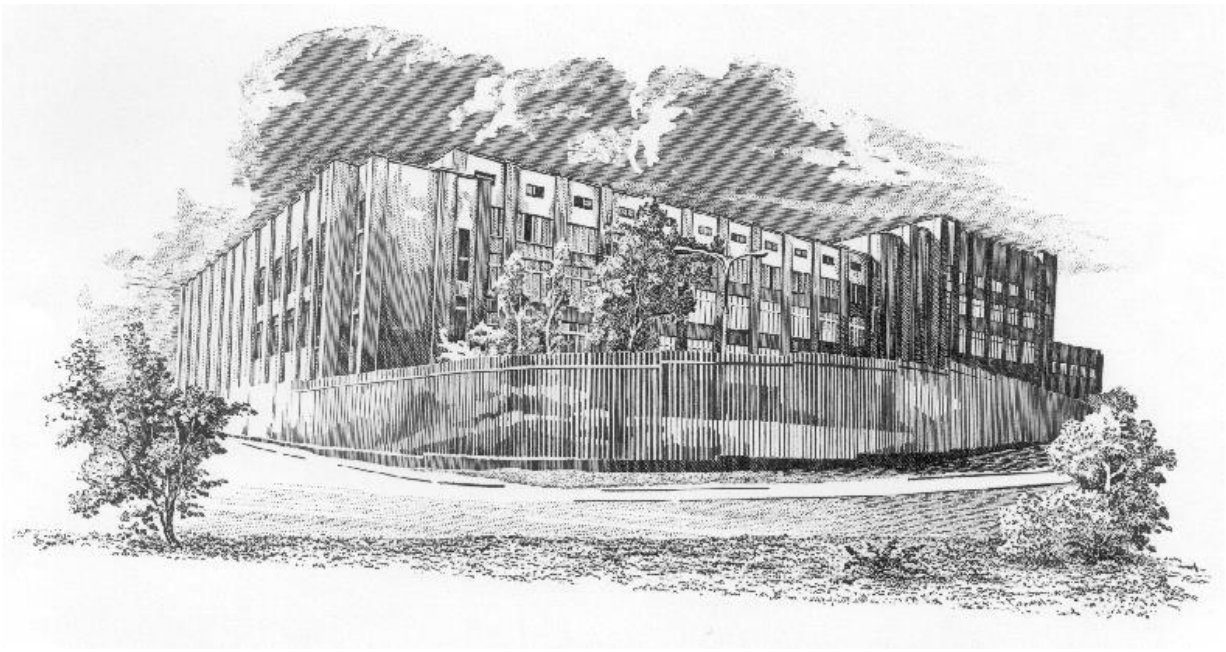
PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH



# PWPW SmartApp-MRTD 1.0

## Security Target Lite

This page is intentionally left blank.

# Table of contents

# List of figures

# List of tables

# 1 Introduction

## 1.1 References

### 1.1.1 Security Target reference

| | |
|---|---|
| ST title: | PWPW SmartApp-MRTD 1.0: Security Target Lite |
| ST author: | Polska Wytwórnia Papierów Wartościowych S.A. |
| ST version: | 1.0.3.0 |
| Evaluation body: | TÜV Informationstechnik GmbH (TÜViT) |
| Certification body: | Bundesamt für Sicherheit in der Informationstechnik (BSI) |
| Evaluation assurance level: | EAL4 augmented with the following assurance components ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5 |

### 1.1.2 Target of evaluation reference

| | |
|---|---|
| TOE identification: | PWPW SmartApp-MRTD 1.0 |
| TOE developer: | Polska Wytwórnia Papierów Wartościowych S.A. |
| TOE certification ID: | BSI-DSZ-CC-1176 |
| TOE HW: | SLC52GDA448, SLC52GDA448A2, SLC52GDA448A3 (IFX_CCI_000005h) |
| TOE FW version: | FW-00.100.17.0-SLCx2V3, NrgOS-02.01.2783-SLCx2V3, RFAPI_ROM-20.04.0006-SLCx2V3 |
| TOE HW certification ID: | BSI-DSZ-CC-1110-V5-2022 |

## 1.2 Intended usage

The TOE is intended for the usage in travel documents, e.g. e-passports or residence permit cards.

## 1.3 Target of evaluation

### 1.3.1 Overview

This security target defines the security objectives and requirements for the chip of machine readable travel documents based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) and EU Commission of Article 6.

It addresses the advanced security methods Password Authenticated Connection Establishment and Extended Access Control (Chip Authentication + Terminal Authentication) as defined in [Doc9303], [TR03110-1] and [TR03110-3].

The PWPW SmartApp-MRTD 1.0 comprises of:

- the hardware (microcontroller, the integrated circuit, IC),
- the native implementation of the e-passport,
- the guidance documentation.

The following hardware is used: SLC52GDA448, SLC52GDA448A2 and SLC52GDA448A3. The hardware is identified in [IC_ST] by the Common Criteria Identifier (CCI) as follows: IFX_CCI_000005h. The microcontroller is certified according to the Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1.

The information on the hardware components and their certifications are given in Table 1.1.

The e-passport application components are identified in Table 1.2.

The guidance documentation components are identified in Table 1.3.

**Table 1.1: TOE hardware and libraries components**

| Type | Developer | Name | Certification ID | EAL |
|---|---|---|---|---|
| Chip | IFX | SLC52GDA448, SLC52GDA448A2, SLC52GDA448A3 (IFX_CCI_000005h) | BSI-DSZ-CC-1110-V5-2022 | EAL 6+ |
| Crypto lib | IFX | Asymmetric Crypto Library, v02.08.007 | BSI-DSZ-CC-1110-V5-2022 | EAL 6+ |
| Other lib | IFX | Hardware Support Library, v03.12.8812 | BSI-DSZ-CC-1110-V5-2022 | EAL 6+ |

**Table 1.2: TOE native implementation components**

| Type | Developer | Name | Version |
|---|---|---|---|
| Executable | PWPW | PWPW SmartApp-MRTD | 1.0.44.0 |

**Table 1.3: Guidance documentation components**

| Type | Developer | Name |
|---|---|---|
| Document | PWPW | PWPW SmartApp-MRTD 1.0: Preparative procedures |
| Document | PWPW | PWPW SmartApp-MRTD 1.0: Operational user guidance |

*Note:*
*The exact versions of guidance documents are given in the certification report.*

The TOE supports the following security protocols/mechanisms specific for travel documents:

1. PACE or PACE with CAM,
2. Extended Access Control, i.e.:
   - Chip Authentication,
   - Terminal Authentication,
3. Passive Authentication.

Passive Authentication data is calculated by the TOE environment and stored securely in the TOE during its personalization.

### 1.3.2 TOE definition

The Target of Evaluation (TOE) addressed by this security target is an electronic travel document representing a contactless smart card programmed according to ICAO Technical Report “Security Mechanisms for MRTDs” [Doc9303-P11] (which means amongst others

according to the Logical Data Structure (LDS) defined in [Doc9303]) and additionally providing the Extended Access Control according to [Doc9303] and [TR03110-1], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to [PP-PACE].

The TOE comprises of at least:

- the circuitry of the travel document'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 (application) and
- the associated guidance documentation.

*Developer note:*

1. The IC being the part of the TOE is contactless

### 1.3.3 TOE usage and security features for operational use

A State or Organization 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 security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the machine readable zone (MRZ) and (iii) data elements on the travel document's chip according to LDS in case of contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid travel document personalized 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 Organization ensures the authenticity of the data of genuine travel documents. The Receiving State trusts a genuine travel document of an Issuing State or Organization.

For this security target the travel document is viewed as unit of:

1. 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:
    - the biographical data on the biographical data page of the travel document surface,
    - the printed data in the Machine Readable Zone (MRZ), and
    - the printed portrait;
2. the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [Doc9303] 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:
    - the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
    - the digitized portraits (EF.DG2),
    - the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1],

[1] These biometric reference data are optional according to [Doc9303]. This security target assumes that the Issuing State or Organization uses this option and protects these data by means of extended access control.

- the other data according to LDS (EF.DG5 to EF.DG16), and
- the Document Security Object ($SO_D$).

The Issuing State or Organization 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 organizational security measures (e.g. control of materials, personalization procedures) [Doc9303]. 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 Organization and the security features of the travel document's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Extended Access Control and the Data Encryption of sensitive biometrics as optional security measure in the [Doc9303] and Password Authenticated Connection Establishment [Doc9303-P11]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This security target 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 security target addresses the Chip Authentication v.1 described in [TR03110-1] as an alternative to the Active Authentication stated in [Doc9303].

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to [PP-PACE]. Note that [PP-PACE] considers high attack potential.

For the PACE protocol according to [Doc9303-P11], the following steps shall be performed:

1. The travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.
2. The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
3. 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 $K_{MAC}$ and $K_{ENC}$ from the shared secret.
4. 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) [TR03110-1], [Doc9303-P11].

The protection profile requires the TOE to implement the Extended Access Control as defined in [TR03110-1]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol v.1 and (ii) the Terminal Authentication Protocol v.1. The Chip Authentication Protocol v.1 (i) authenticates the travel document's chip to the inspection

system and (ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 or PACE-CAM has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the Receiving State or Organization through the Issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The Issuing State or Organization authorizes the Receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

The TOE uses the following cryptographic functions:

- Triple-DES in CBC mode with 112 bit keys complaint to [ISO18033-3] and [NIST800-38A];
- AES in CBC mode with 128, 192 and 256 bit keys complaint to [FIPS197] and [NIST800-38A];
- Retail-MAC, i.e. ISO/IEC 9797-1 MAC algorithm 3 with block cipher DES, zero IV (8 bytes), ISO/IEC 9797-1 padding method 2 and cryptographic key size of 112 complaint to [ISO9797-1];
- CMAC algorithm complaint to [FIPS197] and [NIST800-38B];
- ECDH key generation with key sizes of 224, 256, 320, 384, 512 and 521 bits compliant to [TR03111];
- ECDH with key sizes of 224, 256, 320, 384, 512 and 521 bits compliant to [IEEE1363];
- SHA-1 compliant to [FIPS180-4];
- SHA-224 compliant to [FIPS180-4];
- SHA-256 compliant to [FIPS180-4];
- ECDSA with SHA-1, compliant to [ISO15946-1] and [ISO15946-2];
- ECDSA with SHA-224 compliant to [ISO15946-1] and [ISO15946-2];
- ECDSA with SHA-256 compliant to [ISO15946-1] and [ISO15946-2];
- ECDSA with SHA-384 compliant to [ISO15946-1] and [ISO15946-2];
- ECDSA with SHA-512 compliant to [ISO15946-1] and [ISO15946-2].

Elliptic curve operations use the following curves:

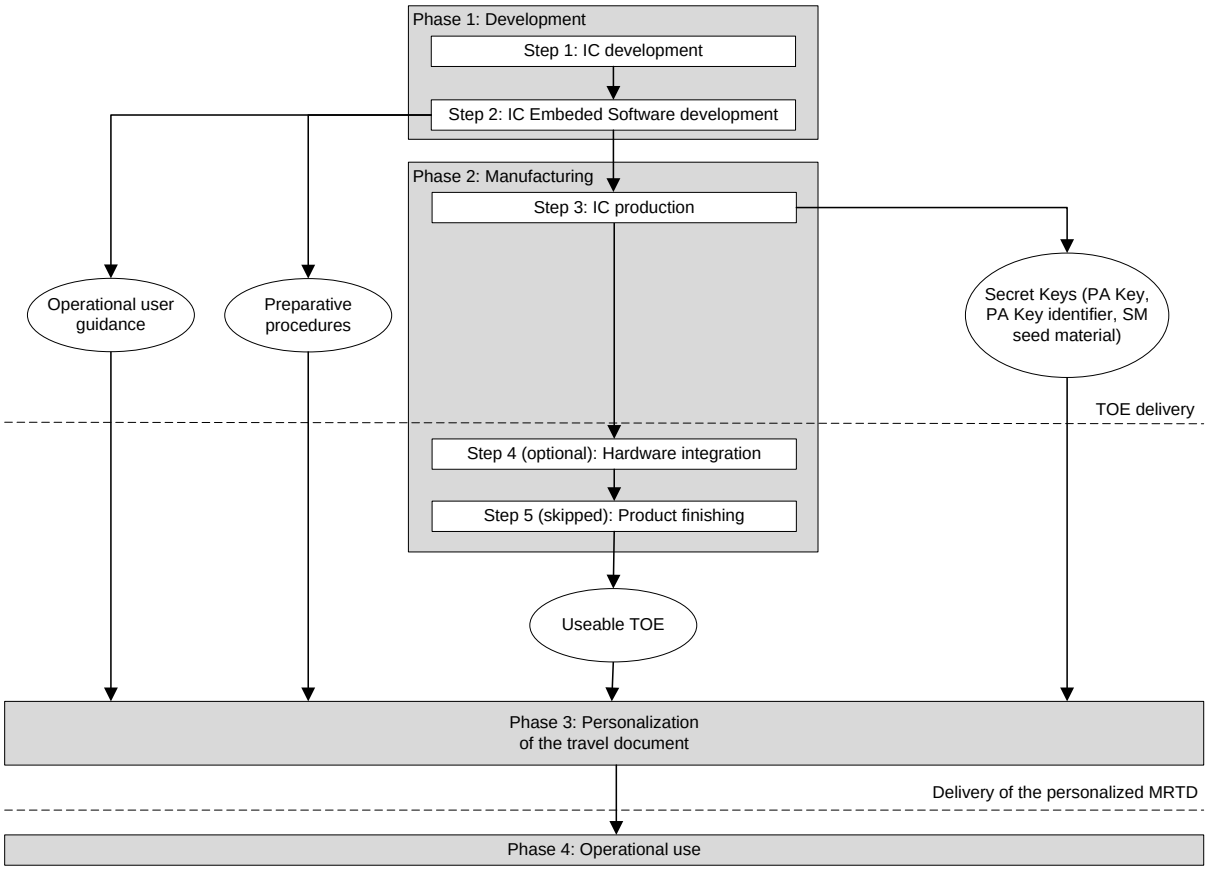
- NIST P-224 (secp224r1) [FIPS186-4],
- BrainpoolP224r1 [RFC5639],
- NIST P-256 (secp256r1) [FIPS186-4],
- BrainpoolP256r1 [RFC5639],
- BrainpoolP320r1 [RFC5639],
- NIST P-384 (secp384r1) [FIPS186-4],
- BrainpoolP384r1 [RFC5639],
- BrainpoolP512r1 [RFC5639],
- NIST P-521 (secp521r1) [FIPS186-4].

