MASKTECH

Security Target

COMMON CRITERIA DOCUMENTS | Version 1.1

MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121)

Machine Readable Travel Document with "ICAO Application",
Extended Access Control with PACE

Certification-ID: BSI-DSZ-CC-1147

Public Version

MaskTech International GmbH | Nordostpark 45 | Nuernberg | www.masktech.com | +49 (0)911 95 51 49-0

Contents

1 ST Introduction (ASE_INT.1)

1.1 ST Reference and TOE Reference

Title	Security Target – Machine Readable Travel Document with “ICAO Application”, MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121)
Version	1.1, 2020-10-12
Editors	Gudrun Schürer
Compliant to	Common Criteria Protection Profile - ’Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP)’
CC Version	3.1 (Revision 5)
Assurance Level	The assurance level for this ST is EAL5 augmented
TOE name	MTCOS Pro 2.5 EAC with PACE / P71D352 (N7121) , operation system for secure passports
TOE Hardware	NXP Semiconductors Germany GmbH, P71D352 (N7121), dual interface Smartcard IC
TOE version	MTCOS Pro 2.5
Keywords	ICAO, Machine Readable Travel Document, Extended Access Control, PACE, Supplemental Access Control (SAC)

1.2 TOE Overview

This security target defines the security objectives and requirements for the contactless-chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Password Authenticated Connection Establishment, Extended Access Control, and Chip Authentication similar to the Active Authentication in ’ICAO Doc 9303’ [ICAO_9303].

MTCOS Pro is a fully interoperable multi-application smart card operating system compliant to ISO/IEC 7816 [ISO_7816]. It provides public and secret key cryptography and supports also other applications like e-purses, health insurance cards and access control.

The operating system software is implemented on the P71D352 (N7121) secure dual-interface controller of NXP Semiconductors Germany GmbH (BSI-DSZ-CC-1040-2019

[NXP_P71_ST]). Chip and cryptographic library are certified according to CC EAL6 augmented compliant to the Protection Profile BSI-CC-PP-0084-2014 [CC_PP-0084]). The TOE consists of software and hardware.

1.2.1 TOE Definition and Operational Usage

The Target of Evaluation (TOE) is an electronic travel document representing a contactless smart card programmed according to ICAO Technical Report "Supplemental Access Control" [ICAO_SAC] (which means amongst others according to the Logical Data Structure (LDS) defined in [ICAO_9303]) and additionally providing the Extended Access Control according to the 'ICAO 9303' [ICAO_9303] and [BSI_TR-03110-1], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 [CC_PP-0068-V2]. Additionally, Active Authentication according to [ICAO_9303] is provided.

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 (operating system),
- the *epassport application* and
- the associated guidance documentation [AGD, MT_Manual]

1.2.2 TOE Major Security Features for Operational Use

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 [ICAO_9303] for 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

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

1. the biographical data on the biographical data page of the travel document surface,

2. the printed data in the Machine Readable Zone (MRZ) and
3. the printed portrait.

the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO_9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the travel document holder

1. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
2. the digitized portraits (EF.DG2),
3. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1],
4. the other data according to LDS (EF.DG5 to EF.DG16) and
5. the Document Security Object (SOD).

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) [ICAO_9303]. These security measures can include the binding of the travel document's chip to the travel document.

The logical travel document is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or 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 Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [ICAO_9303] and Password Authenticated Connection Establishment [ICAO_SAC]. 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 Version 1 described in [BSI_TR-03110-1] as an alternative to the Active Authentication stated in [ICAO_9303].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by BSI-CC-PP-0056-V2 [CC_PP-0056-V2] as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfill the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control' BSI-CC-PP-0055 [CC_PP-0055]. Due to the fact that [CC_PP-0055] does

[1]These biometric reference data are optional according to [ICAO_9303]. This ST assumes that the issuing State or Organization uses this option and protects these data by means of extended access control.

only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately. The evaluation and certification process is carried out contemporaneous to the current process as a re-certification.

If BAC is supported by the TOE, the travel document has to be evaluated and certified separately. This is due to the fact that [CC_PP-0055] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

Note 1: Basic Access Control is addressed in procedure BSI-DSZ-CC-1148.

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)' [CC_PP-0068-V2]. Note that [CC_PP-0068-V2] considers high attack potential.

For the PACE protocol according to [ICAO_SAC], 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-Hellman key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
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) [BSI_TR-03110-1, ICAO_SAC].

The security target requires the TOE to implement Active Authentication described in [ICAO_9303]. This protocol provides evidence of the travel document's chip authenticity.

The security target requires the TOE to implement the Extended Access Control as defined in [BSI_TR-03110-1]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1). The Chip Authentication Protocol v.1 (i) authenticates the 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 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.

Note 2: In addition, the TOE supports PACE ***Chip Authentication Mapping*** (PACE-CAM) according to [ICAO_SAC]. If PACE-CAM is performed, Terminal Authentication can be performed

without explicit Chip Authentication beforehand. The secure messaging established by the PACE protocol is preserved to protect the data transmission from the TOE to the inspection system.

