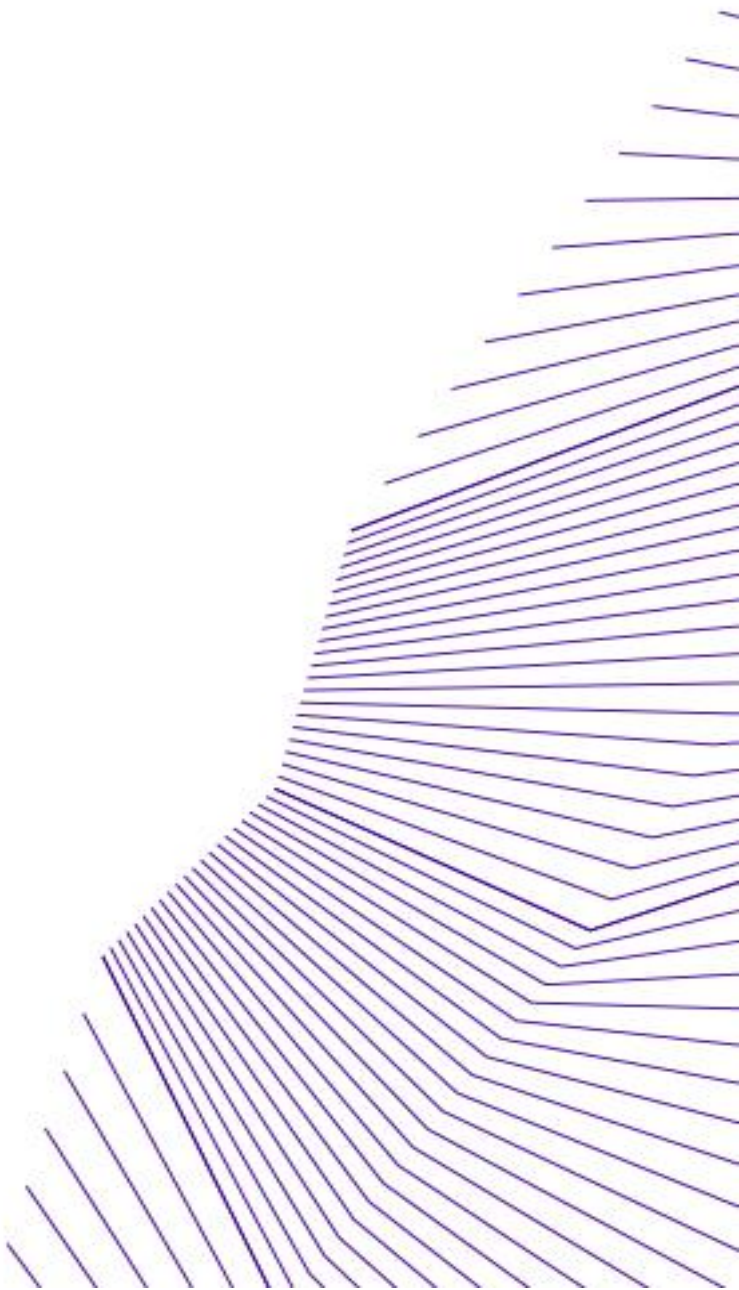
IDEMIA

# IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option

# Public Security Target

ISSUE: 6.0



| DOCUMENT REVISION HISTORY | | | |
|---|---|---|---|
| **Issue** | **Date** | **Author** | **Purpose** |
| 1 | 25/10/2023 | IDEMIA | Creation of the document |
| 2 | 30/10/2023 | IDEMIA | Update with PACE-CAM product identification |
| 3 | 08/11/2023 | IDEMIA | Issue |
| 4 | 13/11/2023 | IDEMIA | Issue for publication |
| 5 | 20/11/2023 | IDEMIA | Issue with AGD_PRE Ed4. |
| 6 | 21/11/2023 | IDEMIA | Issue with AGD_PRE Ed5. |
| | | | |

# TABLE OF CONTENTS

# 1 GENERAL

## 1.1 Introduction

This security target describes the security needs induced by the IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option product.

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,
- 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,
- describe the security objectives of the TOE and its supported environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the product active phases,
- specify the security requirements including the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment,
- describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements,
- 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

IDmove v5 product is a multi-configuration MRTD product. It provides four configurations, which are:

- IDmove v5 on SCR404U in BAC configuration with AA and/or CA in option,
- IDmove v5 on SCR404U in EAC configuration with AA in option,
- IDmove v5 on SCR404U in EAC with PACE configuration with AA in option,
- **IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option.**

IDmove v5 on SCR404U Operating System is embedded in the components identified in [IC_ST] manufactured by IDEMIA.

**Mutatis mutandis**, the product may also be used as an ISO driving license, compliant to ISO/IEC 18013 or ISO/IEC TR 19446 supporting PACE, AA and CA, as both applications (MRTD and IDL) share the same protocols and data structure organisation.
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.

# 2 ST INTRODUCTION

## 2.1 ST reference and TOE reference

### 2.1.1 ST reference

| | |
|---|---|
| ***Title*** | IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option – Public Security Target |
| ***Version*** | 6.0 |
| ***Authors*** | IDEMIA |
| ***Publication date*** | 21/11/2023 |
| ***CC version*** | 3.1 revision 5 |
| ***EAL*** | EAL5 augmented with:<br>• ADV_IMP.2,<br>• ADV_INT.3,<br>• ADV_TDS.5,<br>• ALC_CMC.5,<br>• ALC_TAT.3,<br>• ALC_FLR.3,<br>• ALC_DVS.2,<br>• ATE_COV.3,<br>• ATE_FUN.2,<br>• AVA_VAN.5. |
| ***PP*** | See [PP_PACE] |

Table 1- ST reference

### 2.1.2 TOE reference

| | |
|---|---|
| ***Developer name*** | IDEMIA |
| ***Product name*** | IDmove v5 on SCR404U |
| ***TOE name*** | IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option |
| ***TOE identification*** | |
| ***Integrated Circuit*** | See Table 3 - IC identification |
| ***Embedded Software*** | Operating System Commercial Version SAAAAR: **098912**<br>Operating System Unique Identifier: **B7BC0108** with PACE-CAM or<br>**E48C0108** without PACE-CAM |
| ***User Guidance documentation*** | Preparative Documentation: **FQR 110 A110 Ed5 and FQR 110 A17E Ed1**<br>Operational Documentation: **FQR 110 A111 Ed3** |

Table 2 - TOE reference

### 2.1.3 IC identification

| | |
|---|---|
| ***IC certificates*** | See [IC_CERT] |
| ***IC public Security Target*** | See [IC_ST] |

Table 3 - IC identification

### 2.1.4 TOE Delivered Parts

| ***Part of the TOE*** | ***Format*** | ***Delivery Method*** | ***Comment*** |
|---|---|---|---|
| Integrated Circuit | See [IC_ST] | | |
| Embedded Software | Specific file containing APDUs allowing the embedded software loading. | Encrypted file in email | The file contains all commands to be used to load the embedded software. These commands are already formatted to ensure the integrity and the confidentiality of the embedded software. |
| Optional Updated Code | Specific file containing APDUs allowing the additional code loading | Encrypted file in email | If necessary optional Updated package can be delivered. The file contains all updated packages for the Embedded software. The embedded software Update mechanism ensures the integrity and the confidentiality of the additional code. The updated code need to be Common Criteria certified. |
| Final TOE | ID1 cards, wafers, modules, inlays, ecovers, eDatapage or passeports | Secure transport | Customer can ask for rising of the security of the delivery method. |
| User Guidance Documentation | Personalized pdf | Encrypted file in email | - |

Table 4- TOE delivery parts

## 2.2 TOE overview

### 2.2.1 Usage and major security features of the TOE

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

For this protection profile the travel document is viewed as unit of:

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

(ii) the **logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO_9303] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document holder
(a) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
(b) the digitized portraits (EF.DG2),
(c) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
(d) the other data according to LDS (EF.DG5 to EF.DG16) and
(e) the Document Security Object (SOD).

The issuing State or Organisation implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.
The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [ICAO_9303]. These security measures can include the binding of the travel document's chip to the travel document.

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

The ICAO defines in [ICAO_9303] the secure methods Passive Authentication and the optional advance security methods Password Authenticated Connection Establishment (also defined in the former reference [ICAO_9303]) and alternatively Basic Access Control to the logical travel document. Other security methods are defined such as Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure.

This protection profile addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This protection profile addresses the Chip Authentication Version 1 described in [ICAO_9303] as an alternative to the Active Authentication stated in [ICAO_9303].
If BAC is supported by the TOE, the travel 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).

As defined in [ICAO_9303] in part 11 §6.1, Active Authentication authenticates the contactless IC by signing a challenge sent by the IFD (inspection system) with a private key known only to the IC. For this purpose the contactless IC contains its own Active Authentication Key pair (KPrAA and KPuAA). A hash representation of Data Group 15 (Public Key (KPuAA) info) is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key (KPrAA) is stored in the contactless IC's secure memory. By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SOD)) in combination with the challenge response, using the eMRTD's Active Authentication Key Pair (KPrAA and KPuAA), the inspection system verifies that the Document Security Object (SOD) has been read from the genuine contactless IC, stored in the genuine eMRTD.

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

For the PACE protocol according to [ICAO_9303], the following steps shall be performed:

(i) the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN, PIN data and transmits the encrypted nonce together with the domain parameters to the terminal.

(ii) he terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data, or processing PIN or PUK data provided by the document holder.

(iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [ICAO_9303].

The electronic document holder can control access by consciously presenting his electronic document and/or by entering his secret PIN using:

- PACE PIN/PUK suspend/resume mechanism according to [TR-03110-2] in case of TOE communication over the contactless interface;
- PIN/PUK verify and PIN reset;

The protection profile requires the TOE to implement the Password Authenticated Connection Establishment (PACE) as defined in [ICAO_9303]. Chip Authentication and Active Authentication may be also used with the TOE.

As defined in [ICAO_9303] in part 11 §6.1, Active Authentication authenticates the contactless IC by signing a challenge sent by the IFD (inspection system) with a private key known only to the IC. For this purpose the contactless IC contains its own Active Authentication Key pair (KPrAA and KPuAA). A hash representation of Data Group 15 (Public Key (KPuAA) info) is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key (KPrAA) is stored in the contactless IC's secure memory. By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SOD)) in combination with the challenge response, using the eMRTD's Active Authentication Key Pair (KPrAA and KPuAA), the inspection system verifies that the Document Security Object (SOD) has been read from the genuine contactless IC, stored in the genuine eMRTD.

The Chip Authentication defined in [ICAO_9303] and [TR_03110] is a security feature which is optionally supported by the TOE. The Chip Authentication prevents data traces described in [ICAO_9303]. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document

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

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

The **PACE-CAM** Chip Authentication Mapping is an optional new mapping for PACE which extends the Generic Mapping that integrates Chip Authentication into the PACE protocol. This mapping combines PACE and Chip Authentication into one protocol PACE-CAM, which allows faster execution than the separate protocols (i.e. PACE + Chip Authentication + Terminal Authentication).
The chip computes the Chip Authentication Data using the chip's static private key then sends this data to the terminal. The terminal verifies the authenticity of the chip using the recovered Chip Authentication Data. As an additional PACE mode, Chip Authentication Mapping (PACE-CAM) defined in [ICAO_9303] part 11, which combines PACE-GM with Chip Authentication into a single protocol is optionally configured.
The PACE-CAM protocol is an optional protocol where the associated code can be removed.

**Mutatis mutandis**, the TOE may also be used as an ISO driving license, compliant to [ISO_18013] or ISO/IEC TR 19446 supporting PACE, EAC and AA, as both applications (MRTD and IDL) share the same protocols and data structure organisation. 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_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 | MRZ or SAI (Scanning area identifier) |
| Traveler | Holder |

Finally, the TOE can be updated in post-emission. The mechanism allows to protect the integrity and confidentiality of product data loaded and data already in the product as established in the PP module [PP_0090]. The mechanism is called Update Mechanism in this document.

### 2.2.2 TOE type

The TOE is the contactless and/or contact integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Password Authenticated Connection Establishment, the Basic Access Control, the Active Authentication and the Chip Authentication according to [ICAO_9303].

The TOE comprises at least:

- the circuitry of the MRTD's chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application,
- the associated guidance documentation.

**Note:** The antenna and the form factor are not part of the TOE as they do not have any impact on the security.

### 2.2.3 TOE life cycle

#### 2.2.3.1 Life cycle overview

The following table presents the TOE subjects and the corresponding responsible:

| **Subject** | | **Responsible** |
|---|---|---|
| **IC developer** | | IDEMIA |
| **TOE developer** | | IDEMIA |
| **Manufacturer** | IC manufacturer | IDEMIA or identified actors in [IC_ST] |
| | MRTD packaging responsible | IDEMIA or another agent |
| | Embedded software loading responsible | IDEMIA or identified actors in [IC_ST] |
| | Pre-personalization Agent | IDEMIA or another agent |
| **Personalization Agent** | | IDEMIA or another agent |

Table 5 - Roles identification on the life cycle

Several life cycles are available, depending when the Flash Code is loaded and who loads the Flash Code. 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:

Scheme 1, MRTD chip Embedded Software loaded by the IC Manufacturer in step 3:

| ***Phase*** | ***Step*** | ***Subject*** | ***Emb. Sw. loading*** | ***Covered by*** | ***Sites*** |
|---|---|---|---|---|---|
| 1 - Development | 1 | IC developer | × | IC certification | IC certification |
| | 2 | TOE developer | × | ALC R&D sites | Pessac and Courbevoie |
| 2 - Manufacturing | 3 | IC manufacturer | × | IC certification | IC manufacturer site |
| | | Embedded software loading responsible | ✓ | | |
| | **TOE delivery point** | | | | |
| | 4 | MRTD packaging responsible | × | | Packaging centre |
| | 5 | Pre-personalization agent | × | AGD_PRE | |
| 3 - Personalization | 6 | Personalization agent | × | AGD_PRE | |
| 4 - Operational Use | 7 | End user | × | AGD_OPE | |

Table 6 - Subjects identification following life cycle steps – Scheme 1

For the scheme 1, the OS loading is done at IC manufacturer site (audited). Once OS loaded, the TOE is auto-protected. Thus, the delivery to other entities (IDEMIA or any other not audited site) is a standard delivery.

Scheme 2, MRTD chip Embedded Software loaded by the Flash Loader with the optional Package 1 (See [IC_ST]) in step 4 before TOE delivery point:

| ***Phase*** | ***Step*** | ***Subject*** | ***Emb. Sw. loading*** | ***Covered by*** | ***Sites*** |
|---|---|---|---|---|---|
| 1 - Development | 1 | IC developer | × | IC certification | IC developer site |
| | 2 | TOE developer | × | ALC R&D sites | Pessac and Courbevoie |
| 2 - Manufacturing | 3 | IC manufacturer | × | IC certification | IC manufacturer site |
| | 4 | MRTD packaging responsible | × | | Packaging centre |
| | | Embedded software loading responsible | ✓ | ALC Embedded software loading centre | IDEMIA audited sites |
| | **TOE delivery point** | | | | |
| | 5 | Pre-personalization agent | × | AGD_PRE | |
| 3 - Personalization | 6 | Personalization agent | × | AGD_PRE | |
| 4 - Operational Use | 7 | End user | × | AGD_OPE | |

Table 7 - Subjects identification following life cycle steps – Scheme 2

For the scheme 2, the IC is delivered to IDEMIA after IC manufacturing (audited). Then the OS loading is done at one audited IDEMIA site. Once OS loaded, the TOE is auto-protected. The next delivery to any entity is done following ALC_DEL.

#### 2.2.3.2 Life cycle phases

The following text was extracted from [PP_PACE]. Due to the previous specified life cycles and to the technology of the IC, some interpretations have to be done by the reader of this ST. The table below indicates how terms shall be read:

| **Term in** [PP_PACE] | **Meaning in this ST** |
|---|---|
| Software developer | TOE developer |
| non-volatile non-programmable memory(ies) | Part of the Flash memory where the Flash Loader and the OS are loaded. This memory is programmable by the IC manufacturer or using the Flash Loader. Once the Flash Loader is blocked, this memory is Read Only Memory |
| ROM | |
| non-volatile programmable memory(ies) | Part of the Flash memory where initialization data and user data are written. |

The TOE life cycle is described in terms of the four life cycle phases and subdivided into 7 steps (with respect to the [PP_IC]).

##### 2.2.3.2.1 Phase 1 “Development”

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

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

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

Note: the Embedded Software in the Flash memory is securely delivered to the IC manufacturer. For details, please refer to ALC and in particular to [ALC_STM].

##### 2.2.3.2.2 Phase 2 “Manufacturing”

(Step3) In a first step the TOE integrated circuit is produced containing the MRTD’s IC Dedicated Software and the parts of the MRTD’s chip Embedded Software in the Flash memory. The IC manufacturer writes the IC Identification Data onto the IC to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance Flash memory). The manufacturer can use the update mechanism to add a Update Package.

Note: If scheme 2 is applied, the TOE integrated circuit is produced containing IC dedicated software. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

(Step4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

(Step5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD’s chips with pre-personalization Data.

*Application Note (1 in* [PP_PACE]*)*: Creation of the application implies the creation of MF and ICAO.DF.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Also this step authorizes to update the OS.

#### 2.2.3.2.3 Phase 3 “Personalization of the MRTD”

(Step6) The personalization of the MRTD includes (i) the survey of the MRTD holder’s biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object and file for the TOE configuration such as (but not limited to) the PACE parameters and keys, CA keys and TA trust point.

The signing of the Document security object by the Document Signer [ICAO_9303] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

*Application note (2 in* [PP_PACE]*)***:** The TSF data comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the control PACE Key.

*Application note:* This security target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [ICAO_9303]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

Also this step authorizes to update the OS.

#### 2.2.3.2.4 Phase 4 “Operational Use”

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

*Application note*: The authorized Personalization Agents might be allowed to add data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.

*Application note (4 in* [PP_PACE]*)***:** The intention of this security target is to consider at least the Phase 1 and parts of Phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase 2 or later. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.
Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the “Operational Use” (phase 4) have to be considered in the product evaluation process under AGD assurance

class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

Also this step authorizes to update the OS.

### 2.2.4 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 TOE Architecture

The TOE is composed of an IC and some software components as presented in Figure 1. Each part of the TOE is presented in the following chapters.

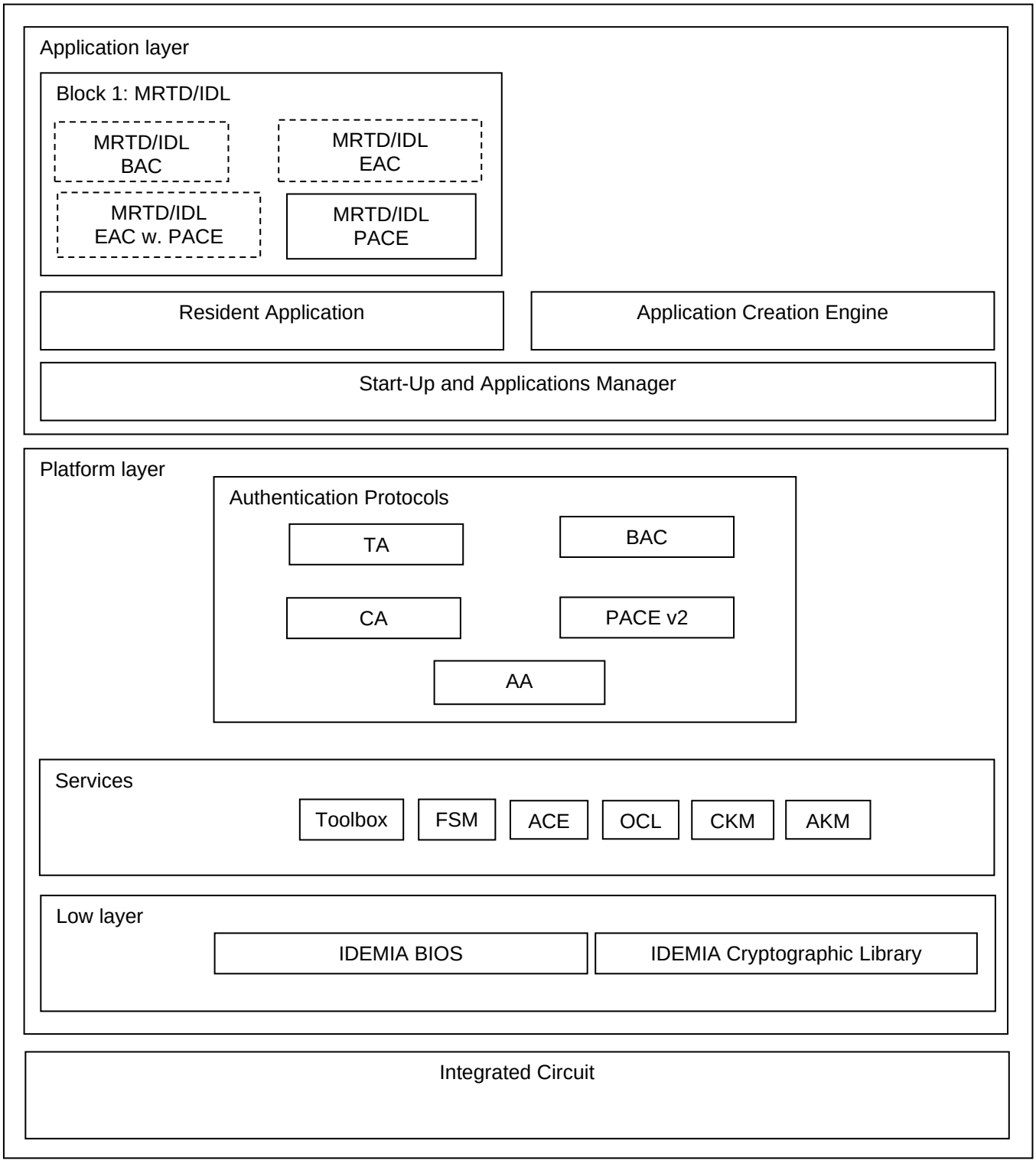



Figure 1 - TOE architecture

### 2.3.2 Integrated Circuit

The TOE is embedded on SCR404U components (cf § Table 3 - IC identification).

IC is part of the TOE and also part of the TSF. More information on the chips with physical and logical protections is given in the related Security Target [IC_ST].
It is a hardware device composed of a processing unit, memories, security components and I/O interfaces. It has to implement security features able to ensure:

- The confidentiality and the integrity of information processed and flowing through the device,
- The resistance of the security IC to externals attacks such as physical tampering, environmental stress or any other attacks that could compromise the sensitive assets stored or flowing through it.

### 2.3.3 Low layer

#### 2.3.3.1 Basic Input/Output System (**BIOS**)

The BIOS module provides access management (read/write) functionalities to upper-layer application. It also provides exception and communication functionalities.

*The BIOS module is part of the TOE and is also part of the TSF.*

#### 2.3.3.2 Cryptographic library (**Crypto**)

The Cryptography module provides secure cryptographic functionalities to upper-layer applications. . Ciphering operations are implemented to resist environmental stress and glitches and include measures for preventing information leakage through covert channels.