Table A.1 of Annex A lists all supported cryptographic algorithms and gives brief information on their usage.

### 1.3.4 Life cycle

The TOE life-cycle is described in terms of the four life-cycle phases. (With respect to the [PP-IC], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.). The TOE life cycle was presented on Figure 1.1.

**Figure 1.1: TOE life-cycle**




#### 1.3.4.1 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.

*Developer note:*
1. The IC is developed by the IFX.
2. The IC Dedicated Software (firmware) is developed by the IFX.

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

*Developer note:*
1. The Asymmetric Crypto Library (ACL) and Hardware Support Library (HSL) are developed by the IFX.
2. The IC Embedded Software (application) with the e-passport functionality is developed by the PWPW.
3. The guidance documentation associated with the application (the IC Embedded Software) is developed by the PWPW.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in an encrypted binary file is securely delivered to the IC manufacturer. The Embedded Software guidance documentation is securely delivered to the Personalization Agent.

#### 1.3.4.2 Phase 2: Manufacturing

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and the travel document's chip Embedded Software in the non-volatile memory (NVM). The IC Manufacturer (the Infineon) writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the IC Packaging Manufacturer.

The IC Manufacturer (the Infineon) during manufacturing process also generates Secret Keys (i.e. Personalization Agent key with its unique identifier and Secure Messaging seed material) and finally locks the Flash Loader, which will permanently disable the ability to reload or delete the Embedded Software.

Prepared IC is securely delivered from the IC Manufacturer (the Infineon) to the IC Packaging Manufacturer.

Generated Secret Keys are securely delivered from the IC Manufacturer (the Infineon) to the Personalization Agent.

*Developer note:*
The IC Manufacturer is represented by the Infineon. IC Packaging Manufacturer determines the smart card or inlay manufacturer. Personalization Agent is an organization acting on behalf of the travel document issuer to personalize the travel document for the travel document holder.

The TOE is delivered in sense of CC after Phase 2, Step 3.

(Step4 optional) The IC Packaging Manufacturer combines the IC with hardware for the contact-based/contactless interface in the travel document unless the travel document consists of the card or inlay only.

Prepared card or inlay is securely delivered from the IC Packaging Manufacturer to the Travel Document Manufacturer which prepares final MRTD.

(Step5) Is skipped.

*Application note 1 from [PP-PACE]:*
*Application note 1 from [PP-EAC]:*
Creation of the application implies:

- For file based operating systems: the creation of MF and ICAO.DF.
- For Java Card operating systems: the Applet instantiation.

*Developer note:*
During manufacturing process the PWPW SmartApp-MRTD 1.0 application is loaded into NVM. If all verification tests are passed and the IC is responding, it is ready to perform IC packaging activities. Chip cards or empty Passport Documents blankets are prepared by the Travel Document Manufacturer, then they are securely delivered from the Travel Document Manufacturer to the Personalization Agent. Personalization Agent also receives the guidance documentations (Preparative procedures and Operational user guidance) from the IC Embedded Software Developer (the PWPW).

#### 1.3.4.3 Phase 3: Personalization of the travel document

(Step6) The personalization of the travel document includes: (i) the survey of the travel document holder's biographical data, (ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the personalization of the visual readable data onto the physical part of the travel document, (iv) the writing of the TOE User Data and TSF Data into the logical travel document 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.

The signing of the document security object by the Document Signer [Doc9303] finalizes the personalization of the genuine travel document for the travel document holder. The personalized travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

*Application note 2 from [PP-EAC] (includes Application note 2 from [PP-PACE]):*
The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [CC-Part1] §92) comprise (but are not limited to) the Personalization Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

*Developer note:*
The TSF data of the TOE comprise:

- Personalization Agent's key and its identifier,
- seed material used to derive secure messaging session keys needed to open secure channel during personalization process,
- configuration data specifying security mechanism to be activated (e.g. PACE, CA, TA),
- cryptographic key to be used to establish PACE and the elliptic curve identifier,
- Chip Authentication Private Key and the elliptic curve identifier,
- Terminal Authentication trust anchor,
- effective date of the document.

*Application note 3 from [PP-PACE]:*
*Application note 3 from [PP-EAC]:*
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 [Doc9303]. This approach allows but does not enforce the separation of these roles.

#### 1.3.4.4 Phase 4: Operational use

(Step7) The TOE is used as a travel document's chip by the traveler and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the Issuing State or Organization and can be used according to the security policy of the Issuing State but they can never be modified.

*Application note 4 from [PP-PACE]:*
*Application note 4 from [PP-EAC]:*
The intention of the PP is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. 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.

*Developer note:*
1. The TOE is the product intended for local (national) and export projects. That is why, this evaluation process is limited to Steps 1-3 of the TOE life cycle. Such limitation is explicitly permitted by the protection profile.
2. If necessary, the evaluation of the other life cycle steps should be done as a separate process according to needs of the specific Issuing State.

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.

Some production steps, e.g. Step 4 in Phase 2 may also take place in the Phase 3.

### 1.3.5 Non-TOE hardware/software/firmware required by the TOE

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

In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless/contact based communication according to ISO/IEC 14443 and ISO/IEC 7816.

From the logical point of view, the TOE shall be able to recognize the following terminal types, which, hence, shall be available:
- Basic Inspection System with PACE,

- Extended Inspection System.

The TOE shall require terminals to evince possessing authorization information (a shared secret) before access according to [Doc9303], option 'PACE' is granted. To authenticate a terminal as a basic inspection system with PACE, Standard Inspection Procedure must be used.

In scope of [PP-PACE] the following types of inspection system shall be distinguished:

- BIS-PACE: Basic Inspection System[2] with PACE[3].

Moreover, [PP-EAC] introduces another type of inspection systems, i.e. EIS: Extended Inspection System.

*Developer note:*
Definitions of above inspection system types are cited in D.3.

[PP-PACE] defines security policy for the usage of only Basic Inspection System with PACE (BIS-PACE) in the context of the e-passport application. Using other types of inspection systems and terminals is out of the scope of [PP-PACE].

[2] Basic Inspection Systems always uses Standard Inspection Procedure
[3] SIP with PACE means: PACE and passive authentication with $SO_D$

# 2 Conformance claims

## 2.1 Common Criteria conformance claims

This security target claims conformance to:

- *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2017-04-001; Version 3.1, Revision 5, April 2017* [CC-Part1]
- *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2017-04-002; Version 3.1, Revision 5, April 2017* [CC-Part2]
- *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements; CCMB-2017-04-003; Version 3.1, Revision 5, April 2017* [CC-Part3]

as follows:

- Part 2 extended
- Part 3 conformant

*Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004; Version 3.1, Revision 5, April 2017* [CC-CEM] has to be taken into account.

## 2.2 Protection profile claims

This security target claims strict conformance to the following Common Criteria protection profiles:

- *Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, Version 1.0, 2nd November 2011* [PP-PACE]
- *Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, version 1.3.2, 5th December 2012* [PP-EAC]

## 2.3 Package claim

This security target is conformant to the assurance package EAL 4 augmented with the following assurance components ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5.

## 2.4 Conformance claims rationale

This security target uses only definitions of assets, threats, organizational security policies and assumptions given in the claimed protection profiles (see section 3 for details). No definition is modified. No additional definition is introduced.

This security target uses only security objectives given in the claimed protection profiles (see section 4 for details). No security objective is modified. No additional security objective is introduced.

This security target uses only extended components given in the claimed protection profiles (see section 5 for details). No extended component is modified. No additional extended component is introduced.

This security target uses SFRs given in the claimed protection profiles (see section 6 for details). Only operations of the SFRs (assignment, iteration, selection and refinement) explicitly permitted by the claimed protection profiles are done. One additional SFR is introduced, i.e. FCS_CKM.1.1/CAPK. It is done with the strict conformance to [PP-EAC].

All application notes given in the claimed protection profiles are considered and addressed. Moreover, all application notes requiring ST writer actions are commented with developer notes.

# 3 Security problem definition

This security target claims strict conformance to [PP-PACE] and [PP-EAC]. All definitions of assets, threats, organizational security policies and assumptions given in these protection profiles are included to the security target. The definitions are taken over as described in the protection profiles, therefore they are not repeated here.

## 3.1 Assets

The following definitions of primary assets are included:

- *user data stored on the TOE* from [PP-PACE]
- *user data transferred between the TOE and the terminal connected* from [PP-PACE]
- *travel document tracing data* from [PP-PACE]
- *logical travel document sensitive user data* from [PP-EAC]

All these primary assets represent User Data in the sense of the CC.

*Application note 6 from [PP-PACE]:*
Please note that user data 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 [PP-PACE] also secures these specific travel document holder's data.

*Application note 5 from [PP-EAC]:*
Due to interoperability reasons [Doc9303] requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC. Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [PP-BAC]). If supported, it is therefore recommended to use PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks.

*Developer note:*
The evaluated product does not support BAC, therefore the PACE protocol shall be used.

The following definitions of secondary assets are included:

- *accessibility to the TOE functions and data only for authorized subjects* from [PP-PACE]
- *genuineness of the TOE* from [PP-PACE]
- *TOE internal secret cryptographic keys* from [PP-PACE]
- *TOE internal non-secret cryptographic material* from [PP-PACE]
- *travel document communication establishment authorization data* from [PP-PACE]
- *authenticity of the travel document's chip* from [PP-EAC]

The secondary assets represent TSF and TSF-data in the sense of the CC.

*Application note 7 from [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 authorized person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.

*Developer note:*
Neither the PACE password nor any data derived from the PACE password is revealed by the TOE.

*Application note 8 from [PP-PACE]:*
Travel document communication establishment authorization 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 authorization attempt. The TOE shall secure the reference information as well as – together with the terminal connected[4] – 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.

*Developer note:*
1. The reference information is securely sent to the TOE during the personalization. Immediately upon its receiving: (i) the TOE derives the cryptographic key using the received reference information as a seed, (ii) stores the derived cryptographic key in the application's secure object and (iii) destroys the received reference data.
2. Neither the reference information nor the information derived from it is sent from the TOE.
3. As the PACE passwords are not sent to the TOE, it is sufficient to protect only authenticity and integrity of the verification information. It is achieved by using MACs as specified in [Doc9303-P11].

Only assets defined in the protection profiles are used in this security target. No additional asset is introduced.

## 3.2 Subjects

The following definitions of subjects are included:

- *travel document holder* from [PP-PACE]
- *travel document presenter (traveler)* from [PP-PACE]
- *terminal* from [PP-PACE][5]
- *basic inspection system with PACE (BIS-PACE)* from [PP-PACE]
- *document signer (DS)* from [PP-PACE]
- *country signing certification authority (CSCA)* from [PP-PACE]
- *personalization agent* from [PP-PACE]
- *manufacturer* from [PP-PACE]
- *country verifying certification authority (CVCA)* from [PP-EAC]

[4] the input device of the terminal
[5] This definition is introduced in [PP-PACE] and repeated in [PP-EAC].

- *document verifier (DV)* from [PP-EAC]
- *inspection system (IS)* from [PP-EAC]
- extended inspection system (EIS) from [PP-EAC]
- *attacker* from [PP-EAC][6]

*Application note 9 from [PP-PACE]:*
Since the TOE does not use BAC, a Basic Inspection System with BAC (BIS-BAC) cannot be recognized by the TOE.

*Developer note:*
The evaluated product does not support BAC, therefore the Basic Inspection System with BAC (BIS-BAC) cannot be recognized by the TOE.

*Application note 6 from [PP-EAC]:*
For definition of Basic Inspection System (BIS) resp. Basic Inspection System with PACE (BIS-PACE) see [PP-PACE].

*Application note 7 from [PP-EAC]:*
An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged travel document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

Only subjects defined in the protection profiles are used in this security target. No additional subject is introduced.

## 3.3 Threats

The following definitions of threats are included:

- *T.Skimming* from [PP-PACE]
- *T.Eavesdropping* from [PP-PACE]
- *T.Tracing* from [PP-PACE]
- *T.Forgery* from [PP-PACE]
- *T.Abuse-Func* from [PP-PACE]
- *T.Information_Leakage* from [PP-PACE]
- *T.Phys-Tamper* from [PP-PACE]
- *T.Malfunction* from [PP-PACE]
- *T.Read_Sensitive_Data* from [PP-EAC]
- *T.Counterfeit* from [PP-EAC]

*Application note 10 from [PP-PACE]:*
A product using BIS-BAC cannot avert *T.Skimming* in the context of the security policy defined in [PP-PACE].

[6] This definition is introduced in [PP-PACE] and then refined in [PP-EAC].

*Developer note:*
BAC is out of the TOE scope, so the above application note is not relevant for the TOE.

*Application note 11 from [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*.

*Application note 12 from [PP-PACE]:*
A product using BIS-BAC cannot avert *T.Eavesdropping* in the context of the security policy defined in [PP-PACE].

*Developer note:*
BAC is out of the TOE scope, so the above application note is not relevant for the TOE.

*Application note 13 from [PP-PACE]:*
*T.Tracing* completely covers and extends *T.Chip-ID* from [PP-BAC].

*Application note 14 from [PP-PACE]:*
A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert *T.Tracing* in the context of the security policy defined in from [PP-PACE].

*Developer note:*
BAC is out of the TOE scope, so the above application note is not relevant for the TOE.

*Application note 15 from [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)[7] cannot be averted by the current TOE.

*Developer note:*
The TOE supports Chip Authentication. It can be used to avert *T.Counterfeit*.

*Application note 8 from [PP-EAC]:*
*T.Forgery* from the [PP-PACE] shall be extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

*Developer note:*
*T.Forgery* definition resulting from the above application note will be as follows:

| | |
|---|---|
| *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 **and/or EIS** 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 |

[7] Such a threat might be formulated like: 'An attacker produces an unauthorized copy or reproduction of a *genuine* travel document to be used as part of a counterfeit Passport: he or she may generate a new data set or extract completely or partially the data from a genuine travel document and copy them on another functionally appropriate chip to imitate this genuine travel document. This violates the authenticity of the travel document being used for authentication of a travel document presenter as the travel document holder'.

*Application note 16 from [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.

*Application note 17 from [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).

*Developer note:*
The TOE uses security mechanisms provided by the hardware (see 1.1.2 for hardware details) to ensure protection against attacks described above.

*Application note 18 from [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.

*Developer note:*
The TOE uses security mechanisms provided by the hardware (see 1.1.2 for hardware details) to ensure protection against attacks described above.