1.2.3 TOE Life Cycle

The TOE life cycle is described in terms of the four life cycle phases (with respect to [CC_PP-0084], the TOE life cycle is additionally subdivided into 7 steps).

Phase 1 Development

Step 1 The TOE is developed in phase 1. NXP Semiconductors Germany GmbH develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

Step 2 MaskTech International GmbH uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the ePassport application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to NXP Semiconductors Germany GmbH. The IC Embedded Software in the non-volatile programmable memories, the ePassport application and the guidance documentation is securely delivered to the travel document manufacturer.

Phase 2 Manufacturing

Step 3 In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and conditionally the parts of the travel document's chip Embedded Software in the non-volatile non-programmable memories (FLASH). NXP Semiconductors Germany GmbH writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.

Conditionally, NXP Semiconductors Germany GmbH adds the parts of the IC Embedded Software in the non-volatile programmable memories (FLASH) and deactivates the Flash Loader permanently. The IC is securely delivered from NXP Semiconductors Germany GmbH to the travel document manufacturer.

Alternatively, MaskTech International GmbH in the role of the *Manufacturer* writes the Embedded Software in the non-volatile non-programmable memories (FLASH) of the chip and deactivates the Flash Loader permanently.

Step 4 (optional) The travel document manufacturer combines the IC with hardware for the contactlessinterface in the travel document unless the travel document consists of the card only.

Note 3: The inlay production including the application of the antenna is NOT part of the TOE and takes part after the delivery.

Step 5 The travel document manufacturer (i) adds the IC Embedded Software or part of it in the non-volatile programmable memories if necessary, (ii) creates the ePassport application (creation of MF and ICAO.DF), and (iii) equips travel document's chips with pre-personalization Data.

Note 4: The role of the *Manufacturer* performing initialization and pre-personalization in the *Card Issuing* phase is taken over by MaskTech International GmbH, Linxens (Thailand) Co Ltd. (see [SC_Linxens]), HID Global Ireland Teoranta (see [SC_HID]), HID Global Malaysia (see [SC_HID_MY]) and NXP Semiconductors Germany GmbH (see [NXP_P71_ST]).

Note 5: In the case of NXP Semiconductors Germany GmbH being the *Manufacturer* performing initialization and pre-personalization, the deactivation of the Flash Loader can also be performed after the initialization/pre-personalization step.

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

Phase 3 Personalization of the travel document

Step 6 The personalization of the travel document includes (i) the survey of the travel document holder's biographical data, (ii) the enrollment 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 [ICAO_9303] 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.

Phase 4 Operational Use

Step 7 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.

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

1.2.4 Non-TOE Hardware/Software/Firmware Required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and

the booklet (holding the printed MRZ) are needed to represent a complete travel document, nevertheless these parts are not inevitable for the secure operation of the TOE.

2 Conformance Claims (ASE_CCL.1)

2.1 CC Conformance Claim

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 Components; CCMB-2017-04-003, Version 3.1 Revision 5, April 2017 [CC_Part3]

as follows

- Part 2 extended
- Part 3 conformant

The

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

has to be taken into account.

2.2 PP Reference

The conformance of this ST to the Common Criteria Protection Profile - 'Machine Readable Travel Document with 'ICAO Application', Extended Access Control with PACE (EAC PP)', BSI-CC-PP-0056-V2-2012 [CC_PP-0056-V2] is claimed.

2.3 Package Claim

The assurance level for the TOE is CC EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC_Part3].

2.4 Conformance Rationale

According section 2.2 this ST claims conformance to [CC_PP-0056-V2] and thus implicitly to [CC_PP-0068-V2]. All items from [CC_PP-0068-V2] that are just referenced in [CC_PP-0056-V2] have been included explicitly in this ST. “Application notes” included in the PP are only resumed, if they are of interest for the reader. In this case they are renamed to “Note” and renumbered consecutively.

In addition to the functionality described in [CC_PP-0056-V2] the TOE provides Active Authentication (AA) and PACE *Chip Authentication Mapping* (PACE-CAM) implying several extensions. These and all other deviations of this ST in comparison to [CC_PP-0056-V2] are listed in Table 2.1 below. None of the changes causes a conflict between ST and PP.

Assurance Component	Description
ASE_INT.1 (see sec. 1)	The TOE is described in detail in compliance to the PP. AA and PACE-CAM are introduced as additional features. A number of *Manufacturers* performing initialization and pre-personalization is included.
ASE_CCL.1 (see sec. 2)	Conformance to CC Parts version 3.1 revision 5 (PP: revision 3) and assurance package EAL5+ (PP: EAL4+) is claimed.
ASE_SPD.1 (see sec. 3)	The inclusion of AA and PACE-CAM causes an extension of • A.Insp_Sys (AA, PACE-CAM) • P.Sensitive_Data (PACE-CAM)
ASE_OBJ.2 (see sec. 4)	The inclusion of AA and PACE-CAM causes the addition of • OT.Active_Auth_Proof (AA) • OE.Active_Auth_Key_Travel_Document (AA) and the extension of • OT.Chip_Auth_Proof (PACE-CAM) • OE.Auth_Key_Travel_Document (PACE-CAM) • OE.Exam_Travel_Document (PACE-CAM)
ASE_ECD.1 (see sec. 5)	This component has not been resumed, but the reference to the according chapter of [CC_PP-0056-V2] is given.