*The Crypto module is part of the TOE and is also part of the TSF.*

### 2.3.4 Platform layer

#### 2.3.4.1 Services

##### 2.3.4.1.1 File System Management (**FSM**)

The FSM module manages files and data objects according to ISO 7816-4 and 7816-9. It also manages the Digitally Blurred Image process, allowing for blurring a JPG or JPEG2000 image stored in a transparent file. This feature is covered by a patent owned by IDEMIA. Sensitive data have to be protected in integrity from modifications: keys, updated code and sensitive MRTD data.

*The FSM module is part of the TOE and is also part of the TSF.*

##### 2.3.4.1.2 Os Communication Layer (**OCL**)

Os Communication Layer (OCL) is the first subsystem that takes in charge the communication layer (ISO7816 and ISO14443) and it's the first entry point to make the link between external to internal. It manages the protocol, the ATR sending, the Secure Messaging and brings some specific functionalities
The Secure Messaging OCL provides functionalities to encrypt/decrypt data for secure communication in Manufacturing, Personalization and Operational Use phases (steps 5, 6 and 7). A Secure Messaging session begins after a successful authentication (GP authentication for Pre-personalization and Personalization phases or CA for Operational Use phase).

*The OCL module is part of the TOE and is also part of the TSF.*

##### 2.3.4.1.3 Cryptography Key Management (**CKM**)

The CKM module is responsible for asymmetric cryptography key management and asymmetric cryptography operations.

*The CKM module is part of the TOE and is also part of the TSF.*

#### 2.3.4.1.4 Authentication and Key Management (**AKM**)

This module supplies:

- Symmetric Key management (read, write, access control),
- Services to manage Global Platform authentication and secure messaging.

*The AKM module is part of the TOE and is also part of the TSF.*

#### 2.3.4.1.5 Access Condition Engine (**ACE**)

The ACE module is in charge of the verification of the Access Conditions of an object (files and keys) when an application tries to access this object.

*The ACE module is part of the TOE and is also part of the TSF.*

#### 2.3.4.1.6 Toolbox (**TBX**)

The Toolbox module provides different kind of services to other modules.

- Services to manage APDU,
- Services to handle BER-TLV constructed data object,
- Services to process specific cryptographic operations,
- Services to handle Object Identifier,
- Services to manage MRZ (personalization and misuse management),
- Services to handle data in a secure way.

*The TBX module is part of the TOE and is also part of the TSF*

### 2.3.5 Authentication Protocols

#### 2.3.5.1 Terminal Authentication (**TA**)

The TA module processes the Terminal Authentication (v1 and v2) mechanism. Terminal Authentication v1 is part of the EACv1 procedure defined in [ICAO_9303].

*The TA module is part of the TOE but is **NOT** part of the TSF.*

#### 2.3.5.2 Chip Authentication (**CA**)

The CA module processes the Chip Authentication (v1 and v2) mechanism. Chip Authentication v1 is part of the EACv1 procedure defined in [ICAO_9303].

*The CA module is part of the TOE and also part of the TSF.*

#### 2.3.5.3 Password Authenticated Connection Establishment (**PACE v2**)

The PACE module provides functionalities to process the PACE v2 mechanism as defined in [ICAO_9303].
PACEv2 protocol is extended with PIN and PUK passwords, to enforce user authentication (document holder verification) in compliance with [TR_03110].

*The PACE v2 module is part of the TOE and also part of the TSF.*

#### 2.3.5.4 Active Authentication (**AA**)

The AA module provides functionalities to process the AA mechanism as defined in [ICAO_9303].

*The AA module is part of the TOE and is also part of the TSF.*

### 2.3.6 Application layer

#### 2.3.6.1 Start-Up and Applications Manager (**Boot**)

The Boot module is responsible to manage the start-up of the applications (MRTD, RA and ACRE).

*The Boot module is part of the TOE and is also part of the TSF*

#### 2.3.6.2 Application Creation Engine (**ACRE**)

The Application Creation Engine is a complete set of commands used to (pre-)personalize the card and its application(s). It includes:

- Creation of application,
- Import and Generation of the Active Authentication key (ECC and RSA keys),
- Import and Generation of multiple Chip Authentication keys under the ADF (supporting ECC and RSA Keys),
- Storage of CVCA Keys under each ADF.

*The ACRE module is part of the TOE and is also part of the TSF.*

#### 2.3.6.3 Resident Application (**RA**)

The Resident Application is a complete set of commands, which allows the management of the card in the Operational Use phase (data management and authentication process under MF). The RA is also in charge of Update mechanism.

The Additional Code Loading, i.e the Update mechanism process is as follow:

1. Additional Code's Secure Messaging keys (authenticity and confidentiality) calculation,
2. Additional Code loading,
3. Additional Code activation.

*The RA module is part of the TOE and is also part of the TSF.*

#### 2.3.6.4 Machine Readable Travel Document (**MRTD**)

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

*The MRTD module is part of the TOE and is also part of the TSF.*

### 2.3.1 Other features

#### 2.3.1.1 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 and is also part of the TSF.*

#### 2.3.1.2 Enhanced protection over Sensitive biometric data reading

The access to sensitive biometric data (such as 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 datas. 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. If this condition is not met (algorithm not strong enough), the access to the sensitive data is denied.

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

#### 2.3.1.3 Automatic TDES SM phasing out

The TOE allows for the automatic deactivation of the TDES algorithm, in the scope of secure channel protection, after the current date has reached a target date - chosen by the issuer and configured by the Personalization Agent. The current date is the internal date updated through the EAC protocol. This mechanism enables smooth phasing out of the TDES protocol in the medium term (due to its cryptographic weaknesses) during the lifetime of the issued MRTDs, without having to wait for the complete renewal of issued MRTD (> 10 years).
*The automatic TDES SM phasing out is part of the TOE and is also part of the TSF.*

# 3 Conformance claims

## 3.1 Common Criteria conformance

This Security Target (ST) claims conformance to the Common Criteria (CC) version 3.1 revision 5.

The conformance to the CC is claimed as follows Part 2 extended and Part 3 Conformant:

| CC | **Conformance Claim** |
|---|---|
| Part 1 | Strict conformance |
| Part 2 | Conformance with extensions:<br>• FAU_SAS.1 *"Audit storage",*<br>• FCS_RND.1 *"Quality metric for random numbers",*<br>• FMT_LIM.1 *"Limited capabilities",*<br>• FMT_LIM.2 *"Limited availability",*<br>• FPT_EMS.1 *"TOE Emanation",*<br>• FIA_API.1[2] *"Authentication Proof of Identity".* |
| Part 3 | Conformance with package EAL5 defined in [CC_3] augmented with:<br>• ADV_IMP.2 "Complete mapping of the implementation representation of the TSF",<br>• ADV_INT.3 "Minimally complex internals",<br>• ADV_TDS.5 "Complete semiformal modular design",<br>• ALC_CMC.5 "Advanced support",<br>• ALC_TAT.3 "Compliance with implementation standards – all parts",<br>• ALC_FLR.3 "Flaw remediation",<br>• ALC_DVS.2 "Sufficiency of security measures",<br>• ATE_COV.3 "Rigorous analysis of coverage",<br>• ATE_FUN.2 "Ordered Functional testing",<br>• AVA_VAN.5 "Advanced methodical vulnerability analysis". |

Table 8 – Common Criteria conformance claim

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

## 3.2 Protection Profile conformance

### 3.2.1 Overview

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

| | |
|---|---|
| **Title** | Common Criteria Protection Profile – Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) |
| **CC Version** | 3.1 (Revision 3) |
| **Assurance Level** | The minimum assurance level for this PP is EAL4 augmented |
| **Version Number** | 1.01 as of 22nd July 2014 |
| **Registration** | BSI-CC-PP-0068-V2-2011-MA-01 |

Table 9 – Protection Profile conformance

This ST also addresses the Manufacturing and Personalization phases at TOE level (cf. §2.2.3 TOE life cycle), as well as the Chip Authentication (CA) and Active Authentication (AA) protocols available in operational use phase. The additions do not contradict any of the threats, assumptions, organizational policies, objectives or SFRs stated in the [PP_PACE] that covers the advanced security methods PACE in operational use phase.

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

This ST is also based on the following PP Configuration:

| | |
|---|---|
| **Title** | Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP] |
| **CC Version** | 3.1 (Revision 4) |
| **Assurance Level** | The minimum assurance level for this PP is EAL4 augmented |
| **Version Number** | Version 0.9.2, August 18th, 2016 |
| **Registration** | BSI-CC-PP-0090-2016 |

Table 10 – Protection Profile Configuration conformance

The strict conformance can't be announced here because the [PP_0087] is not used, but the PP module for OS post emission update [PP_0090] is completely used. For code loading, this ST is also based on the support of [JIL_SRCL] document.

### 3.2.2 Overview of differences between the PP and the ST

The additional functionality of Password Authenticated Connection Establishment with Chip Authentication Mapping (PACE-CAM) has been added to the TOE. It possesses the same security requirements as the PACE functionality, which means that the same security problem definition is applicable for PACE-CAM.

The following additional SFRs have been defined for PACE-CAM:

- **FIA_UID.1/PACE_CAM**
- **FIA_UAU.1/PACE_CAM**
- **FIA_UAU.4/PACE_CAM**
- **FIA_UAU.5/PACE_CAM**
- **FIA_UAU.6/PACE_CAM**

Additions for PIN:

An additional package from PP claimed above for the PIN is presented in this security target. Definitions are based on protection profiles BSI-CC-PP-0086 which enforces the security definitions. See /PIN definitions.

### 3.2.3 Assumptions

The following Assumptions are assumed for this TOE:

- **A.Passive_Auth** *"PKI for Passive Authentication"* defined in [PP_PACE],
- **A.Insp_Sys_Chip_Auth** "Inspection Systems for global interoperability on chip authenticity" defined in this ST,
- **A.MRTD_Manufact** *"MRTD manufacturing on steps 4 to 6"*, defined in this ST,
- **A.MRTD_Delivery** *"MRTD delivery during steps 4 to 6"*, defined in this ST.

A.Insp_Sys_Chip_Auth is additional for the Chip Authentication protocol and for Active Authentication protocol which are not in the original scope of the [PP_PACE]. This assumption is only linked to threats for the Chip Authentication protocol and Active Authentication protocol so this assumption neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the [PP_PACE], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_PACE].

A.MRTD_Manufact is additional for MRTD manufacturing on steps 4 to 6 which is not in the original scope of the [PP_EACwPACE]. This assumption is only linked to threats for the MRTD manufacturing on steps 4 to 6 so this assumption neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the [PP_EACwPACE], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_EACwPACE].

A.MRTD_Delivery is additional for MRTD delivery during steps 4 to 6 which is not in the original scope of the [PP_EACwPACE]. This assumption is only linked to threats for the MRTD delivery during steps 4 to 6 so this assumption neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the [PP_EACwPACE], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_EACwPACE].

### 3.2.4 Threats

The following threats are averted by this TOE:

- **T.Skimming** "Skimming travel document / Capturing Card-Terminal Communication" defined in [PP_PACE],
- **T.Eavesdropping** "Eavesdropping on the communication between the TOE and the PACE terminal" defined in [PP_PACE],
- **T.Tracing** "Tracing travel document" defined in [PP_PACE],
- **T.Forgery** "Forgery of Data" defined in [PP_PACE],
- **T.Abuse-Func** "Abuse of Functionality" defined in [PP_PACE],
- **T.Information_Leakage** "Information Leakage from travel document" in [PP_PACE],
- **T.Phys-Tamper** "Physical Tampering" defined in [PP_PACE],
- **T.Malfunction** "Malfunction due to Environmental Stress" defined in [PP_PACE],
- **T.Configuration** *"Tampering attempt of the TOE during preparation"* defined in this ST,
- **T.Counterfeit** *"MRTD's chip"* defined in this ST,

**Threats** for Update mechanism:

- **T.FaTSF "Faulty TSF"**, defined in [PP_0090],
- **T.UaU** "Unauthorized Update", defined in [PP_0090].

### 3.2.5 Organizational Security Policies

This TOE complies with the following OSP:

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

OSP for Update mechanism:

- **P.Code_Confidentiality**, defined in [PP_0090],
- **P.Secure_Environment**, defined in [PP_0090],
- **P.Eligible_Terminals_Only**, defined in [PP_0090].

### 3.2.6 Security Objectives

The Security Objectives for this TOE are the following:

- **OT.Data_Integrity** *"Integrity of Data"* defined in [PP_PACE],
- **OT.Data_Authenticity** *"Authenticity of Data"* defined in [PP_PACE],
- **OT.Data_Confidentiality** *"Confidentiality of Data"* defined in [PP_PACE],
- **OT.Tracing** *"Tracing travel document"* defined in [PP_PACE],
- **OT.Prot_Abuse-Func** *"Protection against Abuse of Functionality"* defined in [PP_PACE],
- **OT.Prot_Inf_Leak** *"Protection against Information Leakage"* defined in [PP_PACE],
- **OT.Prot_Phys-Tamper** *"Protection against Physical Tampering"* defined in [PP_PACE],
- **OT.Prot_Malfunction** *"Protection against Malfunctions"* defined in [PP_PACE],
- **OT.Identification** *"Identification of the TOE"* defined in [PP_PACE],
- **OT.AC_Pers** *"Access Control for Personalisation of logical MRTD"* defined in [PP_PACE],
- **OT.Configuration** *"Protection of the TOE preparation"* defined in this ST,
- **OT.Chip_Auth_Proof** *"Proof of MRTD's chip authenticity"* defined in this ST,
- **OT.TOE_Identification** *"Secure identification of the TOE"* defined in [JIL_SRCL].
  OT for update mechanism:
- **OT.Update_Mechanism "TOE Update Mechanism"** defined in [PP_0090],
- **OT.Enc_Sign_Update** "Encrypted-then-signed Update Packages" defined in [PP_0090],
- **OT.Update_Terminal_Auth** "Updates only by authenticated Update Terminals" defined in [PP_0090],
- **OT.Attack_Detection** "Detection of Attacks on the TOE using the Update Mechanism" defined in [PP_0090],
- **OT.Key_Secrecy** "Key Secrecy of Cryptographic Update Keys" defined in [PP_0090].

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

- **OE.Legislative_Compliance** *"Issuing of the travel document"* defined in [PP_PACE],
- **OE.Passive_Auth_Sign** *"Authentication of travel document by Signature"* defined in [PP_PACE],
- **OE.Personalisation** *"Personalisation of travel document"* defined in [PP_PACE],
- **OE.Terminal** *"Terminal operating"* defined in [PP_PACE]
- **OE.Travel_Document_Holder** *"Travel document holder Obligations"* defined in [PP_PACE],
- **OE.Exam_Chip_Auth** *"Examination of the chip authenticity"* defined in this ST,
- **OE.MRTD_Manufact** *"Protection of the MRTD Manufacturing"* defined in this ST,
- **OE.MRTD_Delivery** *"Protection of the MRTD delivery"* defined in this ST,
- **OE.Auth_MRTD** *"MRTD Authentication Key"* defined in this ST.
  OE for Update mechanism
- **OE.Secure_Environment** defined in [PP_0090],
- **OE.Eligible_Terminals_Only** defined in [PP_0090],
- **OE.Code_Confidentiality** defined in [PP_0090].

OE.Exam_Chip_Auth and OE.Auth_MRTD are additional objectives for the Chip Authentication protocol and Active Authentication protocol which are not in the original scope of the [PP_PACE]. These objectives are only linked to threats for the Chip Authentication protocol and Active Authentication protocol so these objectives neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the [PP_PACE], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_PACE].

OE.MRTD_Manufact is additional for the Protection of the MRTD manufacturing on steps 4 to 6 which is not in the original scope of the [PP_PACE]. This objective is only linked to assumption for the MRTD manufacturing on steps 4 to 6, so this objective neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the [PP_PACE], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_PACE].

OE.MRTD_Delivery is additional for the Protection of the MRTD delivery during steps 4 to 6 which is not in the original scope of the [PP_PACE]. This objective is only linked to threats for the MRTD delivery during steps 4 to 6, so this objective neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for

the TOE in the [PP_PACE], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [PP_PACE].

# 4 Security problem definition

## 4.1 Assets

### 4.1.1 Overview

The following table presents the assets of the TOE and their corresponding phase(s) according to §2.2.3 TOE life cycle:

| Asset | Step 5 | Step 6 | Step 7 |
|---|---|---|---|
| Personal Data | × | ✓ | ✓ |
| EF.COM | × | ✓ | ✓ |
| CA_SK | × | ✓ | ✓ |
| AA_SK | × | ✓ | ✓ |
| Session_K | ✓ | ✓ | ✓ |
| PACE_Kmac | × | × | ✓ |
| PACE_Kenc | × | × | ✓ |
| ephem-Skpicc-PACE | × | × | ✓ |
| EF.SOD | × | ✓ | ✓ |
| CA_PK | × | ✓ | ✓ |
| AA_PK | × | ✓ | ✓ |
| PACE_PWD | × | ✓ | ✓ |
| CPLC | ✓ | ✓ | ✓ |
| TOE_ID | ✓ | ✓ | ✓ |
| Pre-Perso_K | ✓ | × | × |
| Perso_K | × | ✓ | × |
| LCS | ✓ | ✓ | ✓ |
| Configuration data | ✓ | ✓ | ✓ |
| Update Package | ✓ | ✓ | ✓ |
| LSK | ✓ | ✓ | ✓ |
| DIV_LSK and DIV2_LSK | ✓ | ✓ | ✓ |

Table 11 – Assets of the TOE and their corresponding phase(s)

### 4.1.2 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_9303] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_9303])
This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [PP_PACE].

It includes the Personal Data which are the logical MRTD standard User Data of the MRTD holder (see definition in chapter 9.1).

#### 4.1.2.1 EF.COM

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

*Application note (6 in* [PP_PACE]*):* Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the travel document holder which also include his sensitive (i.e. biometric) data. Hence, the general security policy defined by the current PP also secures these specific travel document holder's data as stated above.

#### 4.1.3 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_9303] between the TOE and an authenticated terminal acting as Extended Inspection System with PACE (in the sense of [ICAO_9303]).
User data can be received and sent (exchange ⇔ {receive, send}).

#### 4.1.4 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.

#### 4.1.5 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.

#### 4.1.6 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].

#### 4.1.7 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:

##### 4.1.7.1 Chip Authentication Private Key (CA_SK)

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

##### 4.1.7.2 Active Authentication Private Key (AA_SK)

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

##### 4.1.7.3 Secure Messaging session keys (Session_K)

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

##### 4.1.7.4 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.

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

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

#### 4.1.8 TOE intrinsic non secret cryptographic material

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

It includes:

#### 4.1.8.1 EF.SOD

The elementary file Document Security Object is used by the inspection system for Passive Authentication of the logical MRTD.

#### 4.1.8.2 Chip Authentication Public Key (CA_PK)

The Chip Authentication Public Key (contained in EF.DG14) is used by the inspection system for the Chip Authentication.

#### 4.1.8.3 Active Authentication Public Key (AA_PK)

The Active Authentication Public Key (contained in EF.DG15) is used by the inspection system for the Active Authentication.

### 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:

#### 4.1.9.1 PACE password (PACE_PWD)

Password needed for PACE authentication, e.g. CAN or MRZ.

*Application Note (7 in* [PP_PACE]*)*: Since the travel document does not support any secret travel document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.

*Application Note (8 in* [PP_PACE]*)*: travel document communication establishment authorisation data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorisation attempt.The TOE shall secure the reference information as well as – together with the terminal connected – the verification information in the 'TOE ↔ terminal' channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be send to the TOE.

#### 4.1.9.2 Secret Electronic Document Holder Authentication Data

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

### 4.1.10 CPLC

The CPLC Data are the Card Production Life Cycle data. They are considered as user data as they enable to track the holder. These data are filled during steps 4, 5 and 6 by subjects.

### 4.1.11 TOE_ID

These data allow the identification of the TOE. These data are part of the IC Embedded Software in the non-volatile non-programmable memory. If Update Package is loaded, then the TOE_ID contains Update Package Identification Data.

#### 4.1.12 Pre-personalization Agent keys (Pre-perso_K)

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

#### 4.1.13 Personalization Agent keys (Perso_K)

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

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

This is the Life Cycle State of the TOE.

#### 4.1.15 Configuration Data

These specific data set the configuration of the TOE in terms of security features and security functions. These configuration data can be set in Manufacturing and Personalization phases (Steps 5 and 6) after authentication of the relevant agent with the relevant key set.

#### 4.1.16 Assets related to Update Mechanism

##### 4.1.16.1 Secret Cryptographic Update Keys

All cryptographic key material related to the update mechanism; i.e. cryptographic material that is used to establish a secure communication channel with the update terminal, to authenticate an update terminal, to decrypt and verify the authenticity of an update package, and for other update-related cryptographic operations. Note that this term deliberately includes public (in the cryptographic sense) signing keys installed on the TOE for verifying the authenticity of update packages, as well as ephemeral keys.
Application Note: the keys are LSK and derived ones: see 4.1.16.8.

##### 4.1.16.2 Meta-Data

Data that contains information about the update, e.g. version information, checksums, information w.r.t. applicability to specific product versions and platforms, etc.

*Application Note 2*: Note that, depending on the deployment scenario, some meta-data are security relevant and must be encrypted. Consider for example an identifier, that uniquely identifies a product version. If the update fixes a security flaw, an attacker that obtains the identifier can directly find out whether some product is vulnerable. The precise definition of meta-data and which data are encrypted shall be given by the ST-Writer.

##### 4.1.16.3 Update Data

Unencrypted data that is used to update the TOE software.

Note that we use the term *update data* to denote the unencrypted data. Encrypted update data, appended with optional additional unencrypted meta-data (i.e. version number, TOE product identifier), and signed, is called an *update package*.

##### 4.1.16.4 Update Log Data

Log records that store information about previously applied updates and failed update attempts.

##### 4.1.16.5 Update Package

Encrypted update data, appended with optional unencrypted meta-data, and signed.
Application Note:
This is the Updated Code to be loaded on the Initial TOE during life cycle by an update Agent C. The result of this operation is the Final TOE.

#### 4.1.16.6 Update Package Verification Status

Security attribute indicating whether the supplied update was successfully verified (and where hence its authenticity and integrity can be assumed) or not, and whether an attempt to verify was made or not. Allowed values are NOT VERIFIED, SUCCESSFULLY VERIFIED and VERIFICATION FAILED.

#### 4.1.16.7 Version Information

Version information that uniquely identify the version of the TOE software currently installed on the TOE.

#### 4.1.16.8 Load Secure Key (LSK) and Diversified LSK (DIV_LSK, DIV2_LSK)

This Load Secure Key (LSK) is the secret key used to calculate the Diversified LSK (DIV_LSK and DIV2_LSK). The Diversified LSK is a session key used to verify the Update Package confidentiality (DIV_LSK) and integrity (DIV2_LSK).