*Application note 19 from [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.

*Developer note:*
The TOE uses security mechanisms provided by the hardware (see 1.1.2 for hardware details) to ensure protection against attacks described above.

Only threats defined in the protection profiles are used in this security target. No additional threat is introduced.

## 3.4 Organizational security policies

The following definitions of organizational security policies are included:

- *P.Manufact* from [PP-PACE]
- *P.Pre-Operational* from [PP-PACE]
- *P.Card_PKI* from [PP-PACE]
- *P.Trustworthy_PKI* from [PP-PACE]
- *P.Terminal* from [PP-PACE]
- *P.Sensitive_Data* from [PP-EAC]
- *P.Personalization* from [PP-EAC]

*Application note 20 from [PP-PACE]:*
The description of *P.Card_PKI* 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.

Only organizational security policies defined in the protection profiles are used in this security target. No additional security policy is introduced.

## 3.5 Assumptions

The following definitions of assumptions are included:

- *A.Passive_Auth* from [PP-PACE]
- *A.Insp_Sys* from [PP-EAC]
- *A.Auth_PKI* from [PP-EAC]

Only assumptions defined in the protection profiles are used in this security target. No additional assumption is introduced.

# 4 Security objectives

This security target claims strict conformance to [PP-PACE] and [PP-EAC]. All definitions of security objectives given in these protection profiles are included to the security target. The definitions are taken over as described in the protection profiles, therefore they are not repeated here.

## 4.1 Security objectives for the target of evaluation

The following definitions of security objectives for the target of evaluation are included:

- *OT.Data_Integrity* from [PP-PACE]
- *OT.Data_Authenticity* from [PP-PACE]
- *OT.Data_Confidentiality* from [PP-PACE]
- *OT.Tracing* from [PP-PACE]
- *OT.Prot_Abuse-Func* from [PP-PACE]
- *OT.Prot_Inf_Leak* from [PP-PACE]
- *OT.Prot_Phys-Tamper* from [PP-PACE]
- *OT.Prot_Malfunction* from [PP-PACE]
- *OT.Identification* from [PP-PACE]
- *OT.AC_Pers* from [PP-PACE]
- *OT.Sens_Data_Conf* from [PP-EAC]
- *OT.Chip_Auth_Proof* from [PP-EAC]

*Application note 21 from [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)[8] cannot be achieved by the current TOE.

*Developer note:*
The TOE supports Chip Authentication v.1. It shall be used when the proof of travel document authenticity is needed.

*Application note 22 from [PP-PACE]:*
*OT.Prot_Inf_Leak* pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

*Developer note:*
The above objective is fulfilled by security mechanisms of the hardware (see 1.1.2 for hardware details).

[8] Such a security objective might be formulated like: 'The TOE must enable the terminal connected to verify the authenticity of the travel document as a whole device as issued by the travel document Issuer (issuing PKI branch of the travel document Issuer) by means of the Passive and Chip Authentication as defined in [6]'.

*Application note 23 from [PP-PACE]:*
The *OT.AC_Pers* implies that the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalization.

*Developer note:*
The TOE permanently blocks writing access at the end of the personalization.

*Application note 9 from [PP-EAC]:*
The *OT.Chip_Auth_Proof* implies the travel document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined
in [Doc9303] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

*Developer note:*
1. The Document Number (the unique identity of the document) is stored in the TOE by the Personalization Agent during the personalization. The Document Number is stored in DG1 as specified in [Doc9303].
2. The Document Number is protected (as part of DG1) with the Passive Authentication as specified in [Doc9303].
3. The Chip Authentication Private Key is stored in the TOE by the Personalization Agent during the personalization.
4. The Chip Authentication Private Key is protected by storing it in a security object provided by the application with the e-passport functionality.
5. The Chip Authentication Public Key (the reference data used to verify the authentication attempt of travel document's chip) is stored in DG14 as specified in [Doc9303].
6. The Chip Authentication Public Key is protected (as part of DG14) with the Passive Authentication as specified in [Doc9303].

Only security objectives for the target of evaluation defined in the protection profiles are used in this security target. No additional security objective is introduced.

## 4.2 Security objectives for the operational environment

The following definitions of security objectives for the operational environment are included:

- *OE.Legislative_Compliance* from [PP-PACE]
- *OE.Passive_Auth_Sign* from [PP-PACE]
- *OE.Personalization* from [PP-PACE]
- *OE.Terminal* from [PP-PACE]
- *OE.Travel_Document_Holder* from [PP-PACE]
- *OE.Auth_Key_Travel_Document* from [PP-EAC]
- *OE.Authoriz_Sens_Data* from [PP-EAC]
- *OE.Exam_Travel_Document* from [PP-EAC]
- *OE.Prot_Logical_Travel_Document* from [PP-EAC]
- *OE.Ext_Insp_Systems* from [PP-EAC]

*Application note 24 from [PP-PACE]:*
*OE.Terminal* completely covers and extends *OE.Exam_MRTD, OE.Passive_Auth_Verif* and *OE.Prot_Logical_MRTD* from [PP-BAC].

Only security objectives for the operational environment defined in the protection profiles are used in this security target. No additional security objective is introduced.

## 4.3 Security objectives rationale

All threats described in this security target are coming from [PP-PACE] and [PP-EAC]. No new threat, no new organization security policy and no new assumption is introduced. Therefore security objectives rationales given in the protection profiles remain in force.

# 5 Extended component definition

This security target claims strict conformance to [PP-PACE] and [PP-EAC]. All definitions of extended components given in these protection profiles are included to the security target. The definitions are taken over as described in the protection profiles, therefore they are not repeated here.

The following definitions of extended components are included:

- *FAU_SAS.1* from [PP-PACE]
- *FCS_RND.1* from [PP-PACE]
- *FMT_LIM.1* from [PP-PACE]
- *FMT_LIM.2* from [PP-PACE]
- *FPT_EMS.1* from [PP-PACE]
- *FIA_API.1* from [PP-EAC]

*Application note 25 from [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.

*Application note 10 from [PP-EAC]:*
The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. [PP-EAC] defines the family FIA_API in the style of [CC-Part2] from a TOE point of view.

Only extended components defined in the protection profiles are used in this security target. No additional extended component is introduced.

# 6 Security requirements

This section defines the functional requirements for the TOE and the assurance requirements for the TOE.

*Application note 11 from [PP-EAC]:*
The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From travel document's point of view the domestic Document Verifier belongs to the issuing State or Organization.

## 6.1 Security functional requirements

The permitted operations (assignment, iteration, selection and refinement) of the SFR, which have been made by the PP author are denoted as underlined text.

The permitted operations (assignment, iteration, selection and refinement) of the SFR, which have been filled in by the ST author are denoted as *underlined and italic text*.

### 6.1.1 Class FCS: Cryptographic Support

#### 6.1.1.1 FCS_CKM: Cryptographic key management

**FCS_CKM.1/DH_PACE**
**Cryptographic key generation – Diffie-Hellman for PACE session keys**

*FCS_CKM.1.1/DH_PACE*

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to [TR03111]* and specified cryptographic key sizes *of 112, 128, 192, 256 bits* that meet the following: [Doc9303-P11].

*Developer note:*
1. Session keys of 112 bits length are generated when secure messaging is based on Triple-DES.
2. Session keys of 128, 192 and 256 bits lengths are generated when secure messaging is based on AES.
3. The complete list of supported elliptic curves is given inA.2.

*Application note 26 from [PP-PACE]:*
The TOE generates a shared secret value K with the terminal during the PACE protocol, see [Doc9303-P11]. This protocol may be based on the Diffie-Hellman Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [PKCS#3]) or on the ECDH compliant to TR-03111 [TR03111] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [Doc9303-P11] and [TR03111] for details). The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-$K_{MAC}$, PACE-$K_{ENC}$) according to [Doc9303-P11] for the TSF required by *FCS_COP.1/PACE_ENC* and *FCS_COP.1/PACE_MAC*.

*Developer note:*
The TOE uses ECDH to generate a shared secret value. Then, the shared secret value is used for deriving the Triple-DES or AES session keys for message encryption and message authentication.

*Application note 27 from [PP-PACE]:*
*FCS_CKM.1/DH_PACE* implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [Doc9303-P11].

*Developer note:*
1. The TOE uses SHA-1 to derive 112 (Triple-DES) and 128 (AES) bits session keys.
2. The TOE uses SHA-256 to derive 192 (AES) and 256 (AES) bits session keys.

**FCS_CKM.1/CA**
**Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys**

*FCS_CKM.1.1/CA*

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *based on an ECDH protocol* and specified cryptographic key sizes *of 112 bits, 128 bits, 192 bits, 256 bits* that meet the following: *based on an ECDH protocol compliant to [TR03111]*.

*Developer note:*
1. Session keys of 112 bits length are generated when secure messaging is based on Triple-DES.
2. Session keys of 128, 192 and 256 bits lengths are generated when secure messaging is based on AES.
3. The complete list of supported elliptic curves is given inA.2.

*Application note 12 from [PP-EAC]:*
FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [TR03110-1].

*Developer note:*
1. The TOE uses SHA-1 to derive 112 (Triple-DES) and 128 (AES) bits session keys.
2. The TOE uses SHA-256 to derive 192 (AES) and 256 (AES) bits session keys.

*Application note 13 from [PP-EAC]:*
The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [TR03110-1]. This protocol may be based on the Diffie-Hellman Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [PKCS#3]) or on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [TR03111], for details). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [TR03110-1]).

*Developer note:*
The TOE uses ECDH to generate a shared secret value. Then, the shared secret value is used for deriving the Triple-DES or AES session keys for message encryption and message authentication.

*Application note 14 from [PP-EAC]:*
The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 may use SHA-1 (cf. [TR03110-1]). The TOE may implement additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [TR03110-1] for details).

*Developer note:*
1. The TOE uses SHA-1 to derive 112 (Triple-DES) and 128 (AES) bits session keys for secure messaging.
2. According to requirements given in the section A.2.3 of [TR03110-3], the bit-length of the hash function shall be greater or equal to the bit-length of the derived key. That is why, the Chip Authentication Protocol implemented by the TOE uses SHA-256 to derive session keys of 192 (AES) and 256 (AES) bits lengths for secure messaging.
3. The Terminal Authentication implemented by the TOE supports SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512.

*Application note 15 from [PP-EAC]:*
The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [PP-PACE] after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

*Developer note:*
Session keys are cleared by the application once a secure messaging session is broken due to:
- receiving APDU in a plain text,
- unsuccessful MAC verification,
- unsuccessful APDU decryption,
- establishing new secure messaging keys (starting a new session),
- card reset resulting with the application selection.

**FCS_CKM.1/CAPK**
**Cryptographic key generation – Chip Authentication key pair**

*FCS_CKM.1.1/CAPK*

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Generating ECDH / ECDSA keys with Brainpool curve or NIST curve (for length 521 bits)* and specified cryptographic key sizes *of 224, 256, 320, 384, 512 and 521 bits* that meet the following: *[ISO15946-1], [ISO15946-3], [TR03110-1] and [TR03110-3].*

*Developer note:*
The complete list of supported elliptic curves is given inA.2.

*Developer note:*
The Chip Authentication key pair can either be generated in the TOE or imported by the Manufacturer or Personalization Agent (see FMT_MTD.1/CAPK). This SFR has been included as required by [PP-EAC] (see application note after FMT_MTD.1/CAPK). This SFR has been included in this security target in addition to the SFRs defined by the protection

profiles claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed protection profiles.

**FCS_CKM.4**
**Cryptographic key destruction – Session keys**

*FCS_CKM.4.1*

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physically overwriting the keys with zeros* that meets the following: *none*.

*Application note 28 from [PP-PACE]:*
The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by *FDP_RIP.1*.

*Developer note:*
Session keys are cleared by the application once a secure messaging session is broken due to:
- receiving APDU in a plain text,
- unsuccessful MAC verification,
- unsuccessful APDU decryption,
- establishing new secure messaging keys (starting a new session),
- the application selection,
- card reset resulting with the application selection.

### 6.1.1.2 FCS_COP: Cryptographic operation

**FCS_COP.1/PACE_ENC**
**Cryptographic operation – Encryption / Decryption AES / 3DES**

*FCS_COP.1.1/PACE_ENC*

The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *Triple-DES and AES* in CBC mode and cryptographic key sizes *of 112, 128, 192, 256 bits* that meet the following: compliant to [Doc9303-P11].

*Developer note:*
1. Session keys of 112 bits length are used for Triple-DES.
2. Session keys of 128, 192 and 256 bits lengths are used for AES.

*Application note 29 from [PP-PACE]:*
This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the *FCS_CKM.1/DH_PACE* (PACE-$K_{ENC}$).

*Developer note:*
The TOE uses secure messaging which is implemented based on cryptographic coprocessor provided by the hardware manufacturer (see 1.1.2 for hardware details).

**FCS_COP.1/PACE_MAC**
**Cryptographic operation – MAC**

*FCS_COP.1.1/PACE_MAC*

The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *Retail-MAC and CMAC* and cryptographic key sizes *of 112, 128, 192, 256 bits* that meet the following: compliant to [Doc9303-P11].

*Developer note:*
1. Retail-MAC and session keys of 112 bits length are used when secure messaging is based on Triple DES algorithm.
2. CMAC and session keys of 128, 192 and 256 bits lengths are used when secure messaging is based on AES algorithm.

*Application note 30 from [PP-PACE]:*
This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the *FCS_CKM.1/DH_PACE* (PACE-$K_{MAC}$). Note that in accordance with [Doc9303-P11] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

*Developer note:*
The TOE uses secure messaging which is implemented based on cryptographic coprocessor provided by the hardware manufacturer (see 1.1.2 for hardware details).

**FCS_COP.1/CA_ENC**
**Cryptographic operation – Symmetric Encryption / Decryption**

*FCS_COP.1.1/CA_ENC*

The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *Triple-DES and AES* and cryptographic key sizes *of 112, 128, 192, 256 bits* that meet the following: [Doc9303-P11].

*Developer note:*
1. Session keys of 112 bits length are used for Triple-DES.
2. Session keys of 128, 192 and 256 bits lengths are used for AES.

*Application note 16 from [PP-EAC]:*
This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

*Developer note:*
The TOE uses secure messaging which is implemented based on cryptographic coprocessor provided by the hardware manufacturer (see 1.1.2 for hardware details).

