24/09/2018
[Applet_Perso_Guide]	CombICAO Applet v2.1and v2;2 – Perso Guide, FQR 220 1455 Ed 8
[Applet_User_Guide]	CombICAO Applet v2.1 and v2.2– User Guide, FQR 220 1456 Ed 7

## ICAO

[ICAO_9303]	ICAO Doc 9303, Machine Readable EDigitalIdentity documents, Seventh Edition, 2015 – Security Mechanisms for MRTDs
[ICAOT]	INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)
[ICAO_TR_SAC ]	International Civil Aviation Organization, ICAO MACHINE READABLE EDIGITALIDENTITY DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable EDigitalIdentity documents, Version 1.00, November 2010

## ISO

[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
[ISO_9796-2]	ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function
[ISO_15946]	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves

## INTERNAL

[ALC_KM]	Key management for Flash code, I CRD13 2 CRD 512 03, January 2016
[ALC_SCT]	ID division: sensitive code transfer, I/R&D/2/SQA 515 01, March 2010
[ALC_STM]	Secure transfer of masks, I CRD13 2 CRD 507 04, January 2012

## Other

[TR_03110]	Technical Guideline Advanced Security Mechanisms for Machine Readable EDigitalIdentity documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[TR_03111]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009
[FIPS_180_2 ]	FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002
[FIPS_46_3]	FIPS 46-3, Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard (DES), 1999 October 25
[FIPS_186_3 ]	FIPS 186-3, Federal Information Processing Standards Publication (FIPS PUB) 186-3, Digital Signature Standard (DSS), June 2009
[FIPS_197]	FIPS 197, Federal Information Processing Standards Publication (FIPS PUB 197), Advanced Encryption Standard (AES)
[NIST_800_3 8A]	NIST Special Publication 800-38A: 2001, <i>Recommendation for Block Cipher Modes of Operation: Methods and Techniques</i> , December 2001
[NIST_800_3 8B]	NIST Special Publication 800-38B: 2005, <i>Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication</i> , May 2005
[GPC_SPE_0 34]	GlobalPlatform – Card Specification – Version 2.2.1 – Public Release, January 2011
[GPC_SPE_0 14]	GlobalPlatform Card Technology - Secure Channel Protocol '03', Card Specification v2.2 – Amendment D Version 1.1.1 - Public Release July 2014
[RGS2_B1]	Référentiel Général de Sécurité version 2.0 – Annexe B1 – Mécanismes cryptographiques – Règles et recommandations concernant le choix et lme dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014.
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993
[X9.62]	AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 september 1998