## 4.2 Subjects

### 4.2.1 Overview

| Subject | Descr. | Step 3 | Step 4 | Step 5 | Step 6 | Step 7 |
|---|---|---|---|---|---|---|
| MRTD Holder | § 4.2.2 | × | × | × | × | ✓ |
| Traveler | § 4.2.3 | × | × | × | × | ✓ |
| Basic Inspection System with PACE | § 4.2.4 | × | × | × | × | ✓ |
| Document Signer | § 4.2.5 | × | × | × | ✓ | × |
| Country Signing Certification Authority | § 4.2.6 | × | × | × | ✓ | × |
| Personalization Agent | § 4.2.7 | × | × | × | ✓ | × |
| IC manufacturer (Manufacturer role) | § 4.2.8 | ✓ | × | × | × | × |
| MRTD packaging responsible (Manufacturer role) | § 4.2.9 | × | ✓ | × | × | × |
| Embedded software loading responsible (Manufacturer role) | § 4.2.10 | ✓ | ✓ | × | × | × |
| Pre-personalization Agent (Manufacturer role) | § 4.2.11 | × | × | ✓ | × | × |
| Terminal | § 4.2.12 | × | × | ✓ | ✓ | ✓ |
| Attacker | § 4.2.13 | ✓ | ✓ | ✓ | ✓ | ✓ |

Table 12 – Subjects of the TOE and their corresponding phase(s)

### 4.2.2 MRTD holder

MRTD holder is the travel document holder defined in [PP_PACE]:

A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with ‘MRTD Holder’ in [PP_PACE]. Please note that a travel document holder can also be an attacker.

### 4.2.3 Traveler

A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with ‘Traveller’ in [PP_PACE]. Please note that a travel document presenter can also be an attacker.

### 4.2.4 Basic Inspection System with PACE (BIS-PACE)

A technical system being used by an inspecting authority and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder).
BIS-PACE implements the terminal’s part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.
See also par. 1.2.5 in [PP_PACE].

### 4.2.5 Document Signer (DS)

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

### 4.2.6 Country Signing Certification Authority (CSCA)

An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate having to be distributed by strictly secure diplomatic means, see [ICAO_9303], 5.5.1.

### 4.2.7 Personalization Agent

An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO_9303], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO_9303] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [PP_PACE].

### 4.2.8 IC manufacturer

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

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.

### 4.2.9 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.

### 4.2.10 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 1 or scheme 2 is applied (cf. § 2.2.3). This subject uses the Flash loader embedded in the IC.

### 4.2.11 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.

### 4.2.12 Terminal

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

PACE Terminal: A PACE terminal implements the terminal part of the PACE protocol, and authenticates itself to the electronic document using a shared password (CAN, PIN, PUK or MRZ). A PACE terminal is not allowed to access sensitive user data.

### 4.2.13 Attacker

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

*Application Note (9 in* [PP_PACE]*)*: Since the TOE does not use BAC, a Basic Inspection System with BAC (BIS-BAC) cannot be recognised by the TOE, see par. 1.2.5 in [PP_PACE].

## 4.3 Assumptions

### *4.3.1* **A.Passive_Auth** *"PKI for Passive Authentication"*

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

### *4.3.2* **A.Insp_Sys_Chip_Auth** *"Inspection Systems for global interoperability on chip authenticity"*

The Inspection System implements Active Authentication to authenticate the MRTD's chip. The Inspection System uses the signature returned by the TOE during Active Authentication as proof of authenticity.

### 4.3.3 **A.MRTD_Manufact** *"MRTD manufacturing on steps 4 to 6"*

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

### 4.3.4 **A.MRTD_Delivery** *"MRTD delivery during steps 4 to 6"*

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

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

## 4.4 Threats

### *4.4.1* **T.Skimming** *"Skimming travel document / Capturing Card-Terminal Communication"*

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

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

*Asset:* confidentiality of logical travel document data

*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 travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder

### 4.4.2 **T.Eavesdropping** *"Eavesdropping on the communication between the TOE and the PACE terminal"*

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

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

*Asset:* confidentiality of logical travel document data

*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]

### 4.4.3 **T.Tracing** *"Tracing travel document"*

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

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

*Asset:* privacy of the travel document holder

*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 travel document's chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document) cannot be averted by the current TOE.

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

#### 4.4.4 **T.Forgery** *"Forgery of Data"*

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

*Threat agent:* having high attack potential

*Asset:* integrity of the travel document

#### 4.4.5 **T.Abuse-Func** *"Abuse of Functionality"*

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

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

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

*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.

#### 4.4.6 **T.Information_Leakage** *"Information Leakage from travel document"*

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

*Threat agent:* having high attack potential

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

*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)

#### 4.4.7 **T.Phys-Tamper** *"Physical Tampering"*

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

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

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

*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 travel 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 travel 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.

#### 4.4.8 **T.Malfunction** *"Malfunction due to Environmental Stress"*

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

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

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

*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

#### 4.4.9 **T.Configuration** *"Tampering attempt of the TOE during preparation"*

*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

#### 4.4.10 **T.Counterfeit "MRTD's chip"**

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

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

*Asset:* authenticity of logical MRTD data

Threats for Update mechanism

#### 4.4.11 **T.FaTSF "Faulty TSF"**

*Adverse action:* An attacker gains read or write access to user data or TSF data, or manipulates or mitigates the TSF, for example due to:

- software issues that were not detected, not exploitable, or deemed unable to being exploitable at the time of certification, but due to unforeseen advances in technology became a security risk during operational use of the TOE, or
- cryptographic mechanisms that were deemed secure at the time of certification, but due to unforeseen advances in the field of cryptography became a security risk during operational use of the TOE.

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

*Asset:* all data stored on the TOE (esp. the integrity, authenticity and – if applicable – secrecy of the data)

#### 4.4.12 **T.UaU "Unauthorized Update"**

*Adverse action:* An attacker gains read or write access to user data or TSF data, or manipulates or mitigates the TSF by misuse of the update functionality. This threat contains two main aspects:

- the unauthorized installation, which may lead to the use of untimely, outdated or revoked updates.
- the installation of updates that are not authorized and authentic.

*Threat agent:* Having high attack potential, being in possession of one or more legitimate electronic documents.

*Asset:* all data stored on the TOE (esp. the integrity, authenticity and – if applicable – secrecy of the data)

## 4.5 Organisational Security Policies

### *4.5.1* **P.Pre-Operational** *"Pre-operational handling of the travel document"*

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

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

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

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

### 4.5.2 **P.Card_PKI** *"PKI for Passive Authentication (issuing branch)"*

*Application Note (20 in* [PP_PACE]*):* 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.

1.) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (CCSCA).

2.) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [ICAO_9303], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [ICAO_9303], 5.5.1.

3.) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

### 4.5.3 **P.Trustworthy_PKI** *"Trustworthiness of PKI"*

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

### 4.5.4 **P.Manufact** *"Manufacturing of the travel document's chip"*

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

### 4.5.5 **P.Terminal** *"Abilities and trustworthiness of terminals"*

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

1.) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [ICAO_9303].

2.) They shall implement the terminal parts of the PACE protocol [ICAO_9303], of the Passive Authentication [ICAO_9303] and use them in this order28. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3.) The related terminals need not to use any own credentials.

4.) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [ICAO_9303]).

5.) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to [PP_PACE].

### 4.5.6 OSP from PP Module for Update mechanism

#### 4.5.6.1 **P.Code_Confidentiality**

Update code packages that are created by the TOE software developer or document manufacturer are kept confidential, are encrypted after development at the site of the electronic document manufacturer, and are delivered to the TOE in encrypted form.

#### 4.5.6.2 **P.Secure_Environment**

Update terminals are placed in a secure environment that prevents unauthorized physical access, and are operated by authorized staff only. Authorized staff oversees the complete update procedure.

#### 4.5.6.3 **P.Eligible_Terminals_Only**

Update terminals (i.e. terminals with appropriate certificates that are able to install updates) are handed only to those entities where P.Secure_Environment is enforced. In case of a security incident, these update terminals are functionally disabled (through organizational and/or cryptographic means by e.g. withdrawing certificates).

# 5 Security objectives

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

## 5.1 Security objectives for the TOE

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

### 5.1.1 **OT.Data_Integrity** *"Integrity of Data"*

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

### 5.1.2 **OT.Data_Authenticity** *"Authenticity of Data"*

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

### 5.1.3 **OT.Data_Confidentiality** *"Confidentiality of Data"*

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

### 5.1.4 **OT.Tracing** *"Tracing travel document"*

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

*Application note (21 in* [PP_PACE]*)*: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity) cannot be achieved by the current TOE.

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

### 5.1.5 **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.

### 5.1.6 **OT.Prot_Inf_Leak** *"Protection against Information Leakage"*

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

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

*Application note (22 in* [PP_PACE]*)*: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

### 5.1.7 **OT.Prot_Phys-Tamper** *"Protection against Physical Tampering"*

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

- 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
- 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),
- manipulation of the hardware and its security functionality, as well as
- controlled manipulation of memory contents (User Data, TSF-data) with a prior
- reverse-engineering to understand the design and its properties and functionality.

### 5.1.8 **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.

### 5.1.9 **OT.Identification** *"Identification 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 travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

**Note**: The IC shall be able to authenticate itself to external entities. The Initialisation Data are used for IC authentication verification data.

### 5.1.10 **OT.AC_Pers** *"Access Control for Personalisation of logical MRTD"*

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO_9303] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

*Application note (23 in* [PP_PACE]*)*: The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

#### 5.1.11 **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.

#### 5.1.12 **OT.Chip_Auth_Proof** *"Proof of MRTD's chip authenticity"*

The TOE must support the Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [ICAO_9303], or the Active Authentication as defined in [ICAO_9303], or the PACE protocol with Chip Authentication Mapping method as defined in [ICAO_9303]. These protocols shall be executed in combination with the Document Security Object (SOD) verification to verify the SOD belongs to the data page, the chip is genuine and chip and data page belong to each other as defined in [ICAO_9303].The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

#### 5.1.13 **OT.TOE_Identification** *"Secure identification of the TOE"*

The Identification Data identifies the Initial TOE and Update Package. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data.
After Atomic Activation of the Update Package, the Identification Data of the Final TOE allows identifications of Initial TOE and Update Package(s). The user must be able to uniquely identify Initial TOE and Update Package(s) which are embedded in the Final TOE.

*Security Objectives from PP Module for Update mechanism*

#### 5.1.14 **OT.Update_Mechanism "TOE Update Mechanism"**

The TSF provides a mechanism to install code-signed updates of the TOE software by authorized staff during operational use.

#### 5.1.15 **OT.Enc_Sign_Update "Encrypted-then-signed Update Packages"**

The TOE only installs update packages that are encrypted, integrity-protected and signed by the authority in charge of delivering and installing updates.

#### 5.1.16 **OT.Update_Terminal_Auth "Updates only by authenticated Update Terminals"**

The TOE allows only authenticated update terminals to upload an update package to the TOE and to initiate the update procedure. The TOE uses a dedicated cryptographic method to authenticate an update terminal.

#### 5.1.17 **OT.Attack_Detection "Detection of Attacks on the TOE using the Update Mechanism"**

The TOE has logging capabilities that track installed updates and failed update attempts. It also limits the amount of faulty (signature verification or decryption fails) update attempts. It allows dedicated terminals to read out the update logs.

#### 5.1.18 **OT.Key_Secrecy "Key Secrecy of Cryptographic Update Keys"**

The TOE keeps the cryptographic update keys secret, and is designed such that emissions from the TOE do not allow to read out or gain full or partial information about the keys.

## 5.2 Security objectives for the operational environment

### 5.2.1 Receiving State or Organisation

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

#### *5.2.1.1* **OE.Exam_Chip_Auth** *"Examination of the chip authenticity"*

The Inspection System performs the Chip Authentication Protocol or the Active Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

### 5.2.2 Traveler document Issuer as general responsible

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

#### 5.2.2.1 **OE.Legislative_Compliance** *"Issuing of the travel document"*

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

### 5.2.3 Traveler document Issuer and CVCA : travel document's PKI (issuing) branch

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the Application Note 20 above):

#### 5.2.3.1 **OE.Passive_Auth_Sign** *"Authentication of travel document by Signature"*

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

#### 5.2.3.2 **OE.Personalisation** *"Personalisation of travel document"*

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

### 5.2.4 Terminal operator : Terminal's receiving branch

#### 5.2.4.1 **OE.Terminal** *"Terminal operating"*

The terminal operators must operate their terminals as follows:

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

*Application note (24 in* [PP_PACE]*):* OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from [PP_BAC].

### 5.2.5 Travel document holder Obligations

#### *5.2.5.1* **OE.Travel_Document_Holder** *"Travel document holder Obligations"*

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

Issuing State or Organisation

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

#### 5.2.5.2 **OE.MRTD_Manufact** *"Protection of the MRTD Manufacturing"*

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

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

#### 5.2.5.3 **OE.MRTD_Delivery** *"Protection of the MRTD delivery"*

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

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

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

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

**Note**: Security procedures shall be used to:
1. maintain confidentiality and integrity of the code to be loaded during Phase 4, Phase 5 and Phase 6,
2. realize appropriate Loader key management in the environment (confidentiality must be maintained).

#### 5.2.5.4 **OE.Auth_MRTD** *"MRTD Authentication Key"*

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

(i) generate the MRTD's Authentication Key Pair(s), (ii) ensure the secrecy of the MRTD's Authentication Private Key(s), (iii) sign and store the Authentication Public Key(s) in the Authentication Public Key data (i.e in EF.DG14 for Chip Authentication Public Key and in EF.DG15 for Active Authentication Public Key) and (iv) 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 Authentication Public Key by means of the Document Security Object.

### 5.2.6 OEs from PP Module for Update mechanism

#### 5.2.6.1 **OE.Secure_Environment**

The operational environment must ensure that update terminals are placed in a secure environment that prevents unauthorized physical access, and are operated by authorized staff only. The operational environment must also ensure through e.g. organizational policies and procedures, that authorized staff oversees the complete update procedure.

#### 5.2.6.2 **OE.Eligible_Terminals_Only**

The operational environment must also ensure by e.g. organizational procedures, supported by cryptographic means, that only those entities that have policies in place that guarantee OE.Secure_Environment, are supplied with update terminals. Moreover the operational environment guarantees that update terminals can be functionally deactivated if these policies are no longer in place or not enforced at the entities. This can be implemented for example by the issuance of certificates for update terminals together with a public key infrastructure.

### 5.2.7 Security Objectives for the Development and Production Environment

#### 5.2.7.1 **OE.Code_Confidentiality**

The operational environment must ensure that the TOE software developer or document manufacturer keeps update code packages confidential, encrypts them after development at the site of the developer/manufacturer, and delivers them to the TOE in encrypted form.

## 5.3 Security objectives rationale

### 5.3.1 Introduction

| Assumption | Related Security Objective(s) | Rationale |
|---|---|---|
| A.Passive_Auth | OE.Passive_Auth_Sign | § 5.3.2.1 |
| A.Insp_Sys_Chip_Auth | OE.Exam_Chip_Auth | § 5.3.2.2 |
| A.MRTD_Manufact | OE.MRTD_Manufact | § 5.3.2.3 |
| A.MRTD_Delivery | OE.MRTD_Delivery | § 5.3.2.4 |

Table 13- Assumptions of the TOE and Security Objectives

| Threat | Related Security Objective(s) | Rationale |
|---|---|---|
| T.Skimming | OT.Data_Integrity<br>OT.Data_Authenticity<br>OT.Data_Confidentiality<br>OE.Travel_Document_Holder | § 5.3.3.1 |
| T.Eavesdropping | OT.Data_Confidentiality | § 5.3.3.2 |
| T.Tracing | OT.Tracing<br>OE.Travel_Document_Holder | § 5.3.3.3 |
| T.Abuse-Func | OT.Prot_Abuse-Func | § 5.3.3.4 |
| T.Information_Leakage | OT.Prot_Inf_Leak | § 5.3.3.5 |
| T.Phys-Tamper | OT.Prot_Phys-Tamper | § 5.3.3.5 |
| T.Malfunction | OT.Prot_Malfunction | § 5.3.3.5 |
| T.Forgery | OT.AC_Pers<br>OT.Data_Integrity<br>OT.Data_Authenticity<br>OT.Prot_Abuse-Func<br>OT.Prot_Phys-Tamper<br>OE.Personalisation<br>OE.Passive_Auth_Sign<br>OE.Terminal | § 5.3.3.6 |
| T.Configuration | OT.Configuration<br>OT.TOE_Identification | § 5.3.3.7 |
| T.Counterfeit | OT.Chip_Auth_Proof<br>OE.Exam_Chip_Auth<br>OE.Auth_MRTD | § 5.3.3.8 |
| T.FaTSF | OT.Update_Mechanism<br>OT.Attack_Detection<br>OT.Key_Secrecy | § 5.3.3.9 |
| T.UaU | OT.Enc_Sign_Update<br>OT.Update_Terminal_Auth | § 5.3.3.10 |

Table 14- Threats of the TOE and Security Objectives

| OSP | Related Security Objective(s) | Rationale |
|---|---|---|
| P.Manufact | OT.Identification | § 5.3.4.1 |
| P.Pre-Operational | OT.AC_Pers<br>OT.Identification<br>OE.Personalisation<br>OE.Legislative_Compliance | § 5.3.4.2 |
| P.Terminal | OE.Terminal | § 5.3.4.3 |
| P.Card_PKI | OE.Passive_Auth_Sign | § 5.3.4.4 |
| P.Trustworthy_PKI | OE.Passive_Auth_Sign | § 5.3.4.5 |
| P.Code_Confidentiality | OE.Code_Confidentiality | § 5.3.4.6 |
| P.Secure_Environment | OE.Secure_Environment | |

| OSP | Related Security Objective(s) | Rationale |
|---|---|---|
| P.Eligible_Terminals_Only | OE.Eligible_Terminals_Only | |

Table 15- OSP of the TOE and Security Objectives

### 5.3.2 Rationales for Assumptions

#### 5.3.2.1 A.Passive_Auth

The assumption **A.Passive_Auth** *"PKI for Passive Authentication"* is directly addressed by OE.Passive_Auth_Sign requiring the travel document issuer to establish a PKI for Passive Authentication, generating Document Signing private keys only for rightful organisations and requiring the Document Signer to sign exclusively correct Document Security Objects to be stored on travel document.

#### 5.3.2.2 A.Insp_Sys_Chip_Auth

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys_Chip_Auth** "Inspection Systems for global interoperability on chip authenticity" is covered by the security objectives for the TOE environment OE.Exam_Chip_Auth *"Examination of the chip authenticity"*.

#### 5.3.2.3 A.MRTD_Manufact

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

#### 5.3.2.4 A.MRTD_Delivery

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

### 5.3.3 Rationales for Threats

#### 5.3.3.1 T.Skimming

The threat **T.Skimming** *"Skimming travel 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** *"Travel document holder Obligations"* ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

#### 5.3.3.2 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.

#### 5.3.3.3 T.Tracing

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

#### 5.3.3.4 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.

#### 5.3.3.5 T.Information_Leakage, T.Phys-Tamper and T.Malfunction

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

#### 5.3.3.6 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 travel document to the trustworthy Personalisation Agent (cf. OE.Personalisation). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives **OT.Data_Integrity** *"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 travel document by Signature"* will be able to effectively verify integrity and authenticity of the data received from the TOE.

#### 5.3.3.7 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"***.**

#### 5.3.3.8 T.Counterfeit

The threat **T.Counterfeit** *"MRTD's chip"* addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** *"Proof of MRTD's chip authenticity"* using a authentication key pair to be generated by the issuing State or Organization. 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_MRTD** *"MRTD Authentication Key"*. According to **OE.Exam_Chip_Auth** *"Examination of the chip authenticity"* the inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip.

This threat is also covered by **OE.Exam_Chip_Auth** *"Examination of the chip authenticity"* using a authentication key pair to be generated by the issuing State or Organization. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Auth_MRTD**

*"MRTD Authentication Key"*. According to **OE.Exam_Chip_Auth** *"Examination of the chip authenticity"* the inspection system has to perform the Active Authentication Protocol to verify the authenticity of the MRTD's chip.

Threats for Update mechanism

#### 5.3.3.9 T.FaTSF

The threat **T.FaTSF** addresses attacks on the TOE and TSF by an attacker exploiting flaws of the TOE software implementation that manifest themselves after the TOE enters the phase operational usage. This threat is countered by the TOE offering a secure update mechanism; in particular:

- The security objective **OT.Update_Mechanism** "TOE Update Mechanism" counters this threat by ensuring that the TOE has the ability to update the TOE software in a secure manner.
- The security objective **OT.Attack_Detection** "Detection of Attacks on the TOE using the Update Mechanism"ensures that the TOE is able to detect multiple failed update attempts and can take action upon that detection.
- The security objective **OT.Key_Secrecy** "Key Secrecy of Cryptographic Update Keys" makes sure that the required cryptographic key material for the update mechanism cannot be accessed or reconstructed by a malicious attacker.

#### 5.3.3.10 T.UaU

The threat **T.UaU** addresses attacks on the TOE and TSF by an attacker installing unauthorized and potential harmful updates:

- The security objective **OT.Enc_Sign_Update** "Encrypted-then-signed Update Packages" ensures that only signed and encrypted updates are installed by the TOE, and that during the transmission to the TOE, a protocol based on encrypt-then-MAC is used.
- The security objective **OT.Update_Terminal_Auth** "Updates only by authenticated Update Terminals" ensures that only authenticated update terminals are able to read version information, upload update packages on the TOE, and initiate the update procedure.

### 5.3.4 Rationales for Organisational Security Policies

#### 5.3.4.1 P.Manufact

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

#### 5.3.4.2 P.PRE-Operational

The OSP **P.Pre-Operational** *"Pre-operational handling of the travel 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 travel 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 travel document"* is affine to the OSP's property 'compliance with laws and regulations'.

#### 5.3.4.3 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.

#### 5.3.4.4 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 travel document by Signature"* (for the Document Security Object).

#### 5.3.4.5 P.Trustworthy_PKI

The OSP **P.Trustworthy_PKI** *"Trustworthiness of PKI"* is enforced by **OE.Passive_Auth_Sign** *"Authentication of travel document by Signature"* (for CSCA, issuing PKI branch).

#### 5.3.4.6 The organizational security policies for Update Mechanism

**P.Code_Confidentiality**, **P.Secure_Environment**, and **P.Eligible_Terminals_Only**, address the confidentiality of the code, the way the update procedure must be carried out, and precise control over which terminals are allowed to carry out the update procedure. Each of these policies are enforced through security objectives for the environment of the TOE, namely **OE.Code_Confidentiality**, **OE.Secure_Environment**, and **OE.Eligible_Terminals_Only**.

# 6 Extended components definition

## 6.1 Extended components definition

### 6.1.1 Definition of the Family FAU_SAS

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

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

**FAU_SAS** ***“Audit data storage”***

*Family behavior*

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

*Component leveling*

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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

**FAU_SAS.1** ***“Audit storage”***

Hierarchical to: No other components.

Dependencies: No dependencies.

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

### 6.1.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

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

**FCS_RND** ***“Generation of random numbers”***

*Family behavior*

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

*Component leveling:*

| | |
|---|---|
| FCS_RND.1 | Generation of random numbers requires that random numbers meet a defined quality metric. |
| Management: | FCS_RND.1<br><br>There are no management activities foreseen. |
| Audit: | FCS_RND.1<br><br>There are no actions defined to be auditable. |

**FCS_RND.1** ***“Quality metric for random numbers”***

Hierarchical to: No other components.

Dependencies: No dependencies.

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

### 6.1.3 Definition of the Family FMT_LIM

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

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

**FMT_LIM** ***“Limited capabilities and availability”***

*Family behavior*

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

*Component leveling:*

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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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

**FMT_LIM.1** ***“Limited capabilities”***

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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

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

**FMT_LIM.2** ***"Limited availability"***

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy]*.

### 6.1.4 Definition of the Family FPT_EMS

The sensitive 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 TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of [CC_2].