**FCS_COP.1/CA_MAC**
**Cryptographic operation – MAC**

*FCS_COP.1.1/CA_MAC*

The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *Retail-MAC and CMAC* and cryptographic key sizes *of 112, 128, 192, 256 bits* that meet the following: [Doc9303-P11].

*Developer note:*
1. Retail-MAC and session keys of 112 bits length are used when secure messaging is based on Triple DES algorithm.
2. CMAC and session keys of 128, 192 and 256 bits lengths are used when secure messaging is based on AES algorithm.

*Application note 18 from [PP-EAC]:*
This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the authentication mechanism.

*Developer note:*
The TOE uses secure messaging which is implemented based on cryptographic coprocessor provided by the hardware manufacturer (see 1.1.2 for hardware details).

**FCS_COP.1/SIG_VER**
**Cryptographic operation – Signature verification by travel document**

*FCS_COP.1.1/SIG_VER*

The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm *ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512* and cryptographic key sizes *of 224, 256, 320, 384, 512 and 521 bits* that meet the following: *[ISO15946-1], [ISO15946-2] and [FIPS180-4]*.

*Developer note:*
The complete list of supported elliptic curves is given inA.2.

*Application note 17 from [PP-EAC]:*
Information for the security target author only – no action required.

### 6.1.1.3 FCS_RND: Generation of random numbers

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

*FCS_RND.1.1*

The TSF shall provide a mechanism to generate random numbers that meet *class PTG.3 according to [AIS20/AIS31]*.

*Developer note:*
Presented below are security functional requirements for the RNG class PTG.3 taken from [IC_ST]:

**FCS_RNG.1**
**Random number generation (Class PTG.3)**

FCS_RNG.1.1
The TSF shall provide a hybrid physical random number generator that implements:

(PTG.3.1)
A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output.

(PTG.3.2)
If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.

(PTG.3.3)
The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.

(PTG.3.4)
The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.3.5)
The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

*IFX-Note*: Continuously means that the raw random bits are scanned continuously. The algorithmic post-processing belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function. The output data rate of the post-processing algorithm shall not exceed its input data rate.

(PTG.3.6)
The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.

FCS_RNG.1.2
The TSF shall provide numbers in the format 8- or 16-bit that meet:

(PTG.3.7)
Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A.

*Application note 31 from [PP-PACE]:*
This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by *FIA_UAU.4/PACE*.

### 6.1.2 Class FIA: Identification and Authentication

*Application note 19 from [PP-EAC]:*
The Table 6.1 provides an overview on the authentication mechanisms used.

**Table 6.1: Overview on authentication SFR**

| Name | SFR for the TOE |
|---|---|
| Authentication Mechanism for Personalization Agents | FIA_UAU.4/PACE |
| Chip Authentication Protocol v.1 | FIA_API.1<br>FIA_UAU.5/PACE<br>FIA_UAU.6/EAC |
| Terminal Authentication Protocol v.1 | FIA_UAU.5/PACE |
| PACE protocol | FIA_UAU.1/PACE<br>FIA_UAU.5/PACE<br>FIA_AFL.1/PACE |
| Passive Authentication | FIA_UAU.5/PACE |

Note the Chip Authentication Protocol Version 1 as defined in this security target includes:

- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol Version 1,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

#### 6.1.2.1 FIA_AFL: Authentication failures

**FIA_AFL.1/PACE**
**Authentication failure handling – PACE authentication using non-blocking authorization data**

*FIA_AFL.1.1/PACE*

The TSF shall detect when *greater than 0 (zero)* unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.

*FIA_AFL.1.2/PACE*

When the defined number of unsuccessful authentication attempts has been met, the TSF shall *delay each following authentication attempt until the next successful authentication using the formula: (1000/999)*n*n, for 0 < n < 64 and 4100 for n greater or equal to 64*.

*Developer note:*
Values of above formula are expressed in seconds, e.g. *4100* is equal to *4100* seconds; *n* represents number of unsuccessful authentication attempts.

*Application note 32 from [PP-PACE]:*
The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [Doc9303-P11]) or for an arbitrary subset of them or may also separately be defined for each datum in question. Since all non-blocking authorization data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy[9], the TOE shall not allow a quick monitoring of its behavior (e.g. due to a long reaction time) in order to make the first step of the skimming attack[10] requiring an attack potential beyond high, so that the threat *T.Tracing* can be averted in the frame of the security policy of [PP-PACE]. One of some opportunities for performing this operation might be 'consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords'.

#### 6.1.2.2 FIA_UID: User identification

**FIA_UID.1/PACE**
**Timing of identification**

*FIA_UID.1.1/PACE*

The TSF shall allow:
1. to establish a communication channel,
2. carrying out the PACE Protocol according to [Doc9303-P11],
3. to read the Initialization Data if it is not disabled by TSF according to *FMT_MTD.1/INI_DIS*,
4. to carry out the Chip Authentication Protocol v.1 according to [TR03110-1],
5. to carry out the Terminal Authentication Protocol v.1 according to [TR03110-1],
6. *none*.

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.

*Application note 33 from [PP-PACE]:*
User identified after a successfully performed PACE protocol is a PACE authenticated BIS-PACE. Please note that neither CAN nor MRZ effectively represent secrets (but other PACE passwords may do so), but are restricted-revealable; i.e. it is either the travel document holder itself or an authorized other person or device (BIS-PACE).

*Developer note:*
The TOE supports MRZ and CAN only. No other PACE password is supported.

[9] ≥ 100 bits; a theoretical maximum of entropy which can be delivered by a character string is N*ld(C), whereby N is the length of the string, C – the number of different characters which can be used within the string.
[10] guessing CAN or MRZ, see *T.Skimming* above

*Application note 20 from [PP-EAC]:*
The SFR FIA_UID.1/PACE in [PP-EAC] covers the definition in [PP-PACE] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to [PP-PACE].

*Application note 21 from [PP-EAC]:*
In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The travel document manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the travel document". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalization Agent (using the Personalization Agent Key).

*Developer note:*
1. In the Phase 2 of the life cycle, the Manufacturer is the only user role known to the TOE.
2. Transition from Phase 2 to Phase 3 of the life cycle creates the user role Personalization Agent and involves permanent blocking of the user role Manufacturer.
3. Transition from Phase 3 to Phase 4 of the life cycle creates the user role Inspection System and permanently blocks the user role Personalization Agent.

*Application note 22 from [PP-EAC]:*
User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. it is either the travel document holder itself or an authorized other person or device (Basic Inspection System with PACE).

*Application note 23 from [PP-EAC]:*
In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. Please note that a Personalization Agent acts on behalf of the travel document issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalization Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalization Agent', when a terminal proves the respective Terminal Authorization Level as defined by the related policy (policies).

*Developer note:*
The authentication procedure for Personalization Agents is specified in AGD_PRE.1.

#### 6.1.2.3 FIA_UAU: User authentication

**FIA_UAU.1/PACE**
**Timing of authentication**

*FIA_UAU.1.1/PACE*

The TSF shall allow:
1. to establish a communication channel,
2. carrying out the PACE Protocol according to [Doc9303-P11] [11],
3. to read the Initialization Data if it is not disabled by TSF according to *FMT_MTD.1/INI_DIS*,
4. to identify themselves by selection of the authentication key,
5. to carry out the Chip Authentication Protocol Version 1 according to [TR03110-1],
6. to carry out the Terminal Authentication Protocol Version 1 according to [TR03110-1],
7. *none*.

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.

*Application note 34 from [PP-PACE]:*
The user authenticated after a successfully performed PACE protocol is a PACE authenticated BIS-PACE. Please note that neither CAN nor MRZ effectively represent secrets (but other PACE passwords may do so), but are restricted-revealable; i.e. it is either the travel document holder itself or an authorized other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$), cf. *FTP_ITC.1/PACE*.

*Application note 24 from [PP-EAC]:*
The SFR FIA_UAU.1/PACE. in [PP-EAC] covers the definition in [PP-PACE] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to [PP-PACE].

*Application note 25 from [PP-EAC]:*
The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. it is either the travel document holder itself or an authorized other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$), cf. FTP_ITC.1/PACE.

**FIA_UAU.4/PACE**
**Single-use authentication mechanisms – Single-use authentication of the Terminals by the TOE**

*FIA_UAU.4.1/PACE*

The TSF shall prevent reuse of authentication data related to:

[11] travel document identifies itself within the PACE protocol by selection of the authentication key ephem-$PK_{PICC}$-PACE

1. PACE Protocol according to [Doc9303-P11],
2. Authentication Mechanism based on *AES-256*,
3. Terminal Authentication Protocol v.1 according to [TR03110-1].

*Application note 35 from [PP-PACE]:*
For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits length being (almost) uniformly distributed.

*Developer note:*
As input of a generic mapping function required by the PACE protocol and used by the TOE has to be of the same length as an elliptic curve base point order, the selected nonce is extended with the leading zeros to the required length.

*Application note 26 from [PP-EAC]:*
The SFR FIA_UAU.4.1 in [PP-EAC] covers the definition in [PP-PACE] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to [PP-PACE]. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [PP-PACE].

*Application note 27 from [PP-EAC]:*
The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalization Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

*Developer note:*
All authentication mechanisms listed in FIA_UAU.4.1/PACE use challenges freshly and randomly generated by the TOE.

**FIA_UAU.5/PACE**
**Multiple authentication mechanisms**

*FIA_UAU.5.1/PACE*

The TSF shall provide:
1. PACE Protocol according to [Doc9303-P11],
2. Passive Authentication according to [Doc9303],
3. Secure messaging in MAC-ENC mode according to [Doc9303-P11],
4. Symmetric Authentication Mechanism based on *AES-256*,
5. Terminal Authentication Protocol v.1 according to [TR03110-1].

to support user authentication.

*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 Personalization Agent by the Authentication Mechanism with Personalization Agent Key(s).
3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1
5. *none*.

*Application note 36 from [PP-PACE]:*
Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of e-passport application.

*Application note 28 from [PP-EAC]:*
The SFR FIA_UAU.5.1/PACE in [PP-EAC] covers the definition in [PP-PACE] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in [PP-EAC] covers the definition in [PP-PACE] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to [PP-PACE].

**FIA_UAU.6/PACE**
**Re-authenticating of Terminal by the TOE**

*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.

*Application note 37 from [PP-PACE]:*
The PACE protocol specified in [Doc9303-P11] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see *FCS_COP.1/PACE_MAC* for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

*Developer note:*
1. The TOE uses Retail-MAC or CMAC to verify APDUs protected with secure messaging.
2. Once APDU with incorrect MAC is received, the TOE breaks secure messaging session.

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

*FIA_UAU.6.1/EAC*

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

*Application note 29 from [PP-EAC]:*
The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [Doc9303] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

*Developer note:*
1. The TOE uses Retail-MAC or CMAC to verify APDUs protected with secure messaging.
2. Once APDU with incorrect MAC is received, the TOE breaks secure messaging session.

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

*FIA_API.1.1*

The TSF shall provide a Chip Authentication Protocol Version 1 according to [TR03110-1] to prove the identity of the TOE.

*Application note 30 from [PP-EAC]:*
This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [TR03110-1]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or ECDH) and two session keys for secure messaging in ENC_MAC mode according to [Doc9303]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

*Developer note:*
The TOE implements the Chip Authentication Mechanism v.1 based on ECDH.

### 6.1.3 Class FDP: User Data Protection

#### 6.1.3.1 FDP_ACC: Access control policy

**FDP_ACC.1/TRM**
**Subset access control – Terminal Access**

*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 and data stored in EF.SOD of the logical travel document.

*Application note 38 from [PP-PACE]:*
Information for the security target author only – no action required.

*Application note 31 from [PP-EAC]:*
The SFR FIA_ACC.1.1 in [PP-EAC] covers the definition in [PP-PACE] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to [PP-PACE].

#### 6.1.3.2 FDP_ACF: Access control functions

**FDP_ACF.1/TRM**
**Security attribute based access control – Terminal Access**

*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,
   c. Extended Inspection System;
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 document,
   d. all TOE intrinsic secret cryptographic keys stored in the travel document[12];
3. Security attributes:
   a. Authentication status of terminals,
   b. Terminal Authentication v.1,
   c. Authorization of the Terminal.

*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 [Doc9303-P11] after a successful PACE authentication as required by *FIA_UAU.1/PACE*.

*FDP_ACF.1.3/TRM*

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

[12] e.g. Chip Authentication Version 1 and ephemeral keys

*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 User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.
3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.
5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.

*Application note 39 from [PP-PACE]:*
Information for the security target author only – no action required.

*Application note 40 from [PP-PACE]:*
Please note that the Document Security Object ($SO_D$) stored in EF.SOD (see [Doc9303]) does not belong to the user data, but to the TSF-data. The Document Security Object can be read out by the PACE authenticated BIS-PACE, see [Doc9303].

*Application note 41 from [PP-PACE]:*
Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by *FTP_ITC.1/PACE*.

*Application note 32 from [PP-EAC]:*
The SFR FDP_ACF.1.1/TRM in [PP-EAC] covers the definition in [PP-PACE] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in [PP-EAC] cover the definition in [PP-PACE]. The SFR FDP_ACF.1.4/TRM in [PP-EAC] covers the definition in [PP-PACE] and extends it by 3) to 6). These extensions do not conflict with the strict conformance to [PP-PACE].

*Application note 33 from [PP-EAC]:*
The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [TR03110-1]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

*Application note 34 from [PP-EAC]:*
Please note that the Document Security Object ($SO_D$) stored in EF.SOD (see [Doc9303]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [Doc9303-P11].

*Application note 35 from [PP-EAC]:*
FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

*Developer note:*
1. After completing the Password Authenticated Connection Establishment, new secure messaging session keys ($K_{ENC}$ and $K_{MAC}$) are derived.
2. After completing Chip Authentication, session keys resulting from Password Authenticated Connection Establishment are cleared. Then a new secure messaging session is started with new keys resulting from the Chip Authentication.

#### 6.1.3.3 FDP_RIP: Residual information protection

**FDP_RIP.1**
**Subset residual information protection**

*FDP_RIP.1.1*

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource from* the following objects:
1. Session Keys (immediately after closing related communication session),
2. the ephemeral private key-$SK_{PICC}$-PACE (by having generated a DH shared secret K[13]),
3. *none*.

*Application note 42 from [PP-PACE]:*
The functional family *FDP_RIP* possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family *FPT_EMS*. Applied to cryptographic keys, *FDP_RIP.1* requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to *FCS_CKM.4* that merely requires a fact of key destruction according to a method/standard.

*Developer note:*
The TOE has implemented own mechanism to store cryptographic keys, which ensure secure clearing and de-allocation.