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

*Family behavior*

This family defines requirements to mitigate intelligible emanations.

Component levelling:

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.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

**FPT_EMS.1** ***"TOE Emanation"***

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

### 6.1.5 Definition of the Family FIA_API

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

**FIA_API** ***"Authentication Proof of Identity"***

*Family behavior*

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

*Component leveling:*

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: There are no actions defined to be auditable.

**FIA_API.1** ***"Authentication Proof of Identity"***

Hierarchical to: No other components.

Dependencies: No dependencies.

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

# 7 Security requirements

## 7.1 Security functional requirements

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality. This following table provides MRTD SFRs. The SFRs for Update Mechanism are in the next table.

| SFR in ST | SFR in [PP_PACE] | Descr. | Step | | | |
|---|---|---|---|---|---|---|
| | | | Before 5 | 5 | 6 | 7 |
| Class FAU *"Security Audit"* | | | | | | |
| FAU_SAS.1.1 | FAU_SAS.1.1 | 7.1.1.1 | ✓ | × | × | × |
| Class FCS *"Cryptographic Support"* | | | | | | |
| FCS_CKM.1.1/DH_PACE | FCS_CKM.1.1/DH_PACE | 7.1.2.1 | × | × | × | ✓ |
| FCS_CKM.1.1/MSK_DIV | Additional SFR | | × | ✓ | × | × |
| FCS_CKM.1.1/GP | | | × | ✓ | ✓ | × |
| FCS_CKM.1.1/CA | | | × | × | × | ✓ |
| FCS_CKM.1.1/KEY_GEN | | | × | ✓ | ✓ | × |
| FCS_CKM.4.1 | FCS_CKM.4.1 | 7.1.2.2 | × | ✓ | ✓ | ✓ |
| FCS_COP.1.1/PACE_ENC | FCS_COP.1.1/PACE_ENC | 7.1.2.3 | × | × | × | ✓ |
| FCS_COP.1.1/PACE_MAC | FCS_COP.1.1/PACE_MAC | | × | × | × | ✓ |
| FCS_COP.1.1/MSK_SHA | Additional SFR | | × | ✓ | × | × |
| FCS_COP.1.1/GP_ENC | | | × | ✓ | ✓ | × |
| FCS_COP.1.1/GP_AUTH | | | × | ✓ | ✓ | × |
| FCS_COP.1.1/GP_MAC | | | × | ✓ | ✓ | × |
| FCS_COP.1.1/GP_SDT_DEC | | | × | ✓ | ✓ | × |
| FCS_COP.1.1/CA_SHA | | | × | × | × | ✓ |
| FCS_COP.1.1/CA_ENC | | | × | × | × | ✓ |
| FCS_COP.1.1/CA_MAC | | | × | × | × | ✓ |
| FCS_COP.1.1/SIG_GEN | | | × | × | × | ✓ |
| FCS_COP.1.1/CA_DATA_GEN | | | × | × | × | ✓ |
| FCS_RND.1.1 | FCS_RND.1.1 | 7.1.2.4 | × | ✓ | ✓ | ✓ |
| Class FIA *"Identification and Authentication"* | | | | | | |
| FIA_UID.1.1/PACE | FIA_UID.1.1/PACE | 7.1.3.1 | × | ✓ | ✓ | ✓ |
| FIA_UID.1.2/PACE | FIA_UID.1.2/PACE | | × | ✓ | ✓ | ✓ |
| FIA_UID.1.1/PACE_CAM | Additional SFR | | × | ✓ | ✓ | ✓ |
| FIA_UID.1.2/PACE_CAM | | | × | ✓ | ✓ | ✓ |
| FIA_UAU.1.1/PACE | FIA_UAU.1.1/PACE | 7.1.3.2 | × | ✓ | ✓ | ✓ |
| FIA_UAU.1.2/PACE | FIA_UAU.1.2/PACE | | × | ✓ | ✓ | ✓ |
| FIA_UAU.1.1/PACE_CAM | Additional SFR | | × | ✓ | ✓ | ✓ |
| FIA_UAU.1.2/PACE_CAM | | | × | ✓ | ✓ | ✓ |
| FIA_UAU.4.1/PACE | FIA_UAU.4.1/PACE | 7.1.3.3 | × | ✓ | ✓ | ✓ |
| FIA_UAU.5.1/PACE | FIA_UAU.5.1/PACE | 0 | × | ✓ | ✓ | ✓ |
| FIA_UAU.5.2/PACE | FIA_UAU.5.2/PACE | | × | ✓ | ✓ | ✓ |
| FIA_UAU.5.2/PACE_CAM | Additional SFR | | × | ✓ | ✓ | ✓ |
| FIA_UAU.6.1/PACE | FIA_UAU.6.1/PACE | 7.1.3.5 | × | × | × | ✓ |
| FIA_UAU.6.1/MP | Additional SFR | | × | ✓ | ✓ | × |
| FIA_UAU.6.1/CA | | | × | × | × | ✓ |
| FIA_AFL.1.1/PACE | FIA_AFL.1.1/PACE | 7.1.3.6 | × | × | × | ✓ |
| FIA_AFL.1.2/PACE | FIA_AFL.1.2/PACE | | × | × | × | ✓ |
| FIA_AFL.1.1/MP | Additional SFR | | × | ✓ | ✓ | × |
| FIA_AFL.1.2/MP | | | × | ✓ | ✓ | × |

| SFR in ST | SFR in [PP_PACE] | Descr. | Step | | | |
|---|---|---|---|---|---|---|
| | | | Before 5 | 5 | 6 | 7 |
| FIA_API.1.1/CA | | 7.1.3.7 | × | × | × | ✓ |
| FIA_API.1.1/AA | | | × | × | × | ✓ |
| FIA_API.1.1/PACE_CAM | Additional SFR | | × | × | × | ✓ |
| Class FDP *"User Data Protection"* | | | | | | |
| FDP_ACC.1.1/TRM | FDP_ACC.1.1/TRM | 7.1.4.1 | × | × | × | ✓ |
| FDP_ACC.1.1/MP | Additional SFR | | × | ✓ | ✓ | × |
| FDP_ACC.1.1/ID | | | × | ✓ | ✓ | ✓ |
| FDP_ACF.1.1/TRM | FDP_ACF.1.1/TRM | 7.1.4.2 | × | × | × | ✓ |
| FDP_ACF.1.2/TRM | FDP_ACF.1.2/TRM | | × | × | × | ✓ |
| FDP_ACF.1.3/TRM | FDP_ACF.1.3/TRM | | × | × | × | ✓ |
| FDP_ACF.1.4/TRM | FDP_ACF.1.4/TRM | | × | × | × | ✓ |
| FDP_ACF.1.1/MP | Additional SFR | | × | ✓ | ✓ | × |
| FDP_ACF.1.2/MP | | | × | ✓ | ✓ | × |
| FDP_ACF.1.3/MP | | | × | ✓ | ✓ | × |
| FDP_ACF.1.4/MP | | | × | ✓ | ✓ | × |
| FDP_ACF.1.1/ID | | | × | ✓ | ✓ | ✓ |
| FDP_ACF.1.2/ID | | | × | ✓ | ✓ | ✓ |
| FDP_ACF.1.3/ID | | | × | ✓ | ✓ | ✓ |
| FDP_ACF.1.4/ID | | | × | ✓ | ✓ | ✓ |
| FDP_RIP.1.1 | FDP_RIP.1.1 | 7.1.4.3 | × | × | × | ✓ |
| FDP_UCT.1.1/TRM | FDP_UCT.1.1/TRM | 7.1.4.4 | × | × | × | ✓ |
| FDP_UCT.1.1/MP | Additional SFR | | × | ✓ | ✓ | × |
| FDP_UCT.1.1/CA | | | × | × | × | ✓ |
| FDP_UIT.1.1/TRM | FDP_UIT.1.1/TRM | 7.1.4.5 | × | × | × | ✓ |
| FDP_UIT.1.2/TRM | FDP_UIT.1.2/TRM | | × | × | × | ✓ |
| FDP_UIT.1.1/MP | Additional SFR | | × | ✓ | ✓ | × |
| FDP_UIT.1.2/MP | | | × | ✓ | ✓ | × |
| FDP_UIT.1.1/CA | | | × | × | × | ✓ |
| FDP_UIT.1.2/CA | | | × | × | × | ✓ |
| FDP_ITC.1.1/MP | | 7.1.4.6 | × | ✓ | ✓ | × |
| FDP_ITC.1.2/MP | | | × | ✓ | ✓ | × |
| FDP_ITC.1.3/MP | | | × | ✓ | ✓ | × |
| Class FMT *"Security Management"* | | | | | | |
| FMT_MOF.1.1/PROT | Additional SFR | 7.1.5.1 | × | ✓ | ✓ | × |
| FMT_MOF.1.1/GP | | | × | ✓ | ✓ | × |
| FMT_SMF.1.1 | FMT_SMF.1.1 | 7.1.5.2 | ✓ | ✓ | ✓ | × |
| FMT_SMR.1.1/PACE | FMT_SMR.1.1/PACE | 7.1.5.3 | × | ✓ | ✓ | ✓ |
| FMT_SMR.1.2/PACE | FMT_SMR.1.2/PACE | | × | ✓ | ✓ | ✓ |
| FMT_LIM.1.1 | FMT_LIM.1.1 | 7.1.5.4 | × | ✓ | ✓ | ✓ |
| FMT_LIM.2.1 | FMT_LIM.2.1 | 7.1.5.5 | × | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/INI_ENA | FMT_MTD.1.1/INI_ENA | 7.1.5.6 | × | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/INI_DIS | FMT_MTD.1.1/INI_DIS | | × | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/KEY_READ | FMT_MTD.1.1/KEY_READ | | ✓ | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/PA | FMT_MTD.1.1/PA | | × | × | ✓ | × |
| FMT_MTD.1.1/PACE_PWD | Additional SFR | | × | × | ✓ | × |
| FMT_MTD.1.1/CAPK | | | × | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/MP_KEY_WRITE | | | ✓ | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/AA_KEY_WRITE | | | × | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/LCS_PREP | | | × | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/LCS_PERS | | | × | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/AA_KEY_GEN | | | × | ✓ | ✓ | ✓ |
| FMT_MTD.1.1/CA_KEY_GEN | | | × | ✓ | ✓ | ✓ |
| Class FPT *"Protection of the Security Functions"* | | | | | | |

| SFR in ST | SFR in [PP_PACE] | Descr. | Step | | | |
|---|---|---|---|---|---|---|
| | | | Before 5 | 5 | 6 | 7 |
| FPT_EMS.1.1 | FPT_EMS.1.1 | 7.1.6.1 | × | ✓ | ✓ | ✓ |
| FPT_EMS.1.2 | FPT_EMS.1.2 | | × | ✓ | ✓ | ✓ |
| FPT_FLS.1.1 | FPT_FLS.1.1 | 7.1.6.2 | × | ✓ | ✓ | ✓ |
| FPT_TST.1.1 | FPT_TST.1.1 | 7.1.6.3 | × | ✓ | ✓ | ✓ |
| FPT_TST.1.2 | FPT_TST.1.2 | | × | ✓ | ✓ | ✓ |
| FPT_TST.1.3 | FPT_TST.1.3 | | × | ✓ | ✓ | ✓ |
| FPT_PHP.3.1 | FPT_PHP.3.1 | 7.1.6.4 | × | ✓ | ✓ | ✓ |
| Class FTP *"Trusted path/channels"* | | | | | | |
| FTP_ITC.1.1/PACE | FTP_ITC.1.1/PACE | 7.1.7.1 | × | × | × | ✓ |
| FTP_ITC.1.2/PACE | FTP_ITC.1.2/PACE | | × | × | × | ✓ |
| FTP_ITC.1.3/PACE | FTP_ITC.1.3/PACE | | × | × | × | ✓ |
| FTP_ITC.1.1/MP | Additional SFR | | × | ✓ | ✓ | × |
| FTP_ITC.1.2/MP | | | × | ✓ | ✓ | × |
| FTP_ITC.1.3/MP | | | × | ✓ | ✓ | × |

Table 16 – SFR of the TOE

The TOE SFR include also the PP module Update Mechanism Post-issuance SFRs mentioned with "/UPD": These SFRs are available Steps 5 to 7 of life cycle:

| SFR in ST and in [PP_0090] | Descr. | Step | | | | | |
|---|---|---|---|---|---|---|---|
| | | 3 | 4 Sch. 1 | 4 Sch. 2 | 5 | 6 | 7 |
| Class FAU "Security Audit" | | | | | | | |
| FAU_SAS.1/UPD | 7.1.1.1 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| Class FCS *"Cryptographic Support"* | | | | | | | |
| FCS_CKM.1/UPD_ITC | 7.1.2.1 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FCS_CKM.1/UPD_DEC | | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FCS_CKM.1/UPD_INT | | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FCS_CKM.4/UPD | 7.1.2.2 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FCS_COP.1/UPD_ITC | 7.1.2.3 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FCS_COP.1/UPD_DEC | | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FCS_COP.1/UPD_SIG | | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FCS_COP.1/UPD_INT | | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| Class FIA *"Identification and Authentication"* | | | | | | | |
| FIA_AFL.1/UPD | 7.1.3.6 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FIA_UID.1/UPD | 7.1.3.1 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FIA_UAU.1/UPD | 7.1.3.2 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| Class FDP *"User Data Protection"* | | | | | | | |
| FDP_ACC.1/UPD | 7.1.4.1 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FDP_ACF.1/UPD | 7.1.4.2 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FDP_IFC.1/UPD | 7.1.4.7 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FDP_IFF.1/UPD | 7.1.4.8 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FDP_RIP.1/UPD | 7.1.4.3 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| Class FMT *"Security Management"* | | | | | | | |
| FMT_SMF.1/UPD | 7.1.5.2 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FMT_MTD.1/UPD_SK_PICC | 7.1.5.6 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FMT_MTD.1/UPD_KEY_READ | | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| FMT_SMR.1/UPD | 7.1.5.3 | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| Class FPT *"Protection of the Security* | | | | | | | |

| SFR in ST and in [PP_0090] | | Descr. | | Step | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 3 | 4 Sch. 1 | 4 Sch. 2 | 5 | 6 | 7 |
| *Functions"* | | | | | | | | | |
| FPT_EMS.1 /UPD | 7.1.6.1 | ✓ | × | ✓ | ✓ | ✓ | ✓ | | |
| FPT_FLS.1/UPD | 7.1.6.2 | ✓ | × | ✓ | ✓ | ✓ | ✓ | | |
| FPT_TST.1/UPD | 7.1.6.3 | ✓ | × | ✓ | ✓ | ✓ | ✓ | | |
| FTP_ITC.1/UPD | 7.1.7.1 | ✓ | × | ✓ | ✓ | ✓ | ✓ | | |

Table 17 – SFR of the TOE for Update Mechanism

### 7.1.1 Class FAU *"Security Audit"*

#### 7.1.1.1 FAU_SAS.1 *"Audit Storage"*

Hierarchical to: No other components.

Dependencies: No dependencies

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

FAU_SAS.1.1/UPD The TSF shall provide **the TOE update functionality** with the capability to store **update log information and version history, namely the following data objects:_Update Package identification and associated hash** in the audit records.

### 7.1.2 Class FCS *"Cryptographic Support"*

#### 7.1.2.1 FCS_CKM.1 *"Cryptographic key generation"*

Hierarchical to: No other components.

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

FCS_CKM.1.1/ DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Algorithm]** and specified cryptographic key sizes **[Key size(s)]** that meet the following: **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **DH compliant to PKCS#3** | **1024 to 2048 bit by steps of 256 bits** | **[ICAO_9303]** |
| **ECDH compliant to [TR_03111]** | **192 to 521 bit** | |

FCS_CKM.1.1/ MSK_DIV The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **MSK derivation from initial MSK, using SHA-256** and specified cryptographic key sizes **256 bit** that meet the following: **none.**

*Application note*: In Step 5, (Master) MSK is diversified during the first command, and then replaced

by the derived MSK generated by FCS_CKM.1/MSK. The secure erasing of the keys is ensured by FCS_CKM.4.

FCS_CKM.1.1/ GP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Algorithm]** and specified cryptographic key sizes **[Key size(s)]** that meet the following: **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Triple-DES in CBC mode** | **112 bit** | **[GPC_SPE_034]; appendix E.4.1** |
| **AES in CBC mode** | **128, 192, 256 bit** | |

FCS_CKM.1.1/ CA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Algorithm]** and specified cryptographic key sizes **[Key size(s)]** that meet the following: **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **DH compliant to PKCS#3** | **1024 to 2048 bit by steps of 256 bits** | **[ICAO_9303]** |
| **ECDH compliant to [ISO_15946]** | **192 to 521 bit** | |

FCS_CKM.1.1/ KEY_GEN

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Algorithm] and specified cryptographic key sizes [key size(s)] that meet the following:[standard].

| Algorithm | key size(s) | standard |
|---|---|---|
| **RSA key generation** | **1024 to 3072 in steps of 256 bits** | **[ICAO_9303]** |
| **Key pair over Elliptic curve** | **192 to 521 bit with prime field p** | |

FCS_CKM.1.1/ UPD_ITC

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Algorithm]** and specified cryptographic key sizes **[Key size(s)]** that meet the following: **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Triple-DES in CBC mode** | **112 bit** | **[GPC_SPE_034]; appendix E.4.1** |
| **AES in CBC mode** | **128, 192, 256 bit** | |

FCS_CKM.1.1/ UPD_DEC

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **LSK derivation from Initial LSK and Derivation Data, using AES 128 ECB** and specified cryptographic key sizes **128 bit** that meet the following: **None.**

FCS_CKM.1.1/ UPD_INT

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **second LSK derivation from Initial LSK and Derivation Data, using AES 128 ECB** and specified cryptographic key sizes **128 bit** that meet the following:**None.**

#### 7.1.2.2 FCS_CKM.4 *"Cryptographic key destruction"*

Hierarchical to: No other components.

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

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

*Application note*: This SFR addresses the destruction of the MSK, ISK, and SM sessions keys.

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

*Application note*: This SFR addresses the destruction of the diversified LSK keys used for update mechanism sessions.

#### 7.1.2.3 FCS_COP.1 *"Cryptographic operation"*

Hierarchical to: No other components.

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

FCS_COP.1.1/ PACE_ENC The TSF shall perform **secure messaging – encryption and decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Triple-DES in CBC mode** | **112 bit** | [ICAO_9303] |
| **AES in CBC mode** | **128, 192 and 256 bit** | |

FCS_COP.1.1/ PACE_MAC The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Retail MAC** | **112 bit** | [ICAO_9303] |
| **AES CMAC** | **128, 192 and 256 bit** | |

FCS_COP.1.1/ MSK_SHA The TSF shall perform **hashing for MSK diversification** in accordance with a specified cryptographic algorithm **SHA-256** and cryptographic key sizes **none** that meets the following [FIPS_180_2]**.**

FCS_COP.1.1/ GP_ENC The TSF shall perform **secure messaging (GP) – encryption and decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following: **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Triple-DES in CBC mode** | **112 bit** | [FIPS_46_3] |
| **AES in CBC mode** | **128, 192 and 256 bit** | **[FIPS_197]** |

FCS_COP.1.1/ GP_AUTH The TSF shall perform **symmetric authentication – encryption and decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Triple-DES** | **112 bit** | **[FIPS_46_3]** |
| **AES** | **128, 192 and 256 bit** | **[FIPS_197]** |

*Application Note:* The Authentication Mechanisms based on Triple-DES is the authentication process performed in phases 5 and 6.

FCS_COP.1.1/ GP_MAC

The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following: **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **MAC Algorithm 1 with Padding M2** | **112 bit** | [ISO_9797_1] |
| **AES CMAC** | **128, 192 and 256 bit** | [NIST_800_38B] |

FCS_COP.1.1/ GP_SDT_DEC

The TSF shall perform **key decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following: **[Standard]**.

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Triple-DES in CBC mode** | **112 bit** | [FIPS_46_3] |
| **AES in CBC mode** | **128, 192 and 256 bit** | **[FIPS_197]** |

FCS_COP.1.1/ CA_SHA

The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1 and SHA-256** and cryptographic key sizes **none** that meets the following [FIPS_180_2]**.**

FCS_COP.1.1/ CA_ENC

The TSF shall perform **secure messaging – encryption and decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Triple-DES in CBC mode** | **112 bit** | **[ICAO_9303]** |
| **AES in CBC mode** | **128, 192 and 256 bit** | |

FCS_COP.1.1/ CA_MAC

The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Retail MAC** | **112 bit** | **[ISO_9797_1]** |
| **AES CMAC** | **128, 192 and 256 bit** | **[NIST_800_38B]** |

FCS_COP.1.1/ SIG_GEN

The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meet the following **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **RSA CRT with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512** | **1024 to 4096 bit by steps of 256 bits** | **[ISO_9796_2]** |
| **ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512** | **192 to 521 bit** | **[TR_03111]** |

FCS_COP.1.1/ CA_DATA_GEN

The TSF shall perform **chip authentication data generation** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meet the following: **[Standard]**.

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **Chip authentication data generation using DH keys compliant to PKCS#3** | **1024 to 2048 bit by steps of 256 bits** | **[ICAO_9303]** |
| **Chip authentication data generation using ECDH keys compliant to** [ISO_15946] | **192 to 521 bit** | **[ICAO_9303]** |

FCS_COP.1.1/ UPD_ITC

Cryptographic Operation – Inter Trusted Channel

The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key size(s)]** that meets the following **[Standard].**

| Algorithm | Key size(s) | Standard |
|---|---|---|
| **AES CMAC** | **128 bit** | [**NIST**_800_38B] |

FCS_COP.1.1/UPD_ DEC

Cryptographic Operation – Decryption of Update Packages

The TSF shall perform **decryption of update package** in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **128 bit** that meets the following **[FIPS_197]**

FCS_COP.1.1/UPD_ SIG

Cryptographic Operation – Signature Verification of Update Packages

The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **checksum verification** and cryptographic key sizes **256 bit** that meet the following **none.**

Application Note: 3 checksums SHA-256 provided by FCS_COP.1.1/UPD_INT are verified.

FCS_COP.1.1/ UPD_INT

Cryptographic Operation – Integrity Verification of Update Package

The TSF shall perform **integrity verification of update packages** in accordance with a specified cryptographic algorithm **SHA-256** and cryptographic key sizes **none** that meets the following **[FIPS_186_5].**

#### 7.1.2.4 FCS_RND.1 *"Quality metric for random numbers"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet:

**1. The requirement for random number generation following [SP800-90A] standard and [ANSSI-PG-083] recommendations.**

### 7.1.3 Class FIA *"Identification and Authentication"*

#### 7.1.3.1 FIA_UID.1 *"Timing of identification"*

Hierarchical to: No other components.