#### 6.1.3.4 FDP_UCT: Inter-TSF user data confidentiality transfer protection

**FDP_UCT.1/TRM**
**Basic data exchange confidentiality – MRTD**

*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.

[13] according to [SAC]

#### 6.1.3.5 FDP_UIT: Inter-TSF user data integrity transfer protection

**FDP_UIT.1/TRM**
**Data exchange integrity**

*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.

### 6.1.4 Class FTP: Trusted Path/Channels

#### 6.1.4.1 FTP_ITC: Inter-TSF trusted channel

**FTP_ITC.1/PACE**
**Inter-TSF trusted channel after PACE**

*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 ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal.

*Application note 43 from [PP-PACE]:*
The trusted IT product is the terminal. In *FTP_ITC.1.3/PACE*, the word “initiate” is changed to ‘enforce”, as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

*Application note 44 from [PP-PACE]:*
The trusted channel is established after successful performing the PACE protocol (*FIA_UAU.1/PACE*). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$): this secure messaging enforces preventing tracing while Passive Authentication and the required properties of *operational* trusted channel; the cryptographic primitives being used for the secure messaging are as required by *FCS_COP.1/PACE_ENC* and *FCS_COP.1/PACE_MAC*. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements *FIA_AFL.1/PACE*.

*Application note 45 from [PP-PACE]:*
Please note that the control on the user data stored in the TOE is addressed by *FDP_ACF.1/TRM*.

### 6.1.5 Class FAU: Security Audit

#### 6.1.5.1 FAU_SAS: Audit data storage

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

*FAU_SAS.1.1*

The TSF shall provide the Manufacturer with the capability to store the Initialization and Pre-Personalization Data in the audit records.

*Application note 46 from [PP-PACE]:*
The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase ‘manufacturing’. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialization and/or Pre-personalization Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see *FMT_MTD.1/INI_ENA*, *FMT_MTD.1/INI_DIS*). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

*Developer note:*
1. In the Phase 2 of the life cycle, the Manufacturer is the only user role known to the TOE.
2. The Manufacturer user role performs the following operations:
   - stores embedded software (including the application with the e-passport functionality) in the chip,
   - writes PA authentication key, PA key identifier and secure messaging seed material for the Personalization Agent user role,
3. All operations listed above are reversible, i.e. they can be repeated many times as long as the TOE is in the Phase 2 of the life cycle.
4. The Manufacturer should lock the ability to reload application at the end of manufacturing.

### 6.1.6 Class FMT: Security Management

#### 6.1.6.1 FMT_SMF: Specification of management functions

**FMT_SMF.1**
**Specification of management functions**

*FMT_SMF.1.1*

The TSF shall be capable of performing the following management functions:
1. Initialization,
2. Pre-personalization,
3. Personalization,
4. Configuration.

#### 6.1.6.2 FMT_SMR: Security management roles

*Application note 36 from [PP-EAC]:*
The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data.

**FMT_SMR.1/PACE**
**Security roles**

*FMT_SMR.1.1/PACE*

The TSF shall maintain the roles
1. Manufacturer,
2. Personalization Agent,
3. Terminal,
4. PACE authenticated BIS-PACE,
5. Country Verifying Certification Authority,
6. Document Verifier,
7. Domestic Extended Inspection System,
8. Foreign Extended Inspection System.

*FMT_SMR.1.2/PACE*

The TSF shall be able to associate users with roles.

*Application note 47 from [PP-PACE]:*
For explanation on the role Manufacturer and Personalization Agent please refer to the glossary. The role Terminal is the default role for any terminal being recognized by the TOE as not PACE authenticated BIS-PACE (‘Terminal’ is used by the travel document presenter).
The TOE recognizes the travel document holder or an authorized other person or device (BIS-PACE) by using PACE authenticated BIS-PACE (*FIA_UAU.1/PACE*).

*Application note 37 from [PP-EAC]:*
The SFR FMT_SMR.1.1/PACE in [PP-EAC] covers the definition in [PP-PACE] and extends it by 5) to 8). This extension does not conflict with the strict conformance to [PP-PACE].

#### 6.1.6.3 FMT_LIM: Limited capabilities and availability

*Application note 38 from [PP-EAC]:*
The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

**FMT_LIM.1**
**Limited capabilities**

*FMT_LIM.1.1*

The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (*FMT_LIM.2*)' the following policy is enforced: Deploying test features after TOE delivery do not allow:
1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks, and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

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

*FMT_LIM.2.1*

The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (*FMT_LIM.1*)' the following policy is enforced: Deploying test features after TOE delivery do not allow:
1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks, and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

*Application note 39 form [PP-EAC] (includes Application note 48 from [PP-PACE]):*
The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.
Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

*Developer note:*
Test features of the TOE are no longer available when the application with the e-passport functionality is used in phase 2 (manufacturing). This test features are even disabled on the source code level.

#### 6.1.6.4 FMT_MTD: Management of TSF data

*Application note 40 from [PP-EAC]:*
The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

*FMT_MTD.1.1/INI_ENA*

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

**FMT_MTD.1/INI_DIS**
**Management of TSF data – Reading and using Initialization and Pre-personalization Data**

*FMT_MTD.1.1/INI_DIS*

The TSF shall restrict the ability to read out the Initialization Data and the Pre-personalization Data to the Personalization Agent.

*Application note 49 from [PP-PACE]:*
The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialization Data (as required by *FAU_SAS.1*) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases ‘manufacturing’ and ‘issuing’, but being not needed and may be misused in the ‘operational use’. Therefore, read and use access to the Initialization Data shall be blocked in the ‘operational use’ by the Personalization Agent, when he switches the TOE from the life cycle phase ‘issuing’ to the life cycle phase ‘operational use’.

*Developer note:*
1. The Initialization Data and the Pre-personalization Data can be written many times when the TOE is in the Phase 2 of the life cycle.
2. The Manufacturer user role is permanently blocked during the transition from the Phase 2 to the Phase 3 of the life cycle.
3. Read and use access to the Initialization Data is permanently blocked during the transition from the Phase 2 to the Phase 3 of the life cycle.
4. Read and use access to the Pre-personalization Data is permanently blocked during the transition from the Phase 3 to the Phase 4 of the life cycle.

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

*FMT_MTD.1.1/KEY_READ*

The TSF shall restrict the ability to read the:
1. PACE passwords,
2. Chip Authentication Private Key,
3. Personalization Agent Keys

to none.

*Application note 45 from [PP-EAC]:*
The SFR FMT_MTD.1/KEY_READ in [PP-EAC] covers the definition in [PP-PACE] and extends it by additional TSF data. This extension does not conflict with the strict conformance to [PP-PACE].

**FMT_MTD.1/PA**
**Management of TSF data – Personalization Agent**

*FMT_MTD.1.1/PA*

The TSF shall restrict the ability to write the Document Security Object ($SO_D$) to the Personalization Agent.

*Application note 50 from [PP-PACE]:*
By writing $SO_D$ into the TOE, the Personalization Agent confirms (on behalf of DS) the correctness and genuineness of all the personalization data related. This consists of user- and TSF-data.

**FMT_MTD.1/CVCA_INI**
**Management of TSF data – Initialization of CVCA Certificate and Current Date**

*FMT_MTD.1.1/CVCA_INI*

The TSF shall restrict the ability to write the:
1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date,
4. *none*

to *the Personalization Agent*.

*Application note 41 from [PP-EAC]:*
Information for the security target author only – no action required.

**FMT_MTD.1/CVCA_UPD**
**Management of TSF data – Country Verifying Certification Authority**

*FMT_MTD.1.1/CVCA_UPD*

The TSF shall restrict the ability to update the:
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate

to Country Verifying Certification Authority.

*Application note 42 from [PP-EAC]:*
The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [TR03110-1]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [TR03110-1]).

**FMT_MTD.1/DATE**
**Management of TSF data – Current date**

*FMT_MTD.1.1/DATE*

The TSF shall restrict the ability to modify the Current date to:
1. Country Verifying Certification Authority,
2. Document Verifier,
3. Domestic Extended Inspection System.

*Application note 43 from [PP-EAC]:*
The authorized roles are identified in their certificate (cf. [TR03110-1]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication v.1 (cf. to [TR03110-1]).

**FMT_MTD.1/CAPK**
**Management of TSF data – Chip Authentication Private Key**

*FMT_MTD.1.1/CAPK*

The TSF shall restrict the ability to *create, load* the Chip Authentication Private Key to *the Manufacturer and Personalization Agent*.

*Application note 44 from [PP-EAC]:*
The component FMT_MTD.1/CAPK is refined by (i) selecting other operations and (ii) defining a selection for the operations “create” and “load” to be performed by the ST writer. The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb “create” means here that the Chip Authentication Private Key is generated by the TOE itself. In the latter case the ST writer shall include an appropriate instantiation of the component FCS_CKM.1/CA as SFR for this key generation. The ST writer shall perform the assignment for the authorized identified roles in the SFR component FMT_MTD.1/CAPK.

*Developer note:*
1. The following operations have been selected: ‘load’, ‘create’.
2. Due to selecting the ‘create’ operation, the following instantiation of the component FCS_CKM.1/CA (as SFR) has been done: FCS_CKM.1/CAPK.

**FMT_MTD.3**
**Secure TSF data**

*FMT_MTD.3.1*

The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control.

**Refinement: The certificate chain is valid if and only if:**

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

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

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

*Application note 46 from [PP-EAC]:*
The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

### 6.1.7 Class FPT: Protection of the Security Functions

#### 6.1.7.1 FPT_EMS: TOE emanation

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

*FPT_EMS.1.1*

The TOE shall not emit *electromagnetic emissions or variations in the time or power consumption required to process an APDU command* in excess of *levels that could be measured or analyzed in the current state of art* enabling access to:
1. Chip Authentication Session Keys,
2. PACE session keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$),
3. the ephemeral private key ephem-$SK_{PICC}$-PACE,
4. *none*,
5. Personalization Agent Key(s),
6. Chip Authentication Private Key, and
7. *none*.

*FPT_EMS.1.2*

The TSF shall ensure any users are unable to use the following interface travel document's contactless/contact interface and circuit contacts to gain access to:
1. Chip Authentication Session Keys,
2. PACE session keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$),
3. the ephemeral private key ephem-$SK_{PICC}$-PACE,
4. *none*,
5. Personalization Agent Key(s),
6. Chip Authentication Private Key, and
7. *none*.

*Application note 51 from [PP-PACE]:*
The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

*Developer note:*
The TOE uses security mechanisms provided by the hardware (see 1.1.2 for hardware details) to ensure protection against attacks described above.

*Application note 47 from [PP-EAC]:*
The SFR FPT_EMS.1.1 in [PP-EAC] covers the definition in [PP-PACE] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in [PP-EAC] covers the definition in [PP-PACE] and extends it by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to [PP-PACE].

*Application note 48 from [PP-EAC]:*
The ST writer shall perform the operation in FPT_EMS.1.1 and FPT_EMS.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 [ISO7816-2] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

*Developer note:*
The TOE uses security mechanisms provided by the hardware (see 1.1.2 for hardware details) to ensure protection against attacks described above.

#### 6.1.7.2 FPT_FLS: Fail secure

**FPT_FLS.1**
**Failure with preservation of secure state**

*FPT_FLS.1.1*

The TSF shall preserve a secure state when the following types of failures occur:
1. exposure to operating conditions causing a TOE malfunction,
2. failure detected by TSF according to *FPT_TST.1*,
3. *none.*

#### 6.1.7.3 FPT_TST: TSF self test

**FPT_TST.1**
**TSF testing**

*FPT_TST.1.1*

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

*FPT_TST.1.2*

The TSF shall provide authorized users with the capability to verify the integrity of the TSF-data.

*FPT_TST.1.3*

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

*Application note 52 from [PP-PACE]:*
If the travel document's chip uses state of the art smart card technology, it will run some self tests at the request of an authorized user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by *FPT_TST.1.3* may be executed during initial start-up by the 'authorized user' Manufacturer in the life cycle phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

*Developer note:*
1. The TOE uses security mechanisms provided by the hardware (see 1.1.2 for hardware details) to ensure integrity of stored TSF executable code.
2. The TOE automatically verifies the integrity of the TSF-data before every use of these data.

#### 6.1.7.4 FPT_PHP: TSF physical protection

**FPT_PHP.3**
**Resistance to physical attack**

*FPT_PHP.3.1*

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

*Application note 53 from [PP-PACE]:*
The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

*Developer note:*
The TOE uses its own counter which is increased after physical manipulation and physical probing. If the counter reaches *five* value, the application is permanently blocked and all sensitive data is cleared.

## 6.2 Security assurance requirements

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the assurance package EAL 4 and augmented by taking the following components ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

*Application note 49 from [PP-EAC]:*
The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using the Chip Authentication Protocol v.1 (*OE.Prot_Logical_Travel_Document*). If the TOE is operated in non-certified mode using the BAC-established communication channel, the confidentiality of the standard data shall be protected against attackers with at least Enhanced-Basic attack potential (AVA_VAN.3).

## 6.3 Security requirements rationale

Most of security functional requirements and security assurance requirements described in this security target are coming from [PP-PACE] and [PP-EAC]. The security requirement rationales stated in chapter 6.3 of both documents [PP-PACE] and [PP-EAC] applies to this Security Target.

The remaining security requirement FCS_CKM.1 (related to cryptographic key generation) described in this security target was derived directly from [CC-Part2].

Mapping of the FCS_CKM.1/CAPK security functional requirement to security objectives was presented in the Table 6.2. The rationale was described below.

**Table 6.2: Functional requirement to TOE security objectives mapping**

| **Security Functional Requirement** | **Security Objectives for the TOE** | OT.Data_Integrity | OT.Data_Authenticity | OT.Data_Confidentiality | OT.Tracing | OT.Prot_Abuse-Func | OT.Prot_Inf_Leak | OT.Prot_Phys-Tamper | OT.Malfunction | OT.Identification | OT.AC_Pers | OT.Sens_Data_Conf | OT.Chip_Auth_Proof |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1/CAPK | | | | | | | | | | | | | X |

The security objective OT.Chip_Auth_Proof "Proof of travel document's chip authenticity" is ensured by the cryptographic key pair generation as required by FCS_CKM.1/CAPK. The FCS_CKM.1/CAPK requirement was described in chapter 6.1.1.1. NIST and Brainpool elliptic curves with cryptographic key sizes of 224, 256, 320, 384, 512 and 521 were selected for key pair generation. These algorithms are sufficient to generate strong enough key pairs used during Chip Authentication version 1, which will allow proving the travel document's authenticity.