Dependencies: No dependencies.

| | |
|---|---|
| FIA_UID.1.1/ PACE | The TSF shall allow<br>**1. to establish the communication channel,**<br>**2. carrying out the PACE Protocol according to** [ICAO_9303]<br>**3. to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS**<br><br>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_UID.1.1/ PACE_CAM | The TSF shall allow<br>**1. to establish the communication channel,**<br>**2. carrying out the PACE Protocol following the Chip Authentication Mapping method according to** [ICAO_9303]<br>**3. to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS**<br>**4. to carry out the Terminal Authentication Protocol v.1 according to [ICAO_9303]**<br><br>on behalf of the user to be performed before the user is identified. |
| FIA_UID.1.2/ PACE_CAM | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |
| FIA_UID.1.1/UPD | The TSF shall allow<br>**1. to establish a communication channel,**<br>**2. to authenticate an update terminal by GP authentication**<br><br>on behalf of the user to be performed before the user is identified. |
| FIA_UID.1.2/UPD | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |

#### 7.1.3.2 FIA_UAU.1 *"Timing of authentication"*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1/ PACE — The TSF shall allow

1. **to establish the communication channel,**
2. **carrying out the PACE Protocol according to** [ICAO_9303]
3. **to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS,**

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.1.1/ PACE_CAM — The TSF shall allow

1. **to establish the communication channel,**
2. **carrying out the PACE Protocol following the Chip Authentication Mapping method according to** [ICAO_9303]
3. **to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS,**
4. **to carry out the Terminal Authentication Protocol v.1 according to** [ICAO_9303]

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

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

FIA_UAU.1.1/UPD — The TSF shall allow

1. **to establish a communication channel,**
2. **to authenticate an update terminal by GP authenticate.**
3. **to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/UPD_SK_PICC,**

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

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

#### 7.1.3.3 FIA_UAU.4 *"Single-use authentication mechanisms"*

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. **PACE Protocol according to** [ICAO_9303]**,**
2. **Authentication Mechanisms based on:**
   - **Triple-DES,**
   - **AES.**

*Application Note:* The Authentication Mechanisms based on Triple-DES is the authentication process performed in phases 5 and 6.

#### 7.1.3.4 FIA_UAU.5 "Multiple authentication mechanisms"

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/ PACE: The TSF shall provide

1. **PACE Protocol according to** [ICAO_9303]
2. **Passive Authentication according to** [ICAO_9303]
3. **Secure messaging in MAC-ENC mode according to** [ICAO_9303]
4. **Symmetric Authentication Mechanism based on:**
   - **Triple-DES,**
   - **AES**

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

1. **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.**
2. **The TOE accepts the authentication attempt as Personalisation Agent by the Authentication Mechanism with Personalization Agent Key(s).**
3. **The TOE accepts the authentication attempt as Personalisation Agent by the Authentication Mechanism with Pre-personalization Agent Key(s).**
4. **After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism**

FIA_UAU.5.2/ PACE_CAM: In addition to the rules from FIA_UAU.5.2/PACE, the TSF shall authenticate any user's claimed identity according to the **following rules:**

1. **After run of the PACE protocol following Chip Authentication Mapping method the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the PACE protocol.**
2. **The TOE accepts the authentication attempt by means of the**

| | |
|---|---|
| **Terminal public key Mapping the PACE** | **Authentication Protocol v.1 only if the terminal uses the presented during PACE following Chip Authentication method and the secure messaging established by means of protocol.** |

#### 7.1.3.5 FIA_UAU.6 *"Re-authenticating"*

Hierarchical to: No other components.

Dependencies: No dependencies.

| | |
|---|---|
| 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.6.1/ 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.** |
| *Application note* | This requirement applies to the authentication protocol used by (1) the Manufacturer and (2) the Personalization Agent |
| FIA_UAU.6.1/ CA | The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.** |

### 7.1.3.6 FIA_AFL.1 *"Authentication failure handling"*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1/ PACE: The TSF shall detect when **an administrator configurable positive integer within range of acceptable values 0 to 255 consecutive** unsuccessful authentication attempts occur related to **authentication attempts using the PACE password shared password**.

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

FIA_AFL.1.1/ MP: The TSF shall detect when **3** 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 or surpassed**, the TSF shall **wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the Authentication Mechanisms (based on Triple-DES or AES) attempts.**

FIA_AFL.1.1/ UPD: The TSF shall detect when **3** unsuccessful **update attempts** occurs related to **authentication of the Manufacturer and the Update Agent.**

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

FIA_AFL.1.1/ PIN/PUK: The TSF shall detect when **an administrator configurable positive integer** unsuccessful authentication attempts occur related to

1. **PACE using PIN/PUK**
2. **Verify PIN/PUK**

FIA_AFL.1.2/ PIN/PUK: When the defined number of unsuccessful authentication attempts has been **met,** the TSF shall **block the reference value of PIN/PUK credential**.

### 7.1.3.7 FIA_API.1 *"Authentication Proof of Identity"*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/ CA: The TSF shall provide a **Chip Authentication protocol according to** [ICAO_9303] to prove the identity of the **TOE**.

FIA_API.1.1/ AA: The TSF shall provide an **Active Authentication protocol according to** [ICAO_9303] to prove the identity of the **TOE**.

FIA_API.1.1/ PACE_CAM: The TSF shall provide a **Chip Authentication Mapping method for the PACE protocol according to** [ICAO_9303] to prove the identity of the **TOE**.

### 7.1.4 Class FDP *"User Data Protection"*

#### 7.1.4.1 FDP_ACC.1 *"Subset access control"*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ TRM: The TSF shall enforce the **Access Control SFP** on **terminals gaining access to the User Data stored in the travel document**.

FDP_ACC.1.1/ MP: The TSF shall enforce the **GP Access Control SFP** on **terminals gaining write, read and modification access to the Pre-Perso_K, the Perso_K, the LCS, the Configuration Data, the Update Package, the Active Authentication Keys (AA_PK and AA_SK) and the Chip Authentication Keys (CA_PK and CA_SK).**

FDP_ACC.1.1/ ID: The TSF shall enforce the **ID Access Control** on **terminals gaining write, read and modification access to the CPLC and the TOE_ID.**

FDP_ACC.1/UPD: **Subset Access Control – Terminal Access**
The TSF shall enforce the **Update Access Control SFP** on

**1) Subjects:**
**a)terminal,**
**b)update terminal.**

**2 )Objects:**
**a)version information identifying the TOE software**
**b)update package**
**c)update log information**

**3 )Operations:**
**a)reading out version information,**

**b)reading out log data,**
**c)uploading an update package on the TOE, or**
**d)initiating an update procedure**
**and none**[3].

#### 7.1.4.2 FDP_ACF.1 *"Basic Security attribute based access control"*

Hierarchical to: No other components.

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

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

**1. Subjects:**
**a. Terminal,**
**b. BIS-PACE;**

**2. Objects:**
**a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document**
**b. data in EF.DG3 of the logical travel document,**
**c. data in EF.DG4 of the logical travel documents,**

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

**3. Security attributes:**
- **a. Authentication status of terminals**
- **b. PACE PIN Authentication**

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:

1. **A BIS-PACE is allowed to read data objects from FDP_ACF.1/TRM according to** [ICAO_9303] **after a successful PACE**

FDP_ACF.1.3/ TRM — The TSF shall explicitly authorize 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:

**1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any data stored on the travel document.**
**2. Terminal not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document**

FDP_ACF.1.1/ MP — The TSF shall enforce the **GP Access Control SFP** to objects based on the following

**1. Subjects:**
- **a. Manufacturer,**
- **b. Personalization Agent,**

**2. Objects:**
- **a. the Pre-Perso_K,**
- **b. the Perso_K,**
- **c. the LCS,**
- **d the Configuration Data,**
- **e the Update Package,**
- **f. the Active Authentication Private Key,**
- **g. the Active Authentication Public Key,**
- **h. the Chip Authentication Private Key,**
- **i. the Chip Authentication Public Key.**

**3. Security attributes**
- **a. authentication status of the Manufacturer,**
- **b. authentication status of the Personalization Agent.**

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

**1. the Manufacturer is allowed to write the Pre-Perso_K, the Perso_K, the LCS and the Configuration Data,**
**2. the Manufacturer is allowed to read the Configuration Data and the LCS,**
**3. the Personalization Agent is allowed to write the Perso_K, the LCS and the Configuration Data,**
**4. the Personalization Agent is allowed to read the Configuration Data and the LCS,**
**5. the Manufacturer is allowed to load and activate the Update Package,**
**6. the Personalization Agent is allowed to import the Active Authentication Private Key,**
**7. the Personalization Agent is allowed to generate the Active Authentication Private Key and the Active Authentication Public Key**

**8. the Personalization Agent is allowed to import the Chip Authentication Private Key,**
**9. the Personalization Agent is allowed to generate the Chip Authentication Private Key and the Chip Authentication Public Key.**

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

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

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

**1. Subjects:**
- **a. Manufacturer,**
- **b. Personalization Agent,**
- **c. BIS-PACE,**
- **d. Terminal,**

**2. Objects:**
- **a. the TOE_ID,**
- **b. the CPLC,**

**3. Security attributes**
- **a. authentication status of the Manufacturer,**
- **b. authentication status of the Personalization Agent,**
- **c. authentication status of the terminal as BIS-PACE.**

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

**1. the Manufacturer is allowed to write and read the CPLC,**
**2. the Personalization Agent is allowed to write and read the CPLC,**
**3. the BIS-PACE is allowed to read the CPLC,**

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

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

**1. Any Terminal is not allowed to read the CPLC and the TOE_ID,**
**2. Any Terminal is not allowed to modify the CPLC.**

FDP_ACF.1.1/UPD — **Security Attribute based Access Control – Terminal Access**
The TSF shall enforce the **Update Access Control SFP** to objects based on the following:

**1. Subjects:**
- **a)terminal,**
- **b)update terminal**

**2. Objects:**
- **a)version information identifying the TOE software**
- **b)update package**
- **c)update log information**

**3. Security attributes:**
- **a)access rights**

**4. none.**

FDP_ACF.1.2/UPD The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
**The authentication level of a terminal must be determined by GP authenticate as required by FIA_UAU.1/UPD. Depending on the authentication level, an authenticated update terminal is allowed one or more of the following:**

**–read one or more data objects from FDP_ACF.1/UPD**

**–upload an update package to the TOE and initiate the update procedure.**

**The precise definition of access rights and how the authentication level is calculated from an authenticated terminal is defined in AGD_PRE.**

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

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

#### 7.1.4.3 FDP_RIP.1 *"Subset residual information protection"*

Hierarchical to: No other components.

Dependencies: No dependencies.

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:**

1. **Session Keys (immediately after closing related communication session),**
2. **the ephemeral private key ephem-Skpicc-PACE (by having generated a DH shared secret K)**

FDP_RIP.1/UPD 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:

1) **session keys (immediately after closing related communication session),**
2) **all ephemeral keys DIV_LSK and DIV2_LSK related to the update mechanism.**
3) **Update package, decrypted update data and meta-data uploaded to the TOE or generated during the update procedure.**
4) **none.**

#### 7.1.4.4 FDP_UCT.1 *"Basic data exchange confidentiality"*

Hierarchical to: No other components.

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

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

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

*Application Note:* Additional SFR FDP_UCT.1/MP enforces confidentiality of data import and export in steps 5 and 6.

FDP_UCT.1.1/ CA — The TSF shall enforce the **CA Access Control SFP** to be able to **transmit and receive** user data in a manner protected from unauthorized disclosure **after Chip Authentication.**

#### 7.1.4.5 FDP_UIT.1 *"Data exchange integrity"*

Hierarchical to: No other components.

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

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

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

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

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

*Application Note:* Additional SFR FDP_UIT.1/MP enforces integrity of data import and export in steps 5 and 6.

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

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

#### 7.1.4.6 FDP_ITC.1 *"Import of user data without security attributes"*

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1/ MP — The TSF shall enforce the **GP Access Control SFP** when importing user data, controlled under the SFP, from outside the TOE.

| | |
|---|---|
| FDP_ITC.1.2/ MP | The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE. |
| FDP_ITC.1.3/ MP | The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **sensitive data (Pre-Perso_K, Perso_K, PACE_PWD, CA_SK and AA_SK) shall be encrypted.** |
| *Application Note:* | Additional SFR FDP_ITC.1/MP enforces confidentiality of sensitive data import in steps 5 and 6. |

#### 7.1.4.7 FDP_IFC.1/UPD *"Subset information flow control*

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFF.1 Simple security attributes, fulfilled by FDP_IFF.1/UPD]

FDP_IFC.1.1/UPD The TSF shall enforce the **Update Flow Control SFP** on **the following**:

**1. Subjects:**
a) **terminal**,
b) **update terminal**.

**2. information:**
a) **update package**
b) **update data**
c) **meta-data, such as version information**

**3. operations:**
a) **performing an update**.

#### 7.1.4.8 FDP_IFF.1/UPD *"S*imple security attributes".

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control: fulfilled by FDP_IFC.1/UPD

FDP_IFF.1.1/UPD The TSF shall enforce the **Update Control SFP** based on the following types of subject and information security attributes:

**1. Subjects:**
a) **terminal**,
b) **update terminal**.

**2. information:**
a) **update package**
b) **update data**
c) **meta-data, such as version information**

**3. security attributes:**
a) **update package verification status with the values: NOT VERIFIED (default status), SUCCESSFULLY VERIFIED, and VERIFICATION FAILED.**

FDP_IFF.1.2/UPD The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. **The terminal has established a secure channel with the TOE.**

2. **The TOE shall only accept update packages sent via a secure channel established with an authenticated update terminal.**

FDP_IFF.1.3/UPD The TSF shall enforce the **following rules in their specific order:**

1) **The integrity (using the keyed or unkeyed hash function cf. FCS_COP.1/UPD_INT) and authenticity (using the digital signature, cf. FCS_COP.1/UPD_SIG) of the first part of the update package is verified. If the integrity and authenticity are not both validated, abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.**
2) **The first part of the update package is only decrypted, cf. FCS_COP.1/UPD_DEC, if the integrity and authenticity of the that part has been verified in rule 1. If the decryption fails, abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.**
3) **If all parts of the update package have been decrypted, continue with rule 4. Otherwise, apply rules 1. and 2. on the remaining parts (replace 'first part' with 'current part' above) until either all parts have been decrypted, or the procedure has been aborted with VERIFICATION FAILED.**
4) **If additional meta-data is stored in the update package Signature of the update package is not verified as correct according to SHA-256 signature the security attribute is set to VERIFICATION FAILED and the update package including all associated data are destroyed, cf. FDP_RIP.1. Correctness w.r.t. the referenced technical specification must not contradict any of the given rules here.**
5) **Next, the TSF shall verify that:**

a) **the version number of the update package must be greater than the version of the installed corresponding software package;**
b) **the update data are suitable to the specific TOE configuration/platform by checking relevant meta-data ( i.e. TOE product identifier, version number etc.).**

**If all conditions in step 5 are verified, the verification status is set to SUCCESSFULLY VERIFIED. Otherwise abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.**

**Only if the verification status is SUCCESSFULLY VERIFIED, the TOE shall install the update data.**

FDP_IFF.1.4/UPD The TSF shall explicitly authorize an information flow based on the following rules: **none**

FDP_IFF.1.5/UPD The TSF shall explicitly deny an information flow based on the following rules: **none.**

### 7.1.5 Class FMT *"Security Management"*

#### *7.1.5.1* FMT_MOF *"Management of functions in TSF"*

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1/ PROT

The TSF shall restrict the ability to **enable** the functions

- **Active Authentication,**
- **Chip Authentication v1**
- **Chip Authentication v1 through MSE: SET KAT**
- **Chip Authentication Mapping method for PACE**

to **the Manufacturer**.

FMT_MOF.1.1/ GP

The TSF shall restrict the ability to **enable** the functions

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

to **the Manufacturer and the Personalization Agent**.

#### 7.1.5.2 FMT_SMF.1 *"Specification of Management Functions"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

FMT_SMF.1.1

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

1. **Initialization**
2. **Pre-personalization**
3. **Personalization**
4. **Configuration**

FMT_SMF.1.1/UPD

The TSF shall provide **the TOE update functionality** with the capability to store **update log information and version history, namely the following data objects: Update Package identification and associated hash** in the audit records.

#### 7.1.5.3 FMT_SMR.1 *"Security roles"*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1/ PACE

The TSF shall maintain the roles:

1. **Manufacturer,**
2. **Personalization Agent,**
3. **Terminal,**
4. **PACE authenticated BIS-PACE.**

FMT_SMR.1.2/ PACE

The TSF shall be able to associate users with roles.

FMT_SMR.1.1/UPD The TSF shall maintain the roles:

**1. Terminal,**
**2. Update terminal,**
**3. Update key installation agent**

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

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

#### 7.1.5.4 FMT_LIM.1 *"Limited capabilities"*

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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

**Deploying Test Features after TOE Delivery does not allow**
**1. User Data to be manipulated and disclosed,**
**2. TSF data to be manipulated or disclosed,**
**3. software to be reconstructed and,**
**4. substantial information about construction of TSF to be gathered which may enable other attacks**.

#### 7.1.5.5 FMT_LIM.2 *"Limited availability"*

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

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

**Deploying Test Features after TOE Delivery does not allow**
**1. User Data to be manipulated and disclosed,**
**2. TSF data to be manipulated or disclosed,**
**3. software to be reconstructed and,**
**4. substantial information about construction of TSF to be gathered which may enable other attacks**.

*Application note (25 in* [PP_PACE]*):* The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that:

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

or conversely

(ii)the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

### 7.1.5.6 FMT_MTD.1 *"Management of TSF data"*

Hierarchical to: No other components.

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

| | |
|---|---|
| FMT_MTD.1.1/ INI_ENA | The TSF shall restrict the ability to **write** the **Initialization Data and Pre-personalization Data** to **the Manufacturer.** |
| FMT_MTD.1.1/ INI_DIS | The TSF shall restrict the ability to **disable read access for users to** the **Initialization Data** to **the Personalization Agent.** |
| FMT_MTD.1.1/ KEY_READ | The TSF shall restrict the ability to **read** the<br>**1. PACE passwords,**<br>**2. Pre-personalization Agent Keys,**<br>**3. Personalization Agent Keys,**<br>**4. Chip Authentication Private Key,**<br>**5. Active Authentication Private Key,**<br>**6. Manufacturer Keys**<br>to **none** |
| FMT_MTD.1.1/ PA | The TSF shall restrict the ability to **write** the **Document Security Object (SOD)** to **the Personalization Agent.** |
| FMT_MTD.1.1/ PACE_PWD | The TSF shall restrict the ability to **load** the **PACE Password** to **the Personalization Agent.** |
| FMT_MTD.1.1/ CAPK | The TSF shall restrict the ability to **load** the **Chip Authentication Private Key** to **the Personalization Agent.** |
| FMT_MTD.1.1/ MP_KEY_WRITE | The TSF shall restrict the ability to **write** the **Pre-personalization Agent Keys and the Personalization Agent Keys** to **the Manufacturer.** |
| FMT_MTD.1.1/ AA_KEY_WRITE | The TSF shall restrict the ability to **write** the **Active Authentication Private Key** to **the Personalization Agent.** |
| FMT_MTD.1.1/ LCS_PREP | The TSF shall restrict the ability **to switch** the **LCS from phase 5 to phase 6** to **the Manufacturer.** |
| 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.1.1/ AA_KEY_GEN | The TSF shall restrict the ability to **generate** the **Active Authentication Keys (AA_PK and AA_SK)** to **the Personalization Agent.** |
| FMT_MTD.1.1/ CA_KEY_GEN | The TSF shall restrict the ability to **generate** the **Chip Authentication Keys (CA_PK and CA_SK)** to **the Personalization Agent.** |
| FMT_MTD.1.1/UPD_SK_PICC | The TSF shall restrict the ability to **create, load** the **LSK** to **the update key installation agent** |

Application Note: The update key installation agent is the Manufacturer.

| | |
|---|---|
| FMT_MTD.1.1/UPD_KEY_READ | The TSF shall restrict the ability to **read** the<br>1)**LSK**<br>2)**DIV_LSK and DIV2_LSK** |

| | |
|---|---|
| | to none. |
| FMT_MTD.1/Initialize_PIN | The TSF shall restrict the ability to **write** the initial **PIN and PUK** to **the personalization agent** |
| FMT_MTD.1/Resume_PIN | The TSF shall restrict the ability to **resume** the **suspended PIN** to **the electronic document holder.**<br>*Application Note* : Resuming is a two-step procedure, subsequently using PACE with the CAN and PACE with the PIN. It must be implemented according to **[TR_03110]** Part 2, and is relevant for the status as required by FIA_AFL.1/ PIN/PUK. The electronic document holder is authenticated as required by FIA_UAU.1/PACE using the PIN as the shared password. |
| FMT_MTD.1/Change_PIN | The TSF shall restrict the ability to **change** the **blocked PIN** to **the authorised identified roles that match the list of PIN changing rules conformant to [TR_03110]** |
| FMT_MTD.1/Unblock_PIN | The TSF shall restrict the ability to **unblock** the **blocked PIN** to<br>1. **the electronic document holder (using the PUK for unblocking),**<br>2. **a PACE terminal of a type that has the terminal authorization level for PIN management**.<br><br>*Application Note* : The unblocking procedure must be implemented according to **[TR_03110]**, and is relevant for the status as required by FIA_AFL.1/Block_PIN. It can be triggered by either (i) the electronic document holder being authenticated as required by FIA_UAU.1/PACE using the PUK as the shared password or (ii) an PACE terminal (FIA_UAU.1/PACE) that proved a terminal authorization level being sufficient for PIN management (FDP_ACF.1/TRM). |
| FMT_MTD.1/Activate_PIN | The TSF shall restrict the ability to **activate and deactivate** the **PIN** to **an PACE terminal of a type that has the terminal authorization level for PIN management.**<br>*Application Note* : The activation/deactivation procedures must be implemented according to **[TR_03110]**. They can be triggered by a terminal (FIA_UAU.1/PACE) that proved a terminal authorization level sufficient for PIN management (FDP_ACF.1/TRM). |

### 7.1.6 Class FPT *"Protection of the Security Functions"*

#### 7.1.6.1 FPT_EMS.1 *"TOE Emanation"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

1. **Chip Authentication Session Keys**
2. **PACE session keys (PACE-Kmac, PACE-Kenc),**
3. **the ephemeral private key ephem-Skpicc-PACE,**
4. - **Chip Authentication Public Key,**
   - **Active Authentication Private Key,**
   - **Active Authentication Public Key,**
   - **Pre-personalization Agent Keys,**
   - **CPLC,**
   - **TOE_ID,**
   - **TOE Life Cycle State,**
   - **Configuration Data,**
   - **Update package.**
5. **Personalization Agent Key(s),**
6. **Chip Authentication Private Key and**
7. - **Personal Data including Biometric Data,**
   - **EF.COM,**
   - **EF.SOD,**
   - **Updatable data**

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

1. **Chip Authentication Session Keys**
2. **PACE session keys (PACE-Kmac, PACE-Kenc),**
3. **the ephemeral private key ephem-Skpicc-PACE,**
4. - **Chip Authentication Public Key,**
   - **Active Authentication Private Key,**
   - **Active Authentication Public Key,**
   - **Pre-personalization Agent Keys,**
   - **CPLC,**
   - **TOE_ID,**
   - **TOE Life Cycle State,**
   - **Configuration Data,**
5. **Personalization Agent Key(s),**
6. **Chip Authentication Private Key and**
7. - **Personal Data including Biometric Data,**
   - **EF.COM,**
   - **EF.SOD.**

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

1. **Update Package ID,**
2. **The LSK, derived LSK, derived MSK,**
3. **Secure Messaging Session Keys,**
4. **Update Package signature Keys.**

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

**1. Update Package ID,**
**2. The LSK, DIV_LSK, DIV2_LSK, derived MSK**
**3. Secure Messaging Session Keys,**
and **Update Package signature Keys.**

### 7.1.6.2 FPT_FLS.1 *"Failure with preservation of secure state"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

**1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,**
**2. failure detected by TSF according to FPT_TST.1.**

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

**1. Failure during a transmission of the update package data file**
**2. Failure detected by TSF according to FPT_TST.1**
3. **Failure detected after a failed update**

### 7.1.6.3 FPT_TST.1 *"TSF testing"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

- **At reset,**
- **Before any cryptographic operation,**
- **When accessing a DG or any EF,**
- **Prior to any use of TSF data,**
- **Before execution of any command,**
- **When performing a PACE authentication,**
- **When performing the EAC Authentication,**
- **When performing the Active Authentication.**

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

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

**1. during initial start-up,**
**2. after a software update**

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

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

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

#### 7.1.6.4 FPT_PHP.3 *"Resistance to physical attack"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

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.

### 7.1.7 Class FTP "Trusted path/channels"

#### 7.1.7.1 FTP_ITC.1 *"Inter-TSF trusted channel"*

Hierarchical to: No other components.

Dependencies: No Dependencies.

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 The TSF shall **enforce** communication via the trusted channel for **any data exchange between the TOE and the Terminal.**

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 and AA_SK) shall be encrypted.**

FTP_ITC.1.1/UPD The TSF shall provide a communication channel between itself and **an update terminal** 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/UPD The TSF shall permit **an update terminal** to initiate communication via the trusted channel.

FTP_ITC.1.3/UPD The TSF shall **enforce** communication via the trusted channel for **any data exchange between the TOE and the Terminal.**

## 7.2 Security assurance requirements

- The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 5 (EAL5) and augmented by taking the following component: ADV_IMP.2, ADV_INT.3 , ADV_TDS.5, ALC_CMC.5, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, ALC_FLR.3, ALC_DVS.2 and AVA_VAN.5.

### 7.2.1 EAL rationale

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

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

### 7.2.2 EAL augmentation rationale

#### 7.2.2.1 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.

#### 7.2.2.2 AVA_VAN.5 "Advanced methodical vulnerability analysis" and others augmentations

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package pre-defined in [PP_PACE], namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3, entry 'Attacker' in [PP_PACE]). This decision represents a part of the conscious security policy for the travel document required by the travel document Issuer and reflected by the [PP_PACE].

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"

Also to enforce security and conformity for this type of TOE, these augmentations ahs been chosen: ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, ALC_FLR.3, added to ALC_DVS.2 and AVA_VAN.5.

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

### 7.2.3 Dependencies

| SAR | Dependencies | Support of the Dependencies |
|---|---|---|
| ADV_ARC.1 | ADV_FSP.1<br>ADV_TDS.1 | ADV_FSP.5<br>ADV_TDS.5 |
| ADV_FSP.5 | ADV_TDS.1<br>ADV_IMP.1 | ADV_TDS.5<br>ADV_IMP.2 |

| SAR | Dependencies | Support of the Dependencies |
|---|---|---|
| ADV_IMP.2 | ADV_TDS.3<br>ALC_TAT.1<br>ALC_CMC.5 | ADV_TDS.5<br>ALC_TAT.3<br>ALC_CMC.5 |
| ADV_INT.3 | ADV_IMP.1<br>ADV_TDS.3<br>ALC_TAT.1 | ADV_IMP.2<br>ADV_TDS.5<br>ALC_TAT.3 |
| ADV_TDS.5 | ADV_FSP.5 | ADV_FSP.5 |
| AGD_OPE.1 | ADV_FSP.1 | ADV_FSP.5 |
| AGD_PRE.1 | No dependencies | n.a. |
| ALC_CMC.5 | ALC_CMS.1<br>ALC_DVS.2<br>ALC_LCD.1 | ALC_CMS.5<br>ALC_DVS.2<br>ALC_LCD.1 |
| ALC_CMS.5 | No dependencies | n.a. |
| ALC_DEL.1 | No dependencies | n.a. |
| ALC_DVS.2 | No dependencies | n.a. |
| ALC_LCD.1 | No dependencies | n.a. |
| ALC_TAT.3 | ADV_IMP.1 | ADV_IMP.2 |
| ASE_CCL.1 | ASE_INT.1<br>ASE_ECD.1<br>ASE_REQ.1 | ASE_INT.3<br>ASE_ECD.1<br>ASE_REQ.2 |
| ASE_ECD.1 | No dependencies | n.a. |
| ASE_INT.1 | No dependencies | n.a. |
| ASE_OBJ.2 | ASE_SPD.1 | ASE_SPD.1 |
| ASE_REQ.2 | ASE_OBJ.2<br>ASE_ECD.1 | ASE_OBJ.2<br>ASE_ECD.1 |
| ASE_SPD.1 | No dependencies | n.a. |
| ASE_TSS.1 | ASE_INT.1<br>ASE_REQ.1<br>ADV_FSP.1 | ASE_INT.3<br>ASE_REQ.2<br>ADV_FSP.5 |
| ATE_COV.3 | ADV_FSP.2<br>ATE_FUN.2 | ADV_FSP.5<br>ATE_FUN.2 |
| ATE_DPT.3 | ADV_ARC.1<br>ADV_TDS.4<br>ATE_FUN.1 | ADV_ARC.1<br>ADV_TDS.5<br>ATE_FUN.2 |
| ATE_FUN.2 | ATE_COV.1 | ATE_COV.3 |
| ATE_IND.2 | ADV_FSP.2<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_COV.1<br>ATE_FUN.1 | ADV_FSP.5<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_COV.3<br>ATE_FUN.2 |
| AVA_VAN.5 | ADV_ARC.1<br>ADV_FSP.4<br>ADV_TDS.3<br>ADV_IMP.1<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_DPT.1 | ADV_ARC.1<br>ADV_FSP.5<br>ADV_TDS.5<br>ADV_IMP.2<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_DPT.3 |
| ALC_FLR.3 | No dependencies | n.a. |

Table 18 – SARs dependencies

## 7.3 Security requirements rationale

### 7.3.1 Security Functional Requirements Rationale

#### 7.3.1.1 Overview

The following table provides an overview for security functional requirements coverage.
The rational for Update mechanism is in Table 20, for other SFRs is in Table 19.

| SFR \ SO | OT.Data_Integrity | OT.Data_Authenticity | OT.Data_Confidentiality | OT.Tracing | OT.Prot_Abuse-Func | OT.Prot_Inf_Leak | OT.Prot_Phys-Tamper | OT.Prot_Malfunction | OT.Identification | OT.AC_Pers | OT.Configuration | OT.Chip_Auth_Proof |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FAU_SAS.1 | | | | | | | | | x | x | | |
| FCS_CKM.1/DH_PACE | x | x | x | | | | | | | | | x |
| FCS_CKM.1/MSK_DIV | | | | | | | | | | | x | |
| FCS_CKM.1/GP | | | | | | | | | | | x | |
| FCS_CKM.1/CA | x | x | x | | | | | | | x | | x |
| FCS_CKM.1/KEY_GEN | | | | | | | | | | x | | |
| FCS_CKM.4 | x | x | x | | | | | | | x | | |
| FCS_COP.1/PACE_ENC | | | x | | | | | | | | | x |
| FCS_COP.1/PACE_MAC | x | x | | | | | | | | | | |
| FCS_COP.1/MSK_SHA | | | | | | | | | | | x | |
| FCS_COP.1/GP_ENC | | | | | | | | | | | x | |
| FCS_COP.1/GP_AUTH | | | | | | | | | | | x | |
| FCS_COP.1/GP_MAC | | | | | | | | | | | x | |
| FCS_COP.1/GP_SDT_DEC | | | | | | | | | | | x | |
| FCS_COP.1/CA_SHA | x | | x | | | | | | | | | x |
| FCS_COP.1/CA_ENC | x | | x | | | | | | | x | | x |
| FCS_COP.1/CA_MAC | x | | x | | | | | | | x | | x |
| FCS_COP.1/SIG_GEN | | | | | | | | | | | | x |
| FCS_COP.1/CA_DATA_GEN | | | | | | | | | | | | x |
| FCS_RND.1 | x | x | x | | | | | | | x | | |
| FIA_UID.1/PACE | x | x | x | | | | | | | x | | |
| FIA_UID.1/PACE_CAM | x | x | x | | | | | | | x | | x |
| FIA_UAU.1/PACE | x | x | x | | | | | | | x | | |
| FIA_UAU.1/PACE_CAM | x | x | x | | | | | | | x | | x |
| FIA_UAU.4/PACE | x | x | x | | | | | | | x | | x |
| FIA_UAU.5/PACE | x | x | x | | | | | | | x | | |
| FIA_UAU.5/PACE_CAM | x | x | x | | | | | | | x | | x |
| FIA_UAU.6/PACE | x | x | x | | | | | | | | | x |
| FIA_UAU.6/MP | x | x | x | | | | | | | x | x | |
| FIA_UAU.6/CA | x | | x | | | | | | | | | |
| FIA_AFL.1/PACE | | | | x | | | | | | | | |
| FIA_AFL.1/PIN/PUK | | | x | x | x | | | | | | | x |
| FIA_AFL.1/MP | | | | | | | | | | x | x | |
| FIA_API.1/CA | | | | | | | | | | | | x |

| SFR \ SO | OT.Data_Integrity | OT.Data_Authenticity | OT.Data_Confidentiality | OT.Tracing | OT.Prot_Abuse-Func | OT.Prot_Inf_Leak | OT.Prot_Phys-Tamper | OT.Prot_Malfunction | OT.Identification | OT.AC_Pers | OT.Configuration | OT.Chip_Auth_Proof |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FIA_API.1/AA | | | | | | | | | | | | x |
| FIA_API.1/PACE_CAM | | | | x | | | | | | | | x |
| FDP_ACC.1/TRM | x | | x | | | | | | | x | | |
| FDP_ACC.1/MP | | | | | | | | | | | x | |
| FDP_ACC.1/ID | | | | | | | | | x | x | x | |
| FDP_ACF.1/TRM | x | | x | | | | | | | x | | |
| FDP_ACF.1/MP | | | | | | | | | | | x | |
| FDP_ACF.1/ID | | | | | | | | | x | x | x | |
| FDP_RIP.1 | x | x | x | | | | | | | | | |
| FDP_UCT.1/TRM | x | | x | | | | | | | | | |
| FDP_UCT.1/MP | x | | | | | | | | | x | | |
| FDP_UIT.1/TRM | x | | x | | | | | | | | | |
| FDP_UIT.1/MP | x | | | | | | | | | x | x | |
| FDP_ITC.1/MP | | | | | | | | | | | x | |
| FMT_MOF.1/PROT | | | | | | | | | | | x | x |
| FMT_MOF.1/GP | x | | | | | | | | | | | x |
| FMT_SMF.1 | x | x | x | | | | | | x | x | x | x |
| FMT_SMR.1/PACE | x | x | x | | | | | | x | x | x | x |
| FMT_LIM.1 | | | | | x | | | | | | | |
| FMT_LIM.2 | | | | | x | | | | | | | |
| FMT_MTD.1/INI_ENA | | | | | | | | | x | x | | |
| FMT_MTD.1/INI_DIS | | | | | | | | | x | x | | |
| FMT_MTD.1/KEY_READ | x | x | x | | | | | | | x | | x |
| FMT_MTD.1/PA | x | x | x | | | | | | | x | | |
| FMT_MTD.1/PACE_PWD | | | | | | | | | | x | | |
| FMT_MTD.1/CAPK | x | | | | | | | | | | | x |
| FMT_MTD.1/MP_KEY_WRITE | x | | | | | | | | | | x | |
| FMT_MTD.1/AA_KEY_WRITE | | | | | | | | | | x | | x |
| FMT_MTD.1/LCS_PREP | | | | | | | | | | x | x | |
| FMT_MTD.1/LCS_PERS | | | | | | | | | | x | | |
| FMT_MTD.1/AA_KEY_GEN | | | | | | | | | | x | | |
| FMT_MTD.1/CA_KEY_GEN | | | | | | | | | | x | | |
| FMT_MTD.1/Initialize_PIN | | | x | x | x | | | | | | | x |
| FMT_MTD.1/Resume_PIN | | | x | x | x | | | | | | | x |
| FMT_MTD.1/Change_PIN | | | x | x | x | | | | | | | x |
| FMT_MTD.1/Unblock_PIN | | | x | x | x | | | | | | | x |
| FMT_MTD.1/Activate_PIN | | | x | x | x | | | | | | | x |
| FPT_EMS.1 | | | | | | x | | | | x | | |
| FPT_FLS.1 | | | | | | x | | x | | | | |
| FPT_TST.1 | | | | | | x | | x | | | | |
| FPT_PHP.3 | x | | | | | x | x | | | | | |
| FTP_ITC.1/PACE | x | x | x | x | | | | | | | | |
| FTP_ITC.1/MP | | | | | | | | | | | x | |

Table 19 - SFRs and Security Objectives

| SO / SFR | OT.Update_Mechanism | OT.Enc_Sign_Update | OT.Update_Terminal_Auth | OT.Attack_Detection | OT.Key_Secrecy |
|---|---|---|---|---|---|
| Class FCS | | | | | |
| FCS_COP.1/UPD_ITC | X | X | | | |
| FCS_CKM.1/UPD_ITC | X | X | | | |
| FCS_COP.1/UPD_DEC | X | X | | | |
| FCS_CKM.1/UPD_DEC | X | X | | | |
| FCS_COP.1/UPD_INT | X | X | | | |
| FCS_CKM.1/UPD_INT | X | X | | | |
| FCS_COP.1/UPD_SIG | X | X | | | |
| FCS_CKM.4/UPD | X | X | | | |
| Class FIA | | | | | |
| FIA_AFL.1/UPD | X | | X | | |
| FIA_UID.1/UPD | X | | X | | |
| FIA_UAU.1/UPD | X | | X | | |
| Class FDP | | | | | |
| FDP_ACC.1/UPD | X | | X | | |
| FDP_ACF.1/UPD | X | | X | | |
| FDP_IFC.1/UPD | X | | X | | |
| FDP_IFF.1/UPD | X | | X | | |
| FDP_RIP.1/UPD | X | | | | |
| Class FAU | | | | | |
| FAU_SAS.1/UPD | X | | | X | |
| Class FMT | | | | | |
| FMT_SMF.1/UPD | X | | | | |
| FMT_MTD.1/UPD_SK_PICC | | X | X | | X |
| FMT_MTD.1/UPD_KEY_READ | | X | X | | X |
| FMT_SMR.1/UPD | | X | X | | X |
| Class FPT | | | | | |
| FPT_EMS.1/UPD | | | | | X |
| FPT_FLS.1/UPD | | | | X | |
| FPT_TST.1/UPD | | | | X | |
| Class FTP | | | | | |
| FTP_ITC.1/UPD | X | | X | | |

Table 20- SFRs and Security Objectives for Update mechanism.

#### 7.3.1.2 OT.Data_Integrity

The security objective **OT.Data_Integrity** *"Integrity of Data"* aims that the TOE always ensures integrity of the User- and TSF-data stored and, after the PACE authentication, of these data exchanged (physical manipulation and unauthorised modifying). The TOE supports ***FCS_COP.1/MSK_SHA*** for integrity check of master key. Physical manipulation is addressed by ***FPT_PHP.3***.Logical manipulation of stored user data is addressed by (***FDP_ACC.1***, ***FDP_ACF.1***). ***FIA_UAU.4/PACE***, ***FIA_UAU.5/PACE*** and ***FCS_CKM.4*** represent some required specific properties of the protocols used.Unauthorised modifying of the exchanged data is addressed, in the first

line, by ***FDP_UCT.1/TRM***, ***FDP_UIT.1/TRM*** and ***FTP_ITC.1/PACE*** using ***FCS_COP.1/PACE_MAC***. A prerequisite for establishing this trusted channel is a successful PACE Authentication (***FIA_UID.1/PACE***, ***FIA_UAU.1/PACE***) using ***FCS_CKM.1/DH_PACE*** and possessing the special properties ***FIA_UAU.5/PACE***, ***FIA_UAU.6/PACE***. ***FDP_RIP.1*** requires erasing the values of session keys (here: for KMAC).
Since PACE can use the PIN as the shared secret, using and management of PIN (***FIA_AFL.1/PIN/PUK***, ***FMT_MTD.1/Resume_PIN***, ***FMT_MTD.1/Change_PIN***, ***FMT_MTD.1/Unblock_PIN***, ***FMT_MTD.1/Activate_PIN,*** ***FMT_MTD.1/Initialize_PIN*****)** also support achievement of this objective. **FDP_RIP.1** requires erasing the temporal values of PIN, PUK.
The SFR ***FMT_MTD.1/KEY_READ*** restricts the access to the PACE passwords.***FMT_MTD.1/PA*** requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy.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.

#### 7.3.1.3 OT.Data_Authenticity

The security objective **OT.Data_Authenticity** *"Authenticity of Data"* 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 Authentication (***FIA_UID.1/PACE***, ***FIA_UAU.1/PACE***) using ***FCS_CKM.1/DH_PACE*** and possessing the special properties ***FIA_UAU.5/PACE***, ***FIA_UAU.6/PACE***. ***FDP_RIP.1*** requires erasing the values of session keys (here: for KMAC). Since PACE can use the PIN as the shared secret, using and management of PIN (***FIA_AFL.1/PIN/PUK***, ***FMT_MTD.1/Resume_PIN***, ***FMT_MTD.1/Change_PIN***, ***FMT_MTD.1/Unblock_PIN***, ***FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PIN*****)** also support achievement of this objective.
The ***SFR FMT_MTD.1/KEY_READ*** restricts the access to the PACE passwords. ***FMT_MTD.1/PA*** requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy.***FIA_UAU.4/PACE***, ***FIA_UAU.5/PACE*** and ***FCS_CKM.4*** represent some required specific properties of the protocols used. The SFR ***FCS_RND.1*** represents a general support for cryptographic operations needed. The SFRs ***FMT_SMF.1*** and ***FMT_SMR.1/PACE*** support the functions and roles related.

#### 7.3.1.4 OT.Data_Confidentiality

The security objective **OT.Data_Confidentiality** *"Confidentiality of Data"* aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication, of these data exchanged.This objective for the data stored is mainly achieved by (***FDP_ACC.1/TRM***, ***FDP_ACF.1/TRM***).***FIA_UAU.4/PACE***, ***FIA_UAU.5/PACE*** and ***FCS_CKM.4*** represent some required specific properties of the protocols used.This objective for the data exchanged is mainly achieved by ***FDP_UCT.1/TRM***, ***FDP_UIT.1/TRM*** and ***FTP_ITC.1/PACE*** using ***FCS_COP.1/PACE_ENC***. A prerequisite for establishing this trusted channel is a successful PACE Authentication (***FIA_UID.1/PACE***, ***FIA_UAU.1/PACE***) using ***FCS_CKM.1/DH_PACE*** and possessing the special properties ***FIA_UAU.5/PACE***, ***FIA_UAU.6/PACE***. ***FDP_RIP.1*** requires erasing the values of session keys (here: for KENC). Since PACE can use the PIN as the shared secret, using and management of PIN (**FIA_AFL.1/PIN/PUK**, **FMT_MTD.1/Resume_PIN**, **FMT_MTD.1/Change_PIN**, **FMT_MTD.1/Unblock_PIN**, **FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PIN)** also support achievement of this objective
The ***SFR FMT_MTD.1/KEY_READ*** restricts the access to the PACE passwords.***FMT_MTD.1/PA*** requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy .The SFR FCS_RND.1 represents the general support for cryptographic operations needed. The SFRs ***FMT_SMF.1*** and ***FMT_SMR.1/PACE*** support the functions and roles related.

The CA confidentiality is ensured by the Chip Authentication Protocol proving the identity of the TOE. The Chip Authentication Protocol defined by ***FCS_CKM.1/CA*** is performed using a TOE internally stored confidential private key as required by ***FMT_MTD.1/KEY_READ***. The Chip Authentication Protocol [TR_03110] requires additional TSF according to ***FCS_COP.1/CA_SHA*** (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).

#### 7.3.1.5 OT.Tracing

The security objective **OT.Tracing** *"Tracing travel document"* aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without a priori knowledge of the correct values of shared PACE passwords. This objective is achieved as follows:(i) while establishing PACE communication with a PACE password (non-blocking authorisation data) – by ***FIA_AFL.1/PACE***;(ii) - while establishing PACE communication using the PIN (blocking authentication data) by **FIA_AFL.1.2/PIN/PUK** for listening to PACE communication (is of importance for the current PP, since SOD is card-individual) – ***FTP_ITC.1/PACE***.

#### 7.3.1.6 OT.Prot_Abuse_Func

The security objective **OT.Prot_Abuse-Func** *"Protection against Abuse of Functionality"* aims preventing TOE's functions being not intended to be used in the operational phase from manipulating and disclosing the User- and TSF-data.This objective is achieved by ***FMT_LIM.1*** and ***FMT_LIM.2*** preventing misuse of test and other functionality of the TOE having not to be used in the TOE's operational life cycle phase.

#### 7.3.1.7 OT.Prot_Inf_Leak

The security objective **OT.Prot_Inf_Leak** *"Protection against Information Leakage"* aims protection against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE. This objective is achieved:
• by ***FPT_EMS.1*** for measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
• by ***FPT_FLS.1*** and ***FPT_TST.1*** for forcing a malfunction of the TOE, and
• by ***FPT_PHP.3*** for a physical manipulation of the TOE.

#### 7.3.1.8 OT.Prot_Phys-Tamper

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

#### 7.3.1.9 OT.Prot_Malfunction

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

#### 7.3.1.10 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.

#### 7.3.1.11 OT.AC_Pers

The security objective **OT.AC_Pers** *"Access Control for Personalisation of logical MRTD"* aims that only Personalisation Agent can write the User- and the TSF-data into the TOE. The justification for the SFRs ***FAU_SAS.1***, ***FMT_MTD.1/INI_ENA*** and ***FMT_MTD.1/INI_DIS*** arises from the justification for OT.Identification above with respect to the Pre-personalisation Data. ***FMT_MTD.1/PA*** covers the related property of OT.AC_Pers

(writing SOD and, in generally, personalisation data). The SFRs ***FMT_SMF.1*** and ***FMT_SMR.1/PACE*** support the functions and roles related. The SFR ***FMT_MTD.1./KEY_READ*** restricts the access to the Personalisation Agent Keys.
Since only a terminal can reach the necessary authorization level, using and managing the PIN (the related SFRs are ***FIA_AFL.1/PIN/PUK***, ***FMT_MTD.1/Resume_PIN***, ***FMT_MTD.1/Change_PIN***, ***FMT_MTD.1/Unblock_PIN***, and ***FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PIN***) also support the achievement of this objective. ***FDP_RIP.1*** requires erasing the temporal values PIN and PUK.

The Manufacturer Secret Key (MSK) loaded by IC Manufacturer is diversified at first command according to SFR ***FCS_CKM.1/MSK_DIV*** and ***FCS_CKM.1/MSK_SHA***. This secures the transport of the chip between IC manufacturing centre and MRTD manufacturing centre.

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), and ***FCS_COP.1/CA_SHA***, ***FCS_COP.1/CA_ENC*** and ***FCS_COP.1/CA_MAC*** (for the ENC_MAC_Mode secure messaging). 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***.