# 7 Target of evaluation summary specification

This section describes all security functions implemented by the TOE and maps their functionalities to SFRs. The mapping allows to demonstrate, that all SFRs defined in this security target have been addressed and each of them is covered by at least one security function.

Each security function has its representation in the module of the application with the e-passport functionality.

## 7.1 SFR to TSF mapping

**Table 7.1: Functional requirement to TOE security functionality mapping**

| TOE security functional requirement / TOE Security functionality | SF.MRTD | SF.CRYPTO | SF.SAUTH | SF.PACE | SF.SM | SF.CA | SF.TA | SF.SEC | SF.CONF |
|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1/DH_PACE | | | | X | | | | | |
| FCS_CKM.1/CA | | | | | | X | | | |
| FCS_CKM.1/CAPK | | | | | | X | | | |
| FCS_CKM.4 | | | | | X | | | | |
| FCS_COP.1/PACE_ENC | | | | | X | | | | |
| FCS_COP.1/PACE_MAC | | | | | X | | | | |
| FCS_COP.1/CA_ENC | | | | | X | | | | |
| FCS_COP.1/CA_MAC | | | | | X | | | | |
| FCS_COP.1/SIG_VER | | | | | | | X | | |
| FCS_RND.1 | | X | | X | | | | | |
| FIA_AFL.1/PACE | | | | X | | | | | |
| FIA_UID.1/PACE | X | | | X | | X | X | | |
| FIA_UAU.1/PACE | X | | | X | | X | X | | |
| FIA_UAU.4/PACE | X | | | X | | | | | |
| FIA_UAU.5/PACE | | | X | X | X | X | X | | |
| FIA_UAU.6/PACE | | | | X | X | | | | |
| FIA_UAU.6/EAC | | | | | X | X | | | |
| FIA_API.1 | | | | | X | X | | | |

**Table 7.1 (continued)**

| TOE Security functionality / TOE security functional requirement | SF.MRTD | SF.CRYPTO | SF.SAUTH | SF.PACE | SF.SM | SF.CA | SF.TA | SF.SEC | SF.CONF |
|---|---|---|---|---|---|---|---|---|---|
| FDP_ACC.1/TRM | X | | | | | | | | |
| FDP_ACF.1/TRM | X | | | | | | | X | |
| FDP_RIP.1 | | | | X | X | | | X | |
| FDP_UCT.1/TRM | | | | | X | | | | |
| FDP_UIT.1/TRM | | | | | X | | | | |
| FTP_ITC.1/PACE | X | | | X | X | | | | |
| FAU_SAS.1 | X | | | | | | | | X |
| FMT_SMF.1 | X | | | | | | | | |
| FMT_SMR.1/PACE | X | | | | | | | | |
| FMT_LIM.1 | X | | | | | | | X | |
| FMT_LIM.2 | X | | | | | | | X | |
| FMT_MTD.1/INI_ENA | X | | X | | | | | | |
| FMT_MTD.1/INI_DIS | X | | X | | | | | | |
| FMT_MTD.1/KEY_READ | X | | | | | | | X | |
| FMT_MTD.1/PA | X | | X | | | | | | |
| FMT_MTD.1/CVCA_INI | X | | | | | | | | |
| FMT_MTD.1/CVCA_UPD | | | | | | | X | | |
| FMT_MTD.1/DATE | | | | | | | X | | |
| FMT_MTD.1/CAPK | X | | X | | | | | | |
| FMT_MTD.3 | | | | | | | X | | |
| FPT_EMS.1 | | | | | | | | X | |
| FPT_FLS.1 | | | | | | | | X | |
| FPT_TST.1 | | | | | | | | X | |
| FPT_PHP.3 | | | | | | | | X | |

## 7.2 SF.MRTD

The content is available in the complete Security Target documentation.

## 7.3 SF.CRYPTO

The content is available in the complete Security Target documentation.

## 7.4 SF.SAUTH

The content is available in the complete Security Target documentation.

## 7.5 SF.PACE

The content is available in the complete Security Target documentation.

## 7.6 SF.SM

The content is available in the complete Security Target documentation.

## 7.7 SF.CA

The content is available in the complete Security Target documentation.

## 7.8 SF.TA

The content is available in the complete Security Target documentation.

## 7.9 SF.SEC

The content is available in the complete Security Target documentation.

## 7.10 SF.CONF

The content is available in the complete Security Target documentation.

# 8 Statement of compatibility concerning the composite ST

## 8.1 Separation of the hardware TSF

### 8.1.1 Security functionalities

Table 8.1 confronts the relevant security functionalities of the platform with the security functionalities of the composite TOE to separate them. The security functionalities provided by the platform are summarized based on [IC_ST] and [IC_CR] (table 3).

## Table 8.1: Platform cryptographic functionalities used by the TOE

| Platform functionalities | Usage by the TOE | References/Remarks |
|---|---|---|
| Symmetric Cryptographic Co Processor | | |
| 3DES encryption in ECB mode | NO | [IC_CR], table 3 |
| **3DES encryption in CBC mode** | **YES** | **[IC_CR], table 3** |
| **3DES integrity verification in CBC-MAC mode** | **YES (dev. note 2)** | **[IC_CR], table 3** |
| 3DES integrity verification in CBC-MAC-ELB mode | NO | [IC_CR], table 3 |
| AES encryption in ECB mode | NO | [IC_CR], table 3 |
| **AES encryption in CBC mode** | **YES** | **[IC_CR], table 3** |
| **AES integrity verification in CBC-MAC mode** | **YES (dev. note 3)** | **[IC_CR], table 3** |
| AES integrity verification in CBC-MAC-ELB mode | NO | [IC_CR], table 3 |
| Symmetric Cryptographic Libraries (both) | | |
| 3DES encryption in ECB mode | NO | [IC_CR], table 3 |
| 3DES encryption in CBC, CRT and CFB modes | NO | [IC_CR], table 3 |
| 3DES encryption in PCBC mode | NO | [IC_CR], table 3 |
| 3DES authenticated encryption in PCBC mode | NO | [IC_CR], table 3 |
| 3DES in BLD (Blinding) and Recrypt modes | NO | [IC_CR], table 3 |
| 3DES-CMAC integrity verification | NO | [IC_CR], table 3 |
| AES encryption in ECB mode | NO | [IC_CR], table 3 |
| AES encryption in CBC, CRT, CFB modes | NO | [IC_CR], table 3 |
| AES encryption in PCBC mode | NO | [IC_CR], table 3 |
| AES authenticated encryption in PCBC mode | NO | [IC_CR], table 3 |
| AES in BLD (Blinding) and Recrypt modes | NO | [IC_CR], table 3 |
| AES-CMAC integrity verification | NO | [IC_CR], table 3 |
| Random Number Generation | | |
| **Hybrid Physical True Random Generation (PTG.2, PTG.3, DRG.2, DRG.3)** | **YES** | **[IC_CR], table 3** |
| RSA library v2.06.003 | | |
| RSA encryption | NO | [IC_CR], table 3 |
| RSA decryption with and without CRT | NO | [IC_CR], table 3 |
| RSA signature generation with and without CRT | NO | [IC_CR], table 3 |
| RSA signature verification (only modular exponentiation part) | NO | [IC_CR], table 3 |
| RSA library v2.07.003 + v2.08.007 | | |
| RSA encryption | NO | [IC_CR], table 3 |
| RSA decryption with and without CRT | NO | [IC_CR], table 3 |
| RSA signature generation with and without CRT | NO | [IC_CR], table 3 |
| RSA signature verification (only modular exponentiation part) | NO | [IC_CR], table 3 |
| RSA library v2.08.007 | | |
| RSA encryption | NO | [IC_CR], table 3 |
| RSA decryption with and without CRT | NO | [IC_CR], table 3 |
| RSA signature generation with and without CRT | NO | [IC_CR], table 3 |
| RSA signature verification (only modular exponentiation part) | NO | [IC_CR], table 3 |
| EC library v2.08.007 | | |
| **ECDSA signature generation** | **YES** | **[IC_CR], table 3** |
| **ECDH** | **YES** | **[IC_CR], table 3** |
| CIPURSE™ | | |
| CIPURSE™ Key Generation AES | NO | [IC_CR], table 3 |
| CIPURSE™ Session Key Agreement AES | NO | [IC_CR], table 3 |
| CIPURSE™ Authentication AES | NO | [IC_CR], table 3 |
| CIPURSE™ Secure Messaging for Integrity | NO | [IC_CR], table 3 |
| CIPURSE™ Secure Messaging for Confidentiality | NO | [IC_CR], table 3 |

*Developer note 1:*
The term platform is understood as: secure microcontroller with IC Dedicated Software and certified crypto libraries (i.e. HSL and ACL).

*Developer note 2:*
The composite TOE uses 3DES integrity verification in CBC-MAC mode of the platform SFRs: FCS_COP.1/TDES and FCS_CKM.4/TDES to implement the following SFRs: FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC, FIA_UAU.6/PACE and FIA_UAU.6/EAC.

*Developer note 3:*
The composite TOE uses AES integrity verification in CBC-MAC mode of the platform SFRs: FCS_COP.1/AES and FCS_CKM.4/AES to implement the following SFRs: FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC, FIA_UAU.6/PACE and FIA_UAU.6/EAC.

### 8.1.2 Security functional requirements

The following composite SFRs are platform related:
- FCS_CKM.1/DH_PACE,
- FCS_CKM.1/CA,
- FCS_CKM.1/CAPK,
- FCS_CKM.4,
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_COP.1/CA_ENC,
- FCS_COP.1/CA_MAC,
- FCS_COP.1/SIG_VER,
- FCS_RND.1,
- FDP_ACC.1/TRM,
- FDP_ACF.1/TRM,
- FAU_SAS.1,
- FMT_LIM.1,
- FMT_LIM.2,
- FPT_TST.1.

Other SFRs of the composite ST are not related directly to the platform.

The following SFRs of the platform contribute to the composite SFRs:
- FCS_COP.1/ECDH-1,
- FCS_COP.1/ECDH-2,
- FCS_CKM.1/EC-1,
- FCS_CKM.1/EC-2,
- FCS_CKM.1/EC-3,
- FCS_CKM.4/TDES,
- FCS_CKM.4/AES,
- FCS_COP.1/TDES,
- FCS_COP.1/AES,
- FCS_COP.1/ECDSA-1,
- FCS_COP.1/ECDSA-2,
- FCS_COP.1/ECDSA-3,

- FCS_RNG.1/HPRG,
- FDP_ACC.1,
- FDP_ACF.1,
- FAU_SAS.1,
- FDP_SDI.2,
- FDP_SDC.1,
- FMT_LIM.1,
- FMT_LIM.1/Loader,
- FMT_LIM.2,
- FMT_LIM.2/Loader,
- FPT_TST.2.

The other platform SFRs are not used.

Mapping of the platform SFRs to the composite SFRs is provided in Table 8.2.

**Table 8.2: SFRs mapping**

| Composite SFR | Platform SFR | Comments |
|---|---|---|
| FCS_CKM.1/DH_PACE | FCS_COP.1/ECDH-1<br>FCS_COP.1/ECDH-2 | ECDH key agreement is performed twice during each PACE establishment. |
| FCS_CKM.1/CA | FCS_COP.1/ECDH-1<br>FCS_COP.1/ECDH-2 | ECDH key agreement is performed during each CA establishment. |
| FCS_CKM.1/CAPK | FCS_CKM.1/EC-1<br>FCS_CKM.1/EC-2<br>FCS_CKM.1/EC-3 | Static ECDH key pair for CA can be generated during personalization of the TOE. |
| FCS_CKM.4 | FCS_CKM.4/TDES<br>FCS_CKM.4/AES | Secure messaging session keys are destroyed if:<br>• secure messaging has failed,<br>• new secure messaging was established<br>• they are not needed any more. |
| FCS_COP.1/PACE_ENC | FCS_COP.1/TDES<br>FCS_COP.1/AES | Triple DES and AES encryption functionality of the platform is used for secure messaging. |
| FCS_COP.1/PACE_MAC | FCS_COP.1/TDES<br>FCS_COP.1/AES | CBC-MAC mode of the platform SCP (Symmetric Cryptographic Coprocessor) is used for message integrity verification in secure messaging. |
| FCS_COP.1/CA_ENC | FCS_COP.1/TDES<br>FCS_COP.1/AES | Triple DES and AES encryption functionality of the platform is used for secure messaging. |
| FCS_COP.1/CA_MAC | FCS_COP.1/TDES<br>FCS_COP.1/AES | CBC-MAC mode of the platform SCP (Symmetric Cryptographic Coprocessor) is used for message integrity verification in secure messaging. |
| FCS_COP.1/SIG_VER | FCS_COP.1/ECDSA-1<br>FCS_COP.1/ECDSA-2<br>FCS_COP.1/ECDSA-3 | During the last step of the Terminal Authentication the TOE is verifying the signature from the terminal. On successful verification access to the sensitive data is granted. |
| FCS_RND.1 | FCS_RNG.1/HPRG | The TOE uses ACL (Asymmetric Crypto Library), which provides random number generation functionality. |

| | | |
|---|---|---|
| FIA_UID.1/PACE | FCS_COP.1/ECDH-1<br>FCS_COP.1/ECDH-2<br>FCS_CKM.1/EC-1<br>FCS_CKM.1/EC-2<br>FCS_CKM.1/EC-3<br>FCS_CKM.4/TDES<br>FCS_CKM.4/AES<br>FCS_COP.1/TDES<br>FCS_COP.1/AES<br>FCS_RNG.1/HPRG | The TOE allows to establish secure channel, PACE, CA and TA on behalf of the user to be performed before the user is identified. |
| FDP_ACC.1/TRM | FDP_ACC.1 | TOE rely on privilege level verification and security implemented on the platform. The TOE is using OS1 privileged level. |
| FDP_ACF.1/TRM | FDP_ACF.1 | TOE rely on privilege level verification and security implemented on the platform. The TOE is using OS1 privileged level. |
| FAU_SAS.1 | FAU_SAS.1 | The Manufacturer user role performs the following operations:<br>• writes identification data of the chip,<br>• stores embedded software (including the e-passport application) in the chip,<br>• writes authentication data for the Personalization Agent user role (Personalization Agent key, Personalization Agent key identifier, secure messaging seed material). |
| | FDP_SDI.2 | TOE is checking all responses from the HSL functions, which inform that data integrity error was detected. |
| | FDP_SDC.1 | TOE rely that confidentiality of data stored in the NVM is achieved by the platform. |
| FMT_LIM.1 | FMT_LIM.1 | Capabilities of the application are adopted to the user role, i.e.: developer, administrator and user. |
| | FMT_LIM.1/Loader | Flash Loader present in the platform can be deactivated during personalization process. |
| FMT_LIM.2 | FMT_LIM.2 | Availability of the application is adopted to the user role, i.e.: developer, administrator and user. |
| | FMT_LIM.2/Loader | Flash Loader present in the platform can be deactivated during personalization process. |
| FPT_TST.1 | FPT_TST.2 | In the operational phase there are run security tests by the Dedicated Software (IFX) as well as by the Embedded Software (PWPW). |

### 8.1.3 Security assurance requirements

It is shown in Table 8.3 that the security assurance requirements of the composite evaluation represent a subset of the SARs of the underlying platform.