Only the Personalization Agent is allowed to generate Chip Authentication Key pair and Active Authentication Key pair according to respectively ***FMT_MTD.1/CA_KEY_GEN*** and ***FMT_MTD.1/AA_KEY_GEN.*** The generation of these key pairs is ensured by ***FCS_CKM.1/KEY_GEN***.

#### 7.3.1.12 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, CPLC Data and the Life Cycle State of the TOE.

The Manufacturer Secret Key (MSK) loaded by IC manufacturer is diversified at first command according to SFR ***FCS_CKM.1/MSK_DIV*** and ***FCS_CKM.1/MSK_SHA***. This secures the transport of the chip between IC manufacturing centre and MRTD manufacturing centre.

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

Once step 4 is done, the MRTD packaging responsible is allowed to set the Pre-personalization Agent keys according to the SFR ***FMT_MTD.1/MP_KEY_WRITE***, ***FDP_ITC.1/MP*** and ***FCS_COP.1/GP_SDT_DEC***. The SFR ***FMT_MTD.1/MP_KEY_READ*** prevents read access to the Pre-personalization keys and ensure together with the SFR ***FPT_EMS.1*** the confidentially of these keys. This operation destroys the MSK (***FCS_CKM.4***).

The write access to these data is defined by the SFR ***FDP_ACC.1/MP*** and ***FDP_ACF.1/MP*** as follows: only the successfully authenticated Pre-personalization Agent and Personalization Agent are allowed to write these data.

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

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

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

The Manufacturer can enable Chip Authentication and Active Authentication functionalities following ***FMT_MOF.1.1/PROT***.

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

The SFR ***FMT_SMR.1/PACE*** lists the roles and the SFR ***FMT_SMF.1*** lists the TSF management functions setting the Pre-personalization Agent Keys according to the SFR ***FMT_MTD.1/MP_KEY_WRITE*** as authentication reference data. The SFR ***FMT_MTD.1/MP_KEY_READ*** prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR ***FCS_CKM.4***, ***FPT_EMS.1, FPT_FLS.1*** and FPT_PHP.3 the confidentially of these keys.

SFR ***FDP_ACF.1/ID*** and ***FDP_ACC.1/ID*** define rules to access TOE_ID and CPLC which allow the TOE identification.

The Manufacturer is the only subject allowed to ends Pre-personalization of logical MRTD, setting the TOE Life Cycle State in Personalization state according to ***FMT_MTD.1.1/LCS_PREP***. Since then it is no more possible to return in manufacturing state and the role Manufacturer is no longer available as ***FCS_CKM.4*** destroys Manufacturer keys.

#### 7.3.1.13 OT.Chip_Auth_Proof

The security objective **OT.Chip_Auth_Proof** *"Proof of MRTD's chip authenticity"* is ensured by the Chip Authentication Protocol v.1 provided by ***FIA_API.1/CA*** or the Active Authentication protocol provided by ***FIA_API.1/AA*** or the PACE protocol with Chip Authentication Mapping method provided by ***FIA_API.1/PACE_CAM*** 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 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 Protocol v.1 [ICAO_9303] 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.

The Manufacturer and the Personalization Agent can select the protection mode of user data following **FMT_MOF.1/GP**

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

The PACE protocol with Chip Authentication Mapping, defined by ***FIA_API.1/PACE_CAM***, is executed using a TOE internally stored confidential private key as required by ***FMT_MTD.1/CAPK*** and ***FMT_MTD.1/KEY_READ***. ***FCS_CKM.1/DH_PACE*** is used for the session key generation, ***FCS_COP.1/CA_DATA_GEN*** for the Chip Authentication Data generation and ***FCS_COP.1.1/PACE_ENC*** for the Chip Authentication Data encryption as per [ICAO_9303], following ***FIA_UID.1/PACE_CAM***, ***FIA_UAU.1/PACE_CAM***, ***FIA_UAU.4/PACE***, ***FIA_UAU.5/PACE_CAM***, ***FIA_UAU.6/PACE***. The SFRs ***FMT_SMF.1*** and ***FMT_SMR.1/PACE*** support the functions and roles related.

#### 7.3.1.14 OT.Update_Mechanism

The update mechanism is dedicated to part or all OS update and is enforced by the SFRs **FCS_COP.1/UPD_ITC, FCS_CKM.1/UPD_ITC, FCS_COP.1/UPD_DEC, FCS_CKM.1/UPD_DEC, FCS_COP.1/UPD_INT, FCS_CKM.1/UPD_INT, FCS_COP.1/UPD_SIG, FCS_CKM.4/UPD** which are concerned with cryptographic operations and key generation. A secure messaging is used for Update Package transport (SCP03 by default). The SFRs are used to decipher the new Update Package and to check the associated signature.
**FIA_AFL.1/UPD, FIA_UID.1/UPD, FIA_UAU.1/UPD** are concerned with identification and authentication towards the TOE, they requires the protection of the received data by means of secure messaging implemented.
The access control policy is supported by **FDP_ACC.1/UPD, FDP_ACF.1/UPD, FDP_IFC.1/UPD, FDP_IFF.1/UPD** and **FDP_RIP.1/UPD**.
**FAU_SAS.1/UPD** addresses the storage of update Data in its non-volatile memory, whereby they also include the Update Package Identification Data uniquely identifying the TOE's Update Package.
**FMT_SMF.1/UPD** are concerned with management functions and data**.**
The Manufacturer is the only one who can load and activate the MSK according to SFRs, the LSK managed by the installation Update Package agent can't be read as required by **FMT_MTD.1/UPD_SK_PICC and FMT_MTD.1/UPD_KEY_READ. FMT_SMR.1/UPD**'.
Unauthorised modifying of the exchanged data is addressed, in the first line, by **FTP_ITC.1/UPD.**
The Update Package installation agent is able to detect any modification of the transmitted code data by means of the Symmetric Authentication mechanism. The SFR ***FCS_COP.1/UPD_ITC*** requires the protection of the received data by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1.1/UPD_DEC***, ***FCS_CKM.1.1/UPD_INT***, and ***FCS_COP.1/UPD_DEC*** for the ENC_MAC_Mode. The LSK used as a seed for DIV_LSK and DIV2_LSK and DIV2_LSK cannot be read by anyone in accordance to ***FMT_MTD.1/UPD_KEY_READ***. ***FCS_CKM.4*** enforces the destruction of Secure Messaging session keys. ***FCS_CKM.4*** also enforces the destruction of the LSK once the TOE is in Step 6.

#### 7.3.1.15 OT.Enc_Sign_Update

The SFRs **FCS_COP.1/UPD_ITC, FCS_CKM.1/UPD_ITC, FCS_COP.1/UPD_DEC, FCS_CKM.1/UPD_DEC, FCS_COP.1/UPD_INT, FCS_CKM.1/UPD_INT, FCS_COP.1/UPD_SIG, FCS_CKM.4/UPD** are concerned with cryptographic operations and key generation for checking installs update packages that are encrypted, integrity-protected and signed by the authority in charge of delivering and installing updates.
The Update Package installation in non-volatile memory is enforced by **FMT_MTD.1/UPD_SK_PICC and FMT_MTD.1/UPD_KEY_READ, FMT_SMR.1/UPD**

#### 7.3.1.16 OT.Update_Terminal_Auth

**FIA_AFL.1/UPD, FIA_UID.1/UPD, FIA_UAU.1/UPD** are concerned with identification and authentication towards the TOE according GP authentication.
The access control policy is supported by **FDP_ACC.1/UPD, FDP_ACF.1/UPD, FDP_IFC.1/UPD, FDP_IFF.1/UPD.**

FMT_MTD.1/UPD_SK_PICC, FMT_MTD.1/UPD_KEY_READ, FTP_ITC.1/UPD and FMT_SMR.1/UPD are concerned with management functions and data. FMT_SMF.1/UPD supports OT.Update_Terminal_Auth,

#### 7.3.1.17 OT.Attack_Detection

**FAU_SAS.1/UPD** addresses the storage of Initialisation update and Pre-Personalisation Data in its non-volatile memory, whereby they also include the Update Package Identification Data uniquely identifying the TOE's Update Package. A bad log can confirm an attack detection.
The security objective requires the TOE to protect confidential TSF data stored and/or processed in the travel document's chip against disclosure by forcing a malfunction of the TOE which is addressed by the SFR **FPT_FLS.1/UPD** and **FPT_TST.1/UPD**.

#### 7.3.1.18 OT.Key_Secrecy

**FMT_MTD.1/UPD_SK_PICC, FMT_SMR.1/UPD** and **FMT_MTD.1/UPD_KEY_READ** addresses the access control of the writing the logical travel document and respect key secrecy.
The security objective requires the TOE to protect confidential TSF data stored and/or processed in the travel document's chip against disclosure - by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR **FPT_EMS.1/UPD**.

### 7.3.2 Dependency Rationale

#### 7.3.2.1 Overview

The Table 21 shows the dependencies between the SFR of the TOE.

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FAU_SAS.1 | No dependencies | n.a. |
| FAU_SAS.1/UPD | No dependencies | n.a. |
| FCS_CKM.1/DH_PACE | [FCS_CKM.2 or FCS_COP.1],<br><br>FCS_CKM.4 | FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC<br><br>FCS_CKM.4 |
| FCS_CKM.1/MSK_DIV | | FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC<br><br>FCS_CKM.4 |
| FCS_CKM.1/GP | | FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC<br><br>FCS_CKM.4 |
| FCS_CKM.1/CA | | FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC<br><br>FCS_CKM.4 |
| FCS_CKM.1/KEY_GEN | | FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC and FCS_COP.1/SIG_GEN<br><br>FCS_CKM.4 |
| FCS_CKM.1/UPD_DEC | | FCS_COP.1/UPD_DEC FCS_CKM.4/UPD |
| FCS_CKM.1/UPD_INT | | FCS_COP.1/UPD_INT FCS_COP.1/UPD_SIG FCS_CKM.4/UPD |
| FCS_CKM.1/UPD_ITC | | FCS_COP.1/UPD_ITC FCS_CKM.4/UPD |
| FCS_CKM.4 | FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] | FCS_CKM.1/PACE_DH and FCS_CKM.1/ MSK_DIV and FCS_CKM.1/GP and FCS_CKM.1/CA |
| FCS_CKM.4/UPD | | FCS_CKM.1/UPD_DEC FCS_CKM.1/UPD_INT FCS_CKM.1/UPD_ITC |
| FCS_COP.1/PACE_ENC | [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1],<br><br>FCS_CKM.4 | FCS_CKM.1/DH_PACE<br><br>FCS_CKM.4 |
| FCS_COP./PACE_MAC | | FCS_CKM.1/DH_PACE<br><br>FCS_CKM.4 |
| FCS_COP.1/MSK_SHA | | FCS_CKM.1/MSK_DIV<br><br>FCS_CKM.4 |
| FCS_COP.1/GP_ENC | | FCS_CKM.1/MSK_DIV and FCS_CKM.1/GP<br><br>FCS_CKM.4 |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FCS_COP.1/GP_AUTH | | FCS_CKM.1/MSK_DIV and FCS_CKM.1/GP<br><br>FCS_CKM.4 |
| FCS_COP.1/GP_MAC | | FCS_CKM.1/MSK_DIV and FCS_CKM.1/GP<br><br>FCS_CKM.4 |
| FCS_COP.1/GP_SDT_DEC | | FCS_CKM.1/MSK_DIV and FCS_CKM.1/GP<br><br>FCS_CKM.4 |
| FCS_COP.1/CA_SHA | | FCS_CKM.1/CA<br><br>FCS_CKM.4 |
| FCS_COP.1/CA_ENC | | FCS_CKM.1/CA<br><br>FCS_CKM.4 |
| FCS_COP.1/CA_MAC | | FCS_CKM.1/CA<br><br>FCS_CKM.4 |
| FCS_COP.1/SIG_GEN | | FDP_ITC.1/MP<br><br>FCS_CKM.4 |
| FCS_COP.1/CA_DATA_GEN | | FCS_CKM.1/CA<br><br>FCS_CKM.4 |
| FCS_COP.1/UPD_ITC | | FCS_CKM.1/UPD_ITC<br>FCS_CKM.4/UPD |
| FCS_COP.1/UPD_DEC | | FCS_CKM.1/UPD_DEC<br>FCS_CKM.4/UPD |
| FCS_COP.1/UPD_SIG | | FCS_CKM.1/UPD_INT<br>FCS_CKM.4/UPD |
| FCS_COP.1/UPD_INT | | FCS_CKM.1/UPD_INT<br>FCS_CKM.4/UPD |
| FCS_RND.1 | No dependencies | n.a. |
| FIA_UID.1/PACE | No dependencies | n.a. |
| FIA_UID.1/PACE_CAM | No dependencies | n.a. |
| FIA_UID.1/UPD | No dependencies | n.a. |
| FIA_UAU.1/PACE | FIA_UID.1 | FIA_UID.1/PACE |
| FIA_UAU.1/PACE_CAM | FIA_UID.1 | FIA_UID.1/PACE_CAM |
| FIA_UAU.1/UPD | FIA_UID.1 | FIA_UID.1/UPD |
| FIA_UAU.4/PACE | No dependencies | n.a. |
| FIA_UAU.5/PACE | No dependencies | n.a. |
| FIA_UAU.5/PACE_CAM | No dependencies | n.a. |
| FIA_UAU.6/PACE | No dependencies | n.a. |
| FIA_UAU.6/MP | | |
| FIA_UAU.6/CA | | |
| FIA_AFL.1/PACE | FIA_UAU.1 | FIA_UAU.1 |
| FIA_AFL.1/MP | | |
| FIA_AFL.1/UPD | | FIA_UAU.1/UPD |
| FIA_API.1/CA | No dependencies | n.a. |
| FIA_API.1/AA | No dependencies | n.a. |
| FIA_API.1/PACE_CAM | No dependencies | n.a. |
| FDP_ACC.1/TRM | FDP_ACF.1 | FDP_ACF.1/TRM |
| FDP_ACC.1/MP | | FDP_ACF.1/MP |
| FDP_ACC.1/ID | | FDP_ACF.1/ID |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FDP_ACC.1/UPD | FDP_ACF.1 | FDP_ACF.1/UPD |
| FDP_ACF.1/TRM | FDP_ACC.1,<br><br>FMT_MSA.3 | FDP_ACC.1/TRM<br><br>See justification in §7.3.2.2.1 |
| FDP_ACF.1/MP | | FDP_ACC.1/MP<br><br>See justification in §7.3.2.2.2 |
| FDP_ACF.1/ID | | FDP_ACC.1/ID<br><br>See justification in §7.3.2.2.2 |
| FDP_ACF.1/UPD | FDP_ACC.1,<br>FMT_MSA.3 | FDP_ACC.1/UPD<br><br>See justification in §7.3.2.2.1 |
| FDP_IFC.1/UPD | FDP_ACC.1,<br>FDP_IFF.1 | FDP_ACC.1/UPD, FDP_IFF.1/UPD |
| FDP_IFF.1/UPD | FDP_IFC.1 | FDP_IFC.1/UPD |
| FDP_RIP.1 | No dependencies | n.a. |
| FDP_RIP.1/UPD | | |
| FDP_UCT.1/TRM | [FTP_ITC.1, or<br>FTP_TRP.1],<br><br>[FDP_IFC.1, or<br>FDP_ACC.1] | FTP_ITC.1<br><br>FDP_ACC.1/TRM |
| FDP_UCT.1/MP | | FTP_ITC.1<br><br>FDP_ACC.1/MP |
| FDP_UCT.1/CA | | FTP_ITC.1<br><br>FDP_ACC.1/CA |
| FDP_UIT.1/TRM | [FTP_ITC.1, or<br>FTP_TRP.1],<br><br>[FDP_IFC.1, or<br>FDP_ACC.1] | FTP_ITC.1<br><br>FDP_ACC.1/TRM |
| FDP_UIT.1/MP | | FTP_ITC.1<br><br>FDP_ACC.1/MP |
| FDP_UIT.1/CA | | FTP_ITC.1<br><br>FDP_ACC.1/CA |
| FDP_ITC.1/MP | [FDP_ACC.1, or<br>FDP_IFC.1]<br><br>FMT_MSA.3 | FDP_ACC.1/MP<br><br>See justification in §7.3.2.2.3 |
| FMT_MOF.1/PROT | FMT_SMF.1<br><br>FMT_SMR.1 | FMT_SMF.1<br><br>FMT_SMR.1/PACE |
| FMT_MOF.1/GP | | |
| FMT_SMF.1 | No dependencies | n.a. |
| FMT_SMF.1/UPD | No dependencies | n.a. |
| FMT_SMR.1/PACE | FIA_UID.1 | FIA_UID.1/PACE |
| FMT_SMR.1/UPD | FIA_UID.1 | FIA_UID.1/UPD |
| FMT_LIM.1 | FMT_LIM.2 | FMT_LIM.2 |
| FMT_LIM.2 | FMT_LIM.1 | FMT_LIM.1 |
| FMT_MTD.1/INI_ENA | FMT_SMF.1,<br><br>FMT_SMR.1 | FMT_SMF.1,<br><br>FMT_SMR.1/PACE |
| FMT_MTD.1/INI_DIS | | |
| FMT_MTD.1/KEY_READ | | |
| FMT_MTD.1/PA | | |
| FMT_MTD.1/PACE_PWD | | |
| FMT_MTD.1/CAPK | | |
| FMT_MTD.1/MP_KEY_WRITE | | |

| SFR | Dependencies | Support of the Dependencies |
|---|---|---|
| FMT_MTD.1/AA_KEY_WRITE | | |
| FMT_MTD.1/LCS_PREP | | |
| FMT_MTD.1/LCS_PERS | | |
| FMT_MTD.1/AA_KEY_GEN | | |
| FMT_MTD.1/CA_KEY_GEN | | |
| FMT_MTD.1/UPD_SK_PICC | | |
| FMT_MTD.1/UPD_KEY_READ | | |
| FPT_EMS.1 | No dependencies | n.a. |
| FPT_EMS.1/UPD | No dependencies | n.a. |
| FPT_FLS.1 | No dependencies | n.a. |
| FPT_FLS.1/UPD | No dependencies | n.a. |
| FPT_TST.1 | No dependencies | n.a. |
| FPT_TST.1/UPD | No dependencies | n.a. |
| FPT_PHP.3 | No dependencies | n.a. |
| FTP_ITC.1/PACE | No dependencies | n.a. |
| FTP_ITC.1/MP | | |
| FTP_ITC.1/UPD | No dependencies | n.a. |

Table 21 - Dependencies between the SFR for the TOE

#### 7.3.2.2 Rationale for the exclusion of dependencies

##### 7.3.2.2.1 FDP_ACF.1/TRM and FDP_ACF.1/UPD

The access control TSF according to **FDP_ACF.1/TRM** and **FDP_ACF.1/UPD** 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.

##### 7.3.2.2.2 FDP_ACF.1/MP and FDP_ACF.1/ID

The access control TSF according to **FDP_ACF.1/MP** and **FDP_ACF.1/ID** uses security attributes which are fixed during the development of the OS 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.

##### 7.3.2.2.3 FDP_ITC.1/MP

The SFR **FDP_ITC.1/MP** requires the verification of security attributes when Manufacturer and Personalization Agent imports user data. There is no need for FMT_MSA.3, e.g. to initialize these security attributes, as they are fixed during the development of the OS.

# 8 TOE summary specification

## 8.1 TOE summary specification

### 8.1.1 Overview

The TOE provides the following Security Functions (TSF):

| TSF | Acronym | Descr. | Step | | |
|---|---|---|---|---|---|
| | | | 5 | 6 | 7 |
| Access Control in Reading | F.ACR | § 8.1.2 | ✓ | ✓ | ✓ |
| Access Control in Writing | F.ACW | § 8.1.3 | ✓ | ✓ | ✓ |
| Active Authentication | F.AA | § 8.1.4 | ✓ | × | ✓ |
| Chip Authentication | F.CA | § 8.1.5 | ✓ | × | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| PACE | F.PACE | § 8.1.6 | ✗ | ✗ | ✓ |
| MRTD Personalization | F.PERS | § 8.1.7 | ✗ | ✓ | ✗ |
| Physical Protection | F.PHY | § 8.1.8 | ✓ | ✓ | ✓ |
| MRTD Pre-personalization | F.PREP | § 8.1.9 | ✓ | ✗ | ✗ |
| Safe State Management | F.SS | § 8.1.10 | ✓ | ✓ | ✓ |
| Secure Messaging | F.SM | § 8.1.11 | ✓ | ✓ | ✓ |
| Self Tests | F.STST | § 8.1.12 | ✓ | ✓ | ✓ |
| Update Mechanism[4] | F.UPD | § 8.1.13 | ✓ | ✓ | ✓ |

Table 22 - TSF of the TOE

### 8.1.2 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:

- MSK,
- Pre-personalization Agent keys,
- Personalization Agent keys,
- AA private key,
- CA private key,
- LSK.

It controls access to the CPLC data as follow:

- It ensures the CPLC data can be read during the personalization phase,
- It ensures it cannot be readable without authentication at the end of the personalization step.

It controls access to the TOE_ID as follow:

- It ensures the TOE_ID data can be read during the manufacturing and personalization phases,
- It ensures it cannot be readable without authentication in operational use phase.

Regarding the file structure:

*In the Operational Use phase:*

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

*In the Manufacturing and Personalization phases:*

- The Manufacturer and the Personalization Agent can read all the data stored in the TOE after it is authenticated by the TOE (using its authentication keys).

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

### 8.1.3 Access Control in Writing

This function controls access to write functions (in Flash memory) 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.

It also ensures the CPLC data cannot be written anymore once the TOE is in Operational Use phase.

[4] The Update mechanism is also available on step before 5, to the manufacturer.

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 CVCA which can be updated if the “Secure Messaging” access condition is verified.

*In the Manufacturing and Personalization phases:*

The Manufacturing and Personalization Agent can create and write through a valid secure channel all the data files it needs after it is authenticated by the TOE (using its authentication keys).

### 8.1.4 Active Authentication

This TSF provides the Active Authentication as described in [ICAO_9303]. It also provides management of this function in phase 5.

### 8.1.5 Chip Authentication

This TSF provides the Chip Authentication, authentication and session keys generation to be used by F.SM, as described in [ICAO_9303].

### 8.1.6 PACE

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

### 8.1.7 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 authentication mechanism. This function allows to:

- Manage symmetric authentication using Personalization Agent keys,
- Compute session keys to be used by F.SM,
- Load user data,
- Load Chip Authentication keys and Active Authentication keys,
- Set Personalization Agent CPLC Data,
- Set TOE life cycle in Operational Use phase.

### 8.1.8 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, CPLC data, configuration data and TOE life cycle. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE.

### 8.1.9 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 symmetric authentication mechanism. This function allows to:

- Diversify the MSK,
- Manage symmetric authentication using Pre-personalization Agent keys,
- Compute session keys to be used by F.SM,

- Load data,
- Create the MRTD application
- Load Personalization Agent keys,
- Load the Pre-personalization Agent CPLC Data,
- Set TOE life cycle in Personalization phase.

This security function ensures the destruction of the MSK, once ISK is loaded. This security function ensures the destruction of the ISK, once Personalization Agent keys are loaded.

### 8.1.10 Safe State Management

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

- an integrity error is detected by F.STST described in § 8.1.12,
- a tearing occurs (during a copy of data in Flash memory).