**Table 8.3: Security assurance requirements of the platform ST and composite ST**

| Assurance component Platform ST | Compare | Assurance component Composite ST |
|---|---|---|
| Development | | |
| ADV_ARC.1 | = | ADV_ARC.1 |
| ADV_FSP.5 | ⊃ | ADV_FSP.4 |
| ADV_IMP.1 | = | ADV_IMP.1 |
| ADV_INT.2 | - | - |
| ADV_TDS.4 | ⊃ | ADV_TDS.3 |
| Guidance documents | | |
| AGD_OPE.1 | = | AGD_OPE.1 |
| AGD_PRE.1 | = | AGD_PRE.1 |
| Life-cycle support | | |
| ALC_CMC.4 | = | ALC_CMC.4 |
| ALC_CMS.5 | ⊃ | ALC_CMS.4 |
| ALC_DEL.1 | = | ALC_DEL.1 |
| ALC_DVS.2 | = | ALC_DVS.2 |
| ALC_LCD.1 | = | ALC_LCD.1 |
| ALC_TAT.2 | = | ALC_TAT.1 |
| Security target evaluation | | |
| ASE_CCL.1 | = | ASE_CCL.1 |
| ASE_ECD.1 | = | ASE_ECD.1 |
| ASE_INT.1 | = | ASE_INT.1 |
| ASE_OBJ.2 | = | ASE_OBJ.2 |
| ASE_REQ.2 | = | ASE_REQ.2 |
| ASE_SPD.1 | = | ASE_SPD.1 |
| ASE_TSS.1 | = | ASE_TSS.1 |
| Tests | | |
| ATE_COV.2 | = | ATE_COV.2 |
| ATE_DPT.3 | ⊃ | ATE_DPT.2 |
| ATE_FUN.1 | = | ATE_FUN.1 |
| ATE_IND.2 | = | ATE_IND.2 |
| Vulnerability assessment | | |
| AVA_VAN.5 | = | AVA_VAN.5 |

## 8.2 Compatibility between the composite ST and the platform ST

### 8.2.1 Threats

#### 8.2.1.1 Summary

The following threats of the composite ST are directly related to the platform functionality:

- T.Phys-Tamper,
- T.Malfunction,
- T.Abuse-Func,
- T.Information_Leakage,
- T.Forgery,
- T.Counterfeit,
- T.Read_Sensitive_Data.

The following platform threats are relevant for the TOE:

- T.Phys-Manipulation,
- T.Phys-Probing,
- T.Malfunction,
- T.Leak-Inherent,
- T.Leak-Forced,
- T.Abuse-Func,
- T.RND,
- T.Masquerade_TOE,
- T.Mem-Access.

#### 8.2.1.2 Rationale

Mapping of the platform threats to the composite ST threats is provided in Table 8.4.

**Table 8.4: Threats mapping**

| **Platform ST threats** | **Composite ST threats** | T.Phys-Tamper | T.Malfunction | T.Abuse-Func | T.Information_Leakage | T.Forgery | T.Counterfeit | T.Read_Sensitive_Data |
|---|---|---|---|---|---|---|---|---|
| T.Phys-Manipulation | | X | | | X | X | | |
| T.Phys-Probing | | X | | | X | | | |
| T.Malfunction | | X | X | | X | X | | |
| T.Leak-Inherent | | X | | | X | | | |
| T.Leak-Forced | | X | | | X | | | |
| T.Abuse-Func | | | | X | X | | | |
| T.RND | | X | X | | | | | |
| T.Masquerade_TOE | | | | | | | X | |
| T.Mem-Access | | | | X | | X | | X |

The content is available in the complete Security Target documentation.

### 8.2.2 Organizational security policies

#### 8.2.2.1 Summary

The following organizational security policies coming from the composite ST are related to the platform:

- P.Sensitive_Data,

- P.Personalisation,
- P.Terminal.

The following organizational security policies of the platform are relevant for the TOE:
- P.Process-TOE,
- P.Add-Functions,
- P.Crypto-Service.

#### 8.2.2.2 Rationale

Mapping of the platform organizational security policies to the composite ST organizational security policies is provided in Table 8.5.

**Table 8.5: Organizational security policies mappings**

| **Platform ST OSP** | **Composite ST OSP** | P.Sensitive_Data | P.Personalisation | P.Terminal |
|---|---|---|---|---|
| P.Process-TOE | | | X | |
| P.Add-Functions | | X | | X |
| P.Crypto-Service | | X | X | X |

The content is available in the complete Security Target documentation.

### 8.2.3 Assumptions

#### 8.2.3.1 Summary

The following platform assumptions are relevant for the TOE:
- A.Process-Sec-IC,
- A.Resp-Appl,
- A.Key-Function.

#### 8.2.3.2 Rationale

The content is available in the complete Security Target documentation.

### 8.2.4 Security objectives of the TOE

#### 8.2.4.1 Summary

The following security objectives of the TOE are related to the platform:
- 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.Sens_Data_Conf,
- OT.Chip_Auth_Proof.

The following security objectives of the platform contribute to security objectives of the TOE:

- O.TDES,
- O.AES,
- O.Add-Functions,
- O.Mem-Access,
- O.Malfunction,
- O.Phys-Manipulation,
- O.Phys-Probing,
- O.Leak-Inherent,
- O.Leak-Forced,
- O.Abuse-Func,
- O.Identification,
- O.RND.

#### 8.2.4.2 Rationale

Mapping between security objectives of the platform and security objectives of the TOE is given in Table 8.6.

**Table 8.6: Mapping security objectives of the platform and of the TOE**

| Platform ST SO | Composite ST 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.Malfunction | OT.Identification | OT.AC_Pers | OT.Sens_Data_Conf | OT.Chip_Auth_Proof |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.TDES | | X | X | X | | | | | | | | | |
| O.AES | | X | X | X | | | | | | | | | |
| O.Add-Functions | | | | | | | | | | | | X | X |
| O.Mem-Access | | | | | | | | | | | X | X | |
| O.Malfunction | | | | | | | | | X | | | | |
| O.Phys-Manipulation | | | | | | | | X | | | | | |
| O.Phys-Probing | | | | | | | | X | | | | | |
| O.Leak-Inherent | | | | | | | X | | | | | | |
| O.Leak-Forced | | | | | | | X | | | | | | |
| O.Abuse-Func | | | | | | X | | | | | | | |
| O.Identification | | | | | X | | | | | X | | | |
| O.RND | | X | X | X | | | | | | | | X | X |

### 8.2.5 Security objectives of the operational environment

#### 8.2.5.1 Summary

The following security objectives of the operational environment coming from the composite ST are related to the platform:

- OE.Personalization,
- OE.Auth_Key_Travel_Document,
- OE.Authoriz_Sens_Data.

The following security objectives of the operational environment coming from ST of the platform are relevant for the TOE:

- OE.TOE_Auth,
- OE.Resp-Appl.

#### 8.2.5.2 Rationale

Mapping between security objectives of the platform operational environment and security objectives of the TOE operational environment is given in Table 8.7.

**Table 8.7: Mappings of security objectives for the operational environment**

| **Platform ST Operational Environment** | **Composite ST Operational Environment** | OE.Personalization | OE.Authoriz_Sens_Data | OE.Prot_Logical_Travel_Document |
|---|---|---|---|---|
| OE.TOE_Auth | | X | | |
| OE.Resp-Appl | | X | X | X |

The content is available in the complete Security Target documentation.

# Annex A Cryptographic Disclaimer

## A.1 Supported mechanisms, protocols and algorithms

Table A.1 presents the cryptographic mechanisms supported by the TOE and lists all cryptographic algorithms used by those mechanisms.

**Table A.1: Cryptographic functionality**

| | Purpose | Cryptographic mechanism | Standard of implementation | Key size in Bits | Standard of Application | Comments |
|---|---|---|---|---|---|---|
| 1 | Key Agreement / Authentication | PACEv2 (Generic Mapping), PACE-CAM (Chip Authentication Mapping), PACE common: ECDH, ECDH key generation, Nonce Encryption, Authentication token | [TR03110-1], [TR03110-3], [Doc9303], [TR03111] (sec. 4.3.2.1), [IEEE1363], [RFC5639], [FIPS186-4], [ANSI X9.63] | [MRZ] = 160 [Nonce] = 128 Brainpool EC: 224, 256, 320, 384, 512 NIST EC: 224, 256, 384, 521 3DES session key: 112 AES session keys: 128, 192, 256 | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs: - FCS_CKM.1/DH_PACE, - FCS_COP.1/PACE_ENC, - FIA_UAU.1/PACE, - FIA_UAU.5/PACE, - FIA_AFL.1/PACE<br><br>IC crypto library used for: - ECDH, - ECDH key generation |
| 2 | Key Agreement / Authentication | Chip Authentication v1<br><br>ECDH, ECDH key generation | [TR03110-1], [Doc9303], [TR03111] (sec. 4.3.2.1), [IEEE1363], [RFC5639], [FIPS186-4], [ANSI X9.63] | 224, 256, 320, 384, 512, 521 | [Doc9303], [TR03110-1] | Related SFRs: - FCS_CKM.1/CA, - FCS_CKM.1/CAPK, - FIA_UAU.5/PACE, - FIA_UAU.6/EAC, - FIA_API.1<br><br>IC crypto library used for: - ECDH, - ECDH key generation |
| 3 | Authentication | Terminal Authentication v1 (signature verification)<br><br>ECDSA using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | [TR03110-1], [TR03110-3], [Doc9303], [ISO15946-1], [ISO15946-2], [RFC5639], [FIPS186-4], [ANSI X9.62]<br><br>also see line 15 | 224, 256, 320, 384, 512, 521 | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs: - FCS_COP.1/SIG_VER, - FIA_UAU.5/PACE<br><br>IC crypto library used for: - ECDSA |
| 4 | Authentication | Personalization Agent authentication using AES-256 in CBC mode | see line 14 | PA key: 256 | N/A | Related SFRs: - FIA_UAU.4/PACE, - FMT_SMR.1/PACE, - FMT_MTD.1/INI_DIS, - FMT_MTD.1/KEY_READ, - FMT_MTD.1/PA, - FMT_MTD.1/CVCA_INI, - FMT_MTD.1/CAPK<br><br>Proprietary implementation |
| 5 | Confidentiality | 3DES in CBC mode for Secure Messaging | [TR03110-1], [TR03110-3], [Doc9303], [ISO10116]<br><br>also see line 13 | 112 | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs: - FCS_COP.1/PACE_ENC, - FCS_COP.1/CA_ENC, - FDP_UCT.1/TRM |
| 6 | Confidentiality | AES in CBC mode for Secure Messaging | [TR03110-1], [TR03110-3], [Doc9303], [ISO10116]<br><br>also see line 14 | 128, 192, 256 | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs: - FCS_COP.1/PACE_ENC, - FCS_COP.1/CA_ENC, - FDP_UCT.1/TRM |
| 7 | Integrity | 3DES in Retail-MAC mode for Secure Messaging | [TR03110-1], [TR03110-3], [Doc9303],<br><br>also see line 13 and 16 | 112 | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs: - FCS_COP.1/PACE_MAC, - FCS_COP.1/CA_MAC, - FDP_UIT.1/TRM<br><br>The first steps (C1…Cn) represent the DES with 56 Bits in CBC mode cipher. The last two steps (finalization of the Retail-MAC token and signature using 3DES) correspond to 3DES with 112 Bits of security in CBC mode. |
| 8 | Integrity | CMAC-AES for Secure Messaging | [TR03110-1], [TR03110-3], [Doc9303],<br><br>also see line 14 | 128, 192, 256 | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs: - FCS_COP.1/PACE_MAC, - FCS_COP.1/CA_MAC, - FDP_UIT.1/TRM |
| 9 | Key Derivation | PACE, Chip Authentication v1, Key derivation using | [TR03110-1], [TR03110-3], [Doc9303], | 3DES: 112<br><br>AES: 128, 192, 256 | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs: - FCS_CKM.1/DH_PACE, - FCS_CKM.1/CA |

| | Purpose | Cryptographic mechanism | Standard of implementation | Key size in Bits | Standard of Application | Comments |
|---|---|---|---|---|---|---|
| | | SHA-1 and SHA-256 | [TR03111]<br><br>also see line 15 | | | |
| 10 | Trusted Channel | Secure Messaging in ENC and MAC modes (PACE) | [TR03110-1], [TR03110-3], [Doc9303] | N/A | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs:<br>- FTP_ITC.1/PACE,<br>- FDP_UCT.1/TRM,<br>- FDP_UIT.1/TRM |
| 11 | Trusted Channel | Secure Messaging in ENC and MAC modes (CA after PACE) | [TR03110-1], [TR03110-3], [Doc9303] | N/A | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs:<br>- FCS_CKM.1/CA<br>- FDP_UCT.1/TRM,<br>- FDP_UIT.1/TRM |
| 12 | Cryptographic Primitive | Hybrid Physical True Random Number Generator (PTG.3, DRG.3) | [AIS20/AIS31] | N/A | [TR03110-1], [TR03110-3], [Doc9303] | Related SFRs:<br>- FCS_RND.1<br><br>IC platform used for:<br>- HRNG |
| 13 | Cryptographic Primitive | 3DES in modes: ECB, CBC, CBC-MAC, CBC-MAC-ELB. | [NIST800-67], [ISO18033-3], [NIST800-38A], [NIST800-67], [ISO9797-1] | 112 | [TR03110-1], [TR03110-3], [Doc9303] | Symmetric Cryptographic Processor is used for:<br>- 3DES in mode ECB |
| 14 | Cryptographic Primitive | AES in modes: ECB, CBC, CBC-MAC, CBC-MAC-ELB | [FIPS197], [ISO18033-3], [NIST800-38A], [NIST800-38B] [ISO9797-1] | 128, 192, 256 | [TR03110-1], [TR03110-3], [Doc9303] | Symmetric Cryptographic Processor is used for:<br>- AES in mode CBC |
| 15 | Cryptographic Primitive | SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | [FIPS180-4] | N/A | [TR03110-1], [TR03110-3], [Doc9303] | Proprietary implementation. |
| 16 | Cryptographic Primitive | DES in CBC mode | [FIPS46-3] | 56 | [TR03110-1], [TR03110-3], [Doc9303] | Symmetric Cryptographic Processor is used for:<br>- DES in mode CBC<br><br>This primitive is only used during computation of the Retail-MAC authentication token. |

## A.2 Supported elliptic curves

The TOE supports the following elliptic curves:

- NIST P-224 (secp224r1) [FIPS186-4],
- BrainpoolP224r1 [RFC5639],
- NIST P-256 (secp256r1) [FIPS186-4],
- BrainpoolP256r1 [RFC5639],
- BrainpoolP320r1 [RFC5639],
- NIST P-384 (secp384r1) [FIPS186-4],
- BrainpoolP384r1 [RFC5639],
- BrainpoolP512r1 [RFC5639],
- NIST P-521 (secp521r1) [FIPS186-4].

# Annex B Bibliography

## B.1 Common Criteria documents

[CC-Part1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2017-04-001; Version 3.1, Revision 5, April 2017

[CC-Part2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2017-04-002; Version 3.1, Revision 5, April 2017

[CC-Part3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements; CCMB-2017-04-003; Version 3.1, Revision 5, April 2017

[CC-CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004; Version 3.1, Revision 5, April 2017

[CC-Smartcard] Common Criteria – Supporting Document Guidance – Smartcard Evaluation, CCDB-2010-03-001, Version 2.0, February 2010

## B.2 Protection profiles

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

[PP-EAC] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP-0056-V2-2012, version 1.3.2, 5th December 2012

[PP-IC] Security IC Platform Protection Profile with Augmentation Packages; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0084-2014, Version 1.0, January 2014

[PP-PACE] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, Version 1.1, 22nd July 2014

## B.3 Travel document specifications

[Doc9303] [Doc9303-P9], [Doc9303-P10], [Doc9303-P11] or [Doc9303-P12]

[Doc9303-P9] ICAO Doc 9303: Machine Readable Travel Documents – Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs, 7th edition, 2015

[Doc9303-P10] ICAO Doc 9303: Machine Readable Travel Documents – Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), 7th edition 2015

[Doc9303-P11] ICAO Doc 9303: Machine Readable Travel Documents – Part 11: Security Mechanisms for MRTDs, 7th edition 2015

[Doc9303-P12] ICAO Doc 9303: Machine Readable Travel Documents – Part 12: Public Key Infrastructure for MRTDs, 7th edition 2015

[TR03110-1] BSI Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1: eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015

[TR03110-3] BSI Technical Guideline TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, Version 2.21, 21 December 2016

## B.4 Hardware documentation

[IC_CR] Certification Report. BSI-DSZ-CC-1110-V5-2022 for Infineon Security Controller IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_000014h, IFX_000015h, IFX_00001Ch, IFX_00001Dh, IFX_000021h IFX_000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions

[IC_ST] Common Criteria Public Security Target – EAL6 Augmented / EAL6+. IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_000014h, IFX_000015h, IFX_00001Ch, IFX_00001Dh, IFX_000021h IFX_000022h. H13. Resistance to attackers with HIGH attack potential. Rev. 2.0. 2022-03-28

## B.5 Cryptographic standards

[AIS20/AIS31] Wolfgang Killmann (T-Systems GEI GmbH), Werner Schindler (BSI), A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011

[ANSI X9.62] Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005

[ANSI X9.63] Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography, November 20, 2001

[FIPS46-3] Federal Information Processing Standards Publication 46-3: Data Encryption Standard (DES). 25th October 1999

[FIPS180-4] Federal Information Processing Standards Publication 180-4: Secure Hash Standard (SHS), National Institute of Standards and Technology. March 2012

[FIPS186-4] Federal Information Processing Standards Publication 186-4: Digital Signature Standard. July 2013

[FIPS197] Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES), U.S. Department of Commerce / National Institute of Standards and Technology, November 26th 2001

[IEEE1363] IEEE 1363-2000: IEEE Standard Specifications for Public-Key Cryptography, 2002-08-06

[ISO9797-1] ISO/IEC 9797-1:2011: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher

[ISO10116] ISO/IEC 10116:2017: Information Technology – Security Techniques – Modes of operation for an n-bit block cipher

[ISO18033-3] ISO/IEC 18033-3:2010: Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers

[ISO15946-1] ISO/IEC 15946-1:2016: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General

[ISO15946-2] ISO/IEC 15946-2:2002: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures

[ISO15946-3] ISO/IEC 15946-3:2002 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment

[NIST800-38A] NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation Methods and Techniques, National Institute of Standards and Technology, December 2001

[NIST800-38B] NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation – The CMAC Mode for Authentication, U.S. Department of Commerce / National Institute of Standards and Technology, May 2005

[NIST800-67] NIST Special Publication 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, National Institute of Standards and Technology, Version 1.2, Revised July 2011

[PKCS#3] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, 1 November 1993

[RFC5639] Elliptic Curve Cryptography (ECC) Brainpool Standard curves and Curve Generation. March 2010

[TR03111] BSI Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 28.06.2012

## B.6 Other

[ISO7816-2] ISO/IEC 7816-2:2007: Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimensions and location of the contacts

# Annex C Acronyms

## C.1 Organizations

| | |
|---|---|
| ANSSI | Agence Nationale de la Sécurité des Systèmes d'Information |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| IFX | Infineon Technologies |
| PWPW | Polska Wytwórnia Papierów Wartościowych S.A. |

## C.2 Terms

| | |
|---|---|
| AS | application software |
| BAC | Basic Access Control |
| BIS | basic inspection system |
| BIS-BAC | basic inspection system with BAC |
| BIS-PACE | basic inspection system with PACE |
| BS | basic software |
| CA | chip authentication |
| CAD | card acceptance device |
| CC | common criteria |
| CSCA | country signing certification authority |
| CVCA | country verifying certification authority |
| DS | document signer |
| DV | document verifier |
| EAL | evaluation assurance level |
| EIS | extended inspection system |
| ES | embedded software |
| IC | integrated circuit |
| IS | inspection system |
| OSP | organization security policy |
| PACE | password authenticated connection establishment |
| PP | protection profile |
| SAR | security assurance requirements |
| SO | security objectives |
| $SO_D$ | document security object |
| ST | security target |
| TA | terminal authentication |

| | |
|---|---|
| TOE | target of evaluation |
| TSF | TOE security function |

# Annex D Glossary

## D.1 Security evaluation terms

*Application Note*

Optional informative part of the protection profile containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

*Common Criteria*

A set of rules and procedures for evaluating the security properties of a product.

*Evaluation Assurance Level*

A set of assurance requirements for a product, its manufacturing process and its security evaluation specified by Common Criteria.

*Protection Profile*

A document specifying security requirements for a class of products that conforms in structure and content to rules specified by Common Criteria.

*Security Target*

A document specifying security requirements for a particular product that conforms in structure and content to rules specified by Common Criteria, which may be based on one or more protection profiles.

*Target of Evaluation*

Abstract reference in a document, such as a protection profile, for a particular product that meets specific security requirements.

*Target of Evaluation Security Functions*

Functions implemented by the TOE to meet the requirements specified for it in a protection profile or security target.

*TSF Data*

Data created by and for the TOE, that might affect the operation of the TOE.

*User Data*

Data created by and for the user, that does not affect the operation of the TSF.

## D.2 Smartcard terms

*Integrated Circuit*

Electronic component(s) designed to perform processing and/or memory functions (i.e. the hardware component containing the micro-controller and IC dedicated software).

A typical IC comprises: a processing unit, security components, I/O ports and volatile and non-volatile memories. It also includes any IC designer/manufacturer proprietary IC dedicated software, required for testing purposes. This IC dedicated software may be either IC embedded software (also known as IC firmware) or security-relevant parts of tests programs outside the IC. The IC may include any IC pre-personalization data.

*IC Dedicated Software*

IC proprietary software embedded in a smartcard IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purposes (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services.

*IC Dedicated Test Software*

That part of the IC Dedicated Software (refer to above) which is used to test the device but which does not provide functionality during Phases 4 to 7.

Phases of the smartcard life-cycle are described in [CC-Smartcard], figure 4.

*IC Dedicated Support Software*

That part of the IC Dedicated Software (refer to above) which provides functions in Phases 4 to 7. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

Phases of the smartcard life-cycle are described in [CC-Smartcard], figure 4.

*Identification Data*

Any data defined by the Integrated Circuit manufacturer and injected into the nonvolatile memory by the Integrated Circuit manufacturer (Phase 3). These data are for instance used for traceability.

Phases of the smartcard life-cycle are described in [CC-Smartcard], figure 4.

*Basic Software*

Smartcard embedded software in charge of generic functions of the Smartcard IC, such as an operating system, general routines and interpreters.

*Application Software*

Smartcard embedded software (may be in ROM or loaded onto a platform in EEPROM or Flash Memory). This is software dedicated to the applications.

*Embedded Software*

Software embedded in a smartcard IC but not developed by the IC Designer. This comprises embedded software in charge of generic functions of the Smartcard IC, such as an operating system, general routines and interpreters (Smartcard Basic Software - BS) and embedded software dedicated to applications (Smartcard Application Software - AS). The Smartcard Embedded Software is designed in Phase 1 and embedded into the Smartcard IC in Phase 3 or in later phases of the smartcard product life-cycle.

Phases of the smartcard life-cycle are described in [CC-Smartcard], figure 4.

*Smartcard Personalization*

Final process under the responsibility of the card issuer, through which a smartcard is to be configured, security parameters loaded and secret keys set. At the end of the personalization process, the smartcard is irreversibly set into "user mode". Hence, it becomes fully operational and can be delivered to the end user.

*IC Platform*

Usually refers to a smartcard component which may undergo an evaluation process, as a complete Target of Evaluation (TOE) in itself, but which is not an end-user product (i.e. a smartcard component without any Application Software loaded).

*IC Initialization*

Process of writing Initialization Data to the IC.

*IC Initialization Data*

Any data defined by the IC Manufacturer and injected into the non-volatile memory during the manufacturing process. These data are for instance used for traceability and for IC identification.

*IC Pre-personalization*

Process performed at the IC manufacturer site, through which customer data can be loaded onto the IC, prior to the IC being irreversibly set into "issuer mode".

*IC Pre-personalization Data*

Any data supplied by the software developer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.

Phases of the smartcard life-cycle are described in [CC-Smartcard], figure 4.

*Smartcard Product*

A product corresponds to a fully operational smartcard, composed of both IC and complete ES, including application software as appropriate.

*IC Developer*

The entity which develops the integrated circuit, the IC Dedicated Software (firmware) and the guidance documentation.

*IC Manufacturer*

Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.

*ES Developer or AS Developer*

Institution (or its agent) responsible for the smartcard Embedded Software or Application Software development and the specification of IC pre-personalization requirements.

*Card Manufacturer*

The customer of the IC Manufacturer who receives the TOE during TOE Delivery. The Card Manufacturer includes all roles after TOE Delivery up to Phase 7. The Card Manufacturer has the following roles: (i) the Smartcard Product Manufacturer (Phase 5); (ii) the Personalizer (Phase 6). If the TOE is delivered after Phase 3 in the form of wafers or sawn wafers (dice) he also assumes the role of the IC Packaging Manufacturer (Phase 4). Usually, the Card Manufacturer is also the ES or AS developer.

Phases of the smartcard life-cycle are described in [CC-Smartcard], figure 4.

*Card Issuer*

Customer for a product who is in charge of the issuance of the product to the smartcard holders (end users).

## D.3 Travel documents terms

*Manufacturer*

Generic term for the IC Manufacturer producing integrated circuit and the travel document manufacturer completing the IC to the travel document.

*Personalization*

The process by which the Personalization Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the enrolment.

*Personalization Agent*

An organization acting on behalf of the travel document issuer to personalize the travel document for the travel document holder by some or all of the following activities:

1. establishing the identity of the travel document holder for the biographic data in the travel document,
2. enrolling the biometric reference data of the travel document holder,
3. writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder,

4. writing the document details data,
5. writing the initial TSF data,
6. signing the Document Security Object (in the role of DS).

*Personalization Data*

A set of data which includes:
1. individual-related data (biographic and biometric data) of the travel document holder,
2. dedicated document details data, and
3. dedicated initial TSF data (including the Document Security Object).

*Country Signing Certification Authority*

An organization enforcing the policy of the travel document issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer certificates within this PKI.

*Document Signer*

An organization enforcing the policy of the CSCA and signing the document security object stored (carrying hashes of LDS data groups) on the travel document for passive authentication.

*Country Verifying Certification Authority*

An organization enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA link-certificates.

*Document Verifier*

An organization enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organization / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorized by at least the national CVCA to issue certificates for national terminals.

*Inspection System*

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

*Issuing State*

The country issuing the travel document.

*Issuing Organization*

Organization authorized to issue an official travel document.

*Receiving State*

The country to which the traveler is applying for entry.

*Basic Inspection System*

An inspection system which implements the terminals part of the Basic Access Control mechanism and authenticates itself to the travel document's chip using the document basic access keys derived from the printed MRZ data for reading the logical travel document.

*Basic Inspection System with BAC*

Another name of Basic Inspection System.

*Basic Inspection System with PACE*

An inspection system which implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) for reading the logical travel document.

*Extended Inspection System*

A role of a terminal as part of an Inspection System which is in addition to Basic Inspection System authorized by the Issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control authentication mechanism.

*Card Access Number*

Password derived from a short number printed on the front side of the data page.

# Annex E Revision history

| VERSION | CHANGES |
|---|---|
| 1.0.0.0 | Initial version |
| 1.0.1.0 | This document was created based on *PWPW SmartApp-MRTD: Security Target* documentation v1.0.12.0, selected parts were removed and are only available in a base document. |
| 1.0.2.0 | TOE HW Certification ID in Table 1.1, [IC_CR] and [IC_ST] references were updated. |
| 1.0.3.0 | TOE life cycle description was updated. |