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

### 8.1.11 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. BAC or CA), a secure channel is established. This security functionality also provides a Secure Messaging (SCP03 – SCP02) for the Pre-personalization and Personalization phases. The protocols can be configured to protect the exchanges integrity and/or confidentiality. If an error occurs in the secure messaging layer, the session keys are destroyed.

### 8.1.12 Self Tests

The TOE performs self-tests to verify the integrity of the TSF data:

- At Reset,
- Before using the TSF data,
- Before using Chip Authentication key and Active Authentication key.

### 8.1.13 Update Mechanism

This function is in charge of loading Updated Package.
The update of the Initial TOE checks an evidence of authenticity and integrity of the loaded additional Code.
The mechanism enforces that only the allowed version of the Update Package can be loaded on the Initial TOE.
The mechanism forbids the loading of an additional Code not intended to be assembled with the Initial TOE.
Activation of the Update Package and update of the Identification Data shall be performed at the same time in an Atomic way.
During the Load Phase of Update Package, the TOE shall remain secure. The secure messaging protects in confidentiality and integrity the exchange with the Update terminal.
A GP secure authentication is used and the TOE is in charge to decipher the Update Package, to check the associated signature and to install the new functionalities. The Update Package contains its identification elements that are used, during audit, to uniquely identify loaded code.

F.STST, F.SM, F.PERS, F.ACR, F.ACW, F.PHY and F_SM protect and support Update Mechanism.

## 8.2 SFR and TSF

| SFR \ TSF | F.ACR | F.ACW | F.AA | F.CA | F.PACE | F.PERS | F.PHY | F.PREP | F.SS | F.SM | F.STST | F.UPD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FAU_SAS.1 | × | × | × | × | × | × | ✓ | × | ✓ | × | × | × |
| FCS_CKM.1/DH_PACE | × | × | × | × | ✓ | × | × | × | × | × | ✓ | × |
| FCS_CKM.1/MSK_DIV | × | × | × | × | × | × | × | ✓ | × | × | ✓ | × |
| FCS_CKM.1/GP | × | × | × | × | × | ✓ | × | ✓ | × | × | ✓ | × |
| FCS_CKM.1/CA | × | × | × | ✓ | × | × | × | × | × | × | ✓ | × |
| FCS_CKM.1/KEY_GEN | × | × | × | × | × | ✓ | × | ✓ | × | × | ✓ | × |
| FCS_CKM.4 | × | × | × | × | × | ✓ | × | ✓ | × | ✓ | × | × |
| FCS_COP.1/PACE_ENC | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FCS_COP.1/PACE_MAC | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FCS_COP.1/MSK_SHA | × | × | × | × | × | × | × | ✓ | × | × | × | × |
| FCS_COP.1/GP_ENC | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FCS_COP.1/GP_AUTH | × | × | × | × | × | ✓ | × | ✓ | × | × | ✓ | ✓ |
| FCS_COP.1/GP_MAC | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FCS_COP.1/GP_SDT_DEC | × | × | × | × | × | ✓ | × | × | × | × | ✓ | × |
| FCS_COP.1/CA_SHA | × | × | × | ✓ | × | × | × | × | × | × | × | × |
| FCS_COP.1/CA_ENC | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FCS_COP.1/CA_MAC | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FCS_COP.1/SIG_GEN | × | × | ✓ | × | × | × | × | × | × | × | ✓ | × |
| FCS_COP.1/CA_DATA_GEN | × | × | × | × | ✓ | × | × | × | × | × | × | × |
| FCS_RND.1 | × | × | ✓ | × | ✓ | ✓ | × | ✓ | × | × | × | × |
| FIA_UID.1/PACE | ✓ | ✓ | × | × | × | × | × | × | × | × | × | × |
| FIA_UID.1/PACE_CAM | ✓ | ✓ | × | × | × | × | × | × | × | × | × | × |
| FIA_UAU.1/PACE | ✓ | ✓ | × | × | × | × | × | × | × | × | × | × |
| FIA_UAU.1/PACE_CAM | ✓ | ✓ | × | × | × | × | × | × | × | × | × | × |
| FIA_UAU.4/PACE | × | × | × | × | ✓ | ✓ | × | ✓ | × | × | ✓ | × |
| FIA_UAU.5/PACE | × | × | × | ✓ | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | × |
| FIA_UAU.5/PACE_CAM | × | × | × | ✓ | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | × |
| FIA_UAU.6/PACE | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FIA_UAU.6/MP | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FIA_UAU.6/CA | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FIA_AFL.1/PACE | × | × | × | × | ✓ | × | × | × | × | × | ✓ | × |
| FIA_AFL.1/MP | × | × | × | × | × | ✓ | × | ✓ | × | × | ✓ | × |
| FIA_API.1/CA | × | × | × | ✓ | × | × | × | × | × | × | × | × |
| FIA_API.1/AA | × | × | ✓ | × | × | × | × | × | × | × | × | × |
| FIA_API.1/PACE_CAM | × | × | × | × | ✓ | × | × | × | × | × | × | × |
| FDP_ACC.1/TRM | ✓ | ✓ | × | × | ✓ | × | × | × | × | × | × | × |
| FDP_ACC.1/MP | ✓ | ✓ | × | × | × | ✓ | × | ✓ | × | × | × | × |
| FDP_ACC.1/ID | ✓ | ✓ | × | × | ✓ | ✓ | × | ✓ | × | × | × | × |
| FDP_ACF.1/TRM | ✓ | ✓ | × | × | ✓ | × | × | × | × | × | × | × |
| FDP_ACF.1/MP | ✓ | ✓ | × | × | × | ✓ | × | ✓ | × | × | × | × |
| FDP_ACF.1/ID | ✓ | ✓ | × | × | ✓ | ✓ | × | ✓ | × | × | × | × |
| FDP_RIP.1 | × | × | × | × | ✓ | × | × | × | × | ✓ | × | × |
| FDP_UCT.1/TRM | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FDP_UCT.1/MP | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FDP_UCT.1/CA | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FDP_UIT.1/TRM | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FDP_UIT.1/MP | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |
| FDP_UIT.1/CA | × | × | × | × | × | × | × | × | × | ✓ | ✓ | × |

| SFR \ TSF | F.ACR | F.ACW | F.AA | F.CA | F.PACE | F.PERS | F.PHY | F.PREP | F.SS | F.SM | F.STST | F.UPD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FDP_ITC.1/MP | × | × | × | × | × | ✓ | × | ✓ | × | × | ✓ | × |
| FMT_MOF.1/PROT | × | × | ✓ | × | × | × | × | × | × | × | × | × |
| FMT_MOF.1/GP | × | × | × | × | × | ✓ | × | ✓ | × | × | × | × |
| FMT_SMF.1 | × | × | ✓ | ✓ | × | ✓ | × | ✓ | × | ✓ | × | × |
| FMT_SMR.1/PACE | × | × | × | × | ✓ | ✓ | × | ✓ | × | ✓ | × | × |
| FMT_LIM.1 | × | × | × | × | × | × | ✓ | × | ✓ | × | × | × |
| FMT_LIM.2 | × | × | × | × | × | × | ✓ | × | ✓ | × | × | × |
| FMT_MTD.1/INI_ENA | ✓ | ✓ | × | × | × | × | × | ✓ | × | × | × | × |
| FMT_MTD.1/INI_DIS | ✓ | × | × | × | × | ✓ | × | × | × | × | × | × |
| FMT_MTD.1/KEY_READ | ✓ | × | × | × | × | × | × | × | × | × | × | × |
| FMT_MTD.1/PA | ✓ | ✓ | × | × | × | ✓ | × | × | × | × | × | × |
| FMT_MTD.1/PACE_PWD | ✓ | ✓ | × | × | × | ✓ | × | × | × | × | × | × |
| FMT_MTD.1/CAPK | ✓ | ✓ | × | × | × | ✓ | × | × | × | × | × | × |
| FMT_MTD.1/MP_KEY_WRITE | ✓ | ✓ | × | × | × | × | × | ✓ | × | × | × | × |
| FMT_MTD.1/AA_KEY_WRITE | ✓ | ✓ | × | × | × | ✓ | × | × | × | × | × | × |
| FMT_MTD.1/LCS_PREP | ✓ | ✓ | × | × | × | × | × | ✓ | × | × | × | × |
| FMT_MTD.1/LCS_PERS | ✓ | ✓ | × | × | × | ✓ | × | × | × | × | × | × |
| FMT_MTD.1/AA_KEY_GEN | × | × | × | × | × | ✓ | × | ✓ | × | × | × | × |
| FMT_MTD.1/CA_KEY_GEN | × | × | × | × | × | ✓ | × | ✓ | × | × | × | × |
| FPT_EMS.1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | × | × |
| FPT_FLS.1 | × | × | × | × | × | × | ✓ | × | ✓ | × | × | × |
| FPT_TST.1 | × | × | × | × | × | × | × | × | × | × | ✓ | × |
| FPT_PHP.3 | × | × | × | × | × | × | ✓ | × | ✓ | × | × | × |
| FTP_ITC.1/PACE | × | × | × | × | ✓ | × | × | × | × | ✓ | × | × |
| FTP_ITC.1/MP | × | × | × | × | × | ✓ | × | ✓ | × | × | ✓ | × |
| FAU_SAS.1/UPD | × | × | × | × | × | × | ✓ | × | ✓ | × | × | × |
| FCS_CKM.1/UPD_ITC | × | × | × | × | × | ✓ | × | ✓ | × | ✓ | ✓ | × |
| FCS_CKM.1/UPD_DEC | × | × | × | × | × | ✓ | × | ✓ | × | ✓ | ✓ | × |
| FCS_CKM.1/UPD_INT | × | × | × | × | × | ✓ | × | ✓ | × | ✓ | ✓ | × |
| FCS_CKM.4/UPD | × | × | × | × | × | ✓ | × | ✓ | × | ✓ | × | ✓ |
| FCS_COP.1/UPD_ITC | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FCS_COP.1/UPD_DEC | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FCS_COP.1/UPD_SIG | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FCS_COP.1/UPD_INT | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FIA_AFL.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FIA_UID.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FIA_UAU.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FDP_ACC.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FDP_ACF.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FDP_IFC.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FDP_IFF.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FDP_RIP.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FMT_SMF.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FMT_MTD.1/UPD_SK_PICC | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FMT_MTD.1/UPD_KEY_READ | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FMT_SMR.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FPT_EMS.1 /UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FPT_FLS.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FPT_TST.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |
| FTP_ITC.1/UPD | × | × | × | × | × | × | × | × | × | × | × | ✓ |

Table 23- SFR and TSF

# 9 GLOSSARY AND ACRONYMS

## 9.1 Glossary

| Term | Definition |
|---|---|
| Active Authentication | Security mechanism defined in [ICAO_9303] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization. |
| *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. |
| *Application note* | Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE. |
| *Audit records* | Write-only-once non-volatile memory area of the travel document's chip to store the Initialisation Data and Pre-personalisation Data. |
| *Authenticity* | Ability to confirm that the travel document itself and the data elements stored in were issued by the travel document Issuer |
| *Basic Access Control (BAC)* | Security mechanism defined in [ICAO_9303] by which means the travel document's chip proves and the basic inspection system (with BAC) protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on travel document's chip according to LDS. |
| *Basic Inspection System with Basic Access Control protocol (BIS-BAC)* | A technical system being used by an official organisation103 and operated by a governmental organisation and verifying correspondence between the stored and printed MRZ.<br>BIS-BAC implements the terminal's part of the Basic Access Control protocol and authenticates itself to the travel document using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (travel document document details data and biographical data) stored on the travel document.<br>See also par. 1.2.5; also [ICAO_9303]. |
| *Basic Inspection System with PACE protocol (BIS-PACE)* | A technical system being used by an inspecting authority104 and verifying the travel document presenter as the travel document holder (for *ePassport*: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder).<br>BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. A technical system being used by an inspecting authority and verifying the<br>ePass presenter as the ePass holder (for ePassport: by comparing the real biometrical data (face) of the ePass presenter with the stored biometrical data (DG2) of the ePass holder).<br>The Basic Inspection System with PACE is a PCT additionally supporting/applying the Passive Authentication protocol. |

| Term | Definition |
|---|---|
| *Biographical data (biodata)* | The personalised details of the travel document holder appearing as text in the visual and machine readable zones of and electronically stored in the travel document. The biographical data are less-sensitive data. |
| *Biometric reference data* | Data stored for biometric authentication of the travel document holder in the travel document as (i) digital portrait and (ii) optional biometric reference data (e.g. finger and iris). |
| *Card Access Number (CAN)* | A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Passport), semi-static (e.g. printed on a label on the Passport) or dynamic (randomly chosen by the electronic travel document and displayed by it using e.g. ePaper, OLED or similar technologies), see [ICAO_9303] |
| *Counterfeit* | An unauthorised copy or reproduction of a genuine security document made by whatever means [ICAO_9303]. |
| *Country Signing CertA Certificate ($C_{CSCA}$)* | Certificate of the Country Signing Certification Authority Public Key ($K_{PuCSCA}$) issued by Country Signing Certification Authority and stored in the rightful terminals. |
| *Country Signing Certification Authority (CSCA)* | An organisation enforcing the policy of the ePass Issuer with respect to<br>confirming correctness of user and TSF data stored in the ePass. The CSCA represents the country specific root of the PKI for the ePasss and creates the Document Signer Certificates within this PKI.<br>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. |
| *Document Basic Access Keys* | Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KBENC) and message authentication (key KBMAC) of data transmitted between the TOE and an inspection system using BAC [ICAO_9303]. They are derived from the MRZ and used within BAC to authenticate an entity able to read the printed MRZ of the passport book; see [ICAO_9303]. |
| *Document Details Data* | Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data. |
| *Document Security Object ($SO_D$)* | A RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups: A hash for each Data Group in use shall be stored in the Security Data. It is stored in the *ePassport* application (EF.SOD) of the travel document. It may carry the Document Signer Certificate (CDS); see [ICAO_9303], sec. A.10.4. |
| *Document Signer (DS)* | An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the ePass for passive authentication.<br>A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS)(CDS), see [ICAO_9303].<br>This role is usually delegated to a Personalisation Agent. |
| *Eavesdropper* | A threat agent reading the communication between the travel document and the terminal to gain the data on the travel document. |
| *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; see [ICAO_9303]. |
| *ePassport application* | A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [ICAO_9303]. |
| *Forgery* | Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [ICAO_9303]. |

| Term | Definition |
|---|---|
| *Global Interoperability* | The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all travel documents; see [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 cycle phases. |
| *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 cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE. |
| *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; see [ICAO_9303] |
| *Improperly documented person* | A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required; see [ICAO_9303] |
| *Initialisation Data* | Any data defined by the travel document manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as travel document material (IC identification data). |
| *Inspection* | The act of an official organisation (inspection authority) examining an travel document presented to it by an travel document presenter and verifying its authenticity as the travel document holder. See also [ICAO_9303]. |
| *Inspection system* | see BIS-PACE for this PP.<br>see also BIS-BAC for general information |
| *Integrated circuit (IC)* | Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit. |
| *Integrity* | Ability to confirm the travel document and its data elements stored upon have not been altered from that created by the travel document Issuer. |
| *Issuing Organisation* | Organisation authorised to issue an official travel document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [ICAO_9303] |
| *Issuing State* | The country issuing the travel document; see [ICAO_9303] |
| *Logical Data Structure (LDS)* | The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the travel document's chip. |
| *Machine readable zone (MRZ)* | Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods; see [ICAO_9303].<br>The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for both PACE and BAC. |
| *Machine-verifiable biometrics feature* | A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine; see [ICAO_9303]. |
| *Manufacturer* | Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life-cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. |
| *PACE password* | A password needed for PACE authentication, e.g. CAN or MRZ. |

| Term | Definition |
|---|---|
| *PACE Terminal (PCT)* | A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter.<br>PCT implements the terminal's part of the PACE protocol and authenticates itself to the ePass using a shared password (CAN or MRZ). |
| *Passive authentication* | Security mechanism implementing (i) verification of the digital signature of the Card/Chip or Document Security Object and (ii) comparing the hash values of the read data fields with the hash values contained in the Card/Chip or Document Security Object. See [ICAO_9303]. |
| *Passport (physical and electronic)* | An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Passport is used in order to verify that identity claimed by the Passport presenter is commensurate with the identity of the Passport holder stored on/in the card. |
| *Password Authenticated Connection Establishment (PACE)* | A communication establishment protocol defined in [ICAO_9303]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained. |
| *Personal data* | The personal data stored in the contactless IC as defined to be the mandatory minimum for global interoperability are the MRZ and the digitally stored image of the bearer's face.<br>The personal data of the document holder contained in the MRZ: last name, first name, date of birth, sex, nationality and optional data. |
| *The Personal Identification Number (PIN)* | Secret password that SHALL be only known to the legitimate holder of the document. |
| *Personalisation* | The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. |
| *Personalisation Agent* | An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:<br>(i)establishing the identity of the travel document holder for the biographic data in the travel document,<br>(ii)enrolling the biometric reference data of the travel document holder,<br>(iii)writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO_9303],<br>(iv) writing the document details data,<br>(v) writing the initial TSF data,<br>(vi)signing the Document Security Object defined in [ICAO_9303] (in the role of DS).<br><br>Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.<br>Generating signature key pair(s) is not in the scope of the tasks of this role. |

| Term | Definition |
|---|---|
| *Personalisation Data* | A set of data incl. (i) individual-related data (biographic and biometric data,) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). 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*. |
| *PIN Unblock Key (PUK)* | A long secret password that SHALL be only known to the legitimate holder of the document. |
| *Pre-personalisation Data* | Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised travel document and/or to secure shipment within or between the life cycle phases *manufacturing* and *card issuing*. |
| *Pre-personalised* travel document*'s chip* | travel document's chip equipped with a unique identifier and a unique Authentication Key Pair of the chip. |
| *Receiving State* | The Country to which the travel document holder is applying for entry; see [ICAO_9303]. |
| *Reference data* | Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt. |
| *RF-terminal* | A device being able to establish communication with an RF-chip according to ISO/IEC 14443 |
| *Rightful equipment (rightful terminal or rightful Card)* | A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either BIS-PACE (see *Inspection System*). |
| *Secondary image* | A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [ICAO_9303]. |
| *Secure messaging in combined mode* | Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 |
| *Skimming* | Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact communication channel of the TOE without knowledge of the printed MRZ and CAN dataPACE password. |
| *Standard Inspection Procedure* | A specific order of authentication steps between an travel document and a terminal as required by [ICAO_9303], namely (i) PACE and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC. |
| *Supplemental Access Control* | A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control. |
| *Terminal* | A Terminal is any technical system communicating with the TOE through a contactless / contact interface. |
| *TOE tracing data* | Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document |
| *Travel document* | Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO_9303] (there "Machine readable travel document"). |
| *Travel document (electronic)* | The contactless/contact smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*. |
| *Travel document holder* | A person for whom the ePass Issuer has personalised the travel document. |
| *Travel document Issuer (issuing authority)* | Organisation authorised to issue an electronic Passport to the travel document holder |
| *Travel document presenter* | A person presenting the travel document to a terminal and claiming the identity of the travel document holder. |
| *TSF data* | Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC_1]). |

| Term | Definition |
|---|---|
| *Unpersonalised travel document* | travel document material prepared to produce a personalised travel document containing an initialised and pre-personalised travel document's chip. |
| *User Data* | All data (being not authentication data)<br>(i)stored in the context of the *ePassport* application of the travel document as defined in [ICAO_9303] and<br>(ii)being allowed to be *read out* solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_9303]).<br><br>CC give the following generic definitions for user data:<br>Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC_1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC_2]). |
| *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 |
|---|---|
| *BAC* | Basic Access Control |
| *BIS-BAC* | Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [PP_BAC]) |
| *BIS-PACE* | Basic Inspection System with PACE |
| *CAN* | Card Access Number |
| *CC* | Common Criteria |
| *CertA* | Certification Authority |
| *MRZ* | Machine readable zone |
| *n.a.* | Not applicable |
| *OSP* | Organisational security policy |
| *PACE* | Password Authenticated Connection Establishment |
| *PCD* | Proximity Coupling Device |
| *PICC* | Proximity Integrated Circuit Chip |
| *PP* | Protection Profile |
| *RF* | Radio Frequency |
| *SAC* | Supplemental Access Control |
| *SAR* | Security assurance requirements |
| *SFR* | Security functional requirement |
| *SIP* | Standard Inspection Procedure, see [ICAO_9303] |
| *TOE* | Target of Evaluation |
| *TSF* | TOE security functionality |
| *TSP* | TOE Security Policy (defined by the current document) |

# 10 LITERATURE


**Common Criteria**

[CC_1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017

[CC_2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 5, April 2017

[CC_3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 5, April 2017

[CC_EM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017

**Protection Profiles**

[PP_IC] Security IC Platform Protection Profile with Augmented Packages, Version 1.0; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0084-2014

[PP_BAC] Machine readable travel documents with “ICAO Application”, Basic Access control – BSI-PP-0055 v1.10 25th march 2009

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

[PP_PACE] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, V1.01 22nd July 2014

[PP_EACwPACE] Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Application Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012-MA-02, Version 1.3.2, 5th December 2012

[PP_0090] Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP], BSI-CC-PP-0090-2016, Version 0.9.2, August 18th, 2016.

[PP_0087] Common Criteria Protection ProfileMachine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], Version 2.0.3, July 18th, 2016, BSI-CC-PP-0087-V2-2016-MA-01

**ANSSI**

[JIL_SRCL] Joint Interpretation Library – Security requirements for post-delivery code loading – Version 1.0, February 2016

[ANSSI-PG-083] Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. ANSSI, Version 2.04, 2020-01-01

**IC**

[IC_CERT] ANSSI-CC-2023_37

[IC_ST][5] Public Security Target SCR404U version B Reference SEC222

**ICAO**

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021 – Part 11: Security Mechanisms for MRTDs

[ICAO_9303_10] ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021 – Part 10: Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

[ICAO_9303_12] ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021 – Part 12: Part 12: Public Key Infrastructure for MRTDs

[ICAO] 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 TRAVEL DOCUMENTS, TECHNICAL REPORT for Machine Readable Travel Documents, Version 1.1, April 2014

**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_15946] Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves

[ISO_9796_2] ISO/IEC 9796-2:2010 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms

[ISO_18013] ISO/IEC 18013-2:2020 Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies, Part 3: Access control, authentication and integrity validation — Amendment 1: PACE protocol, Part 4: Test methods

**IDEMIA**

[ALC_STM] Secure transfer of masks, I CRD13 2 CRD 507

**Other**

[TR_03110] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1: eMRTDs with BAC/PACEv2 and EACv1, and Part 3: Common Specification TR-03110, Version 2.2, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[TR_03111] BSI: Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 2012

[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

[5] The version of this document can be found in [IC_CERT].

[FIPS_186_5] FIPS 186-5, Federal Information Processing Standards Publication (FIPS PUB) 186-5, Digital Signature Standard (DSS), Feb. 2023

[FIPS_197] FIPS 197, Federal Information Processing Standards Publication (FIPS PUB 197), Advanced Encryption Standard (AES)

[NIST_800_38B] NIST Special Publication 800-38B: 2005, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005

[GPC_SPE_034] GlobalPlatform – Card Specification – Version 2.2.1 – Public Release, January 2011

[IEEE] IEEE Std 1363a-2004 Standard Specification of Public-Key Cryptography

[ANSIX9.31] "Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (DSA)" - ANSI X9.31-1998, American Bankers Association

[SP800-90A] NIST SP 800-90 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)