Assurance Component	Description
ASE_REQ.2 (see sec. 6)	The inclusion of AA and PACE-CAM causes the addition of • FCS_COP.1/AA (AA) • FIA_API.1/AA (AA) • FMT_MTD.1/AAPK (AA) • FMT_MTD.1/KEY_READ_AA (AA) • FMT_MTD.1/KEY_READ_PACE_CAM (PACE-CAM) and the extension of • FIA_UID.1/PACE (PACE-CAM) • FIA_UAU.1/PACE (PACE-CAM) • FIA_UAU.5/PACE (PACE-CAM) • FPT_EMS.1 (PACE-CAM) Furthermore, • FCS_RND.1 has been changed according to [CC_PP-0084] (FCS_RNG.1) to meet [BSI_AIS31]

Table 2.1: Conformance claim rationale.

3 Security Problem Definition (ASE_SPD.1)

3.1 Introduction

Assets

The assets to be protected by the TOE include the User Data on the travel document's chip, User Data transferred between the TOE and the terminal, and travel document tracing data defined in PACE PP [CC_PP-0068-V2] (primary assets):

User data stored on the TOE (object no. 1 in [CC_PP-0068-V2]) All data (being not authentication data) stored in the context of the *ePassport* application of the travel document as defined in [ICAO_SAC] and being allowed to be *read out* solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_SAC]).

This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [CC_PP-0055].

User data transferred between the TOE and the terminal connected (object no. 2) All data (being not authentication data) being transferred in the context of the *ePassport* application of the travel document as defined in [ICAO_SAC] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_SAC]).

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

Travel document tracing data (object no. 3) Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided/gathered.

Logical travel document sensitive User Data Sensitive biometric reference data (EF.DG3, EF.DG4)

Note 6: Due to interoperability reasons the 'ICAO Doc 9303' [ICAO_9303] 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 [ICAO_9303]. Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [CC_PP-0055]). 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.

A sensitive asset is the following more general one.

Authenticity of the travel document's chip The authenticity of the travel document's chip personalized by the issuing State or Organization for the travel document holder is used by the traveler to prove his possession of a genuine travel document.

Due to strict conformance to PACE PP, this ST also includes the secondary assets defined in [CC_PP-0068-V2]:

Accessibility to the TOE functions and data only for authorized subjects (object no. 4) Property of the TOE to restrict access to TSF and TSF data stored in the TOE to authorized subjects only.

Genuineness of the TOE (object no. 5) Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD's chip' in [CC_PP-0055].

TOE internal secret cryptographic keys (object no. 6) Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

TOE internal non-secret cryptographic material (object no. 7) Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality.

Travel document communication establishment authorization data (object no. 8) Restricted revealable authorization information for a human user being used for verification of the authorization attempts as authorized user (PACE password). These data are stored in the TOE and are not to be send to it.

Subjects and external entities

This security target considers the following external entities and subjects as defined in PACE PP [CC_PP-0068-V2]:

Travel document holder (subject no. 1 in [CC_PP-0068-V2]) A person for whom the travel document Issuer has personalized the travel document[1].

This entity is commensurate with 'MRTD Holder' in [CC_PP-0055]. Please note that a travel document holder can also be an attacker (s. below).

Travel document presenter (traveler) A person presenting the travel document to a terminal [2] and claiming the identity of the travel document holder.

This external entity is commensurate with 'Traveler' in [CC_PP-0055]. Please note that a travel document presenter can also be an attacker (s. below).

[1] i.e. this person is uniquely associated with a concrete electronic Passport
[2] in the sense of [ICAO_SAC]

Terminal (subject no. 2) A terminal is any technical system communicating with the TOE through the contactless/contact interface. (see below)

The role 'Terminal' is the default role for any terminal being recognized by the TOE as not PACE authenticated ('Terminal' is used by the travel document presenter).

This entity is commensurate with 'Terminal' in [CC_PP-0055].

Basic Inspection System with PACE (BIS-PACE) (subject no. 3) A technical system being used by an inspecting authority[3] verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). (see below 'Inspection System')

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

Document Signer (DS) An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication.

A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [ICAO_9303].

This role is usually delegated to a Personalization Agent.

Country Signing Certification Authority (CSCA) 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 document and creates the Document Signer Certificates within this PKI.

The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [ICAO_9303], 5.5.1.

Personalization Agent (subject no. 4) 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: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [ICAO_9303], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO_9303] (in the role of DS). Please note that the role '*Personalization Agent*' may be distributed among several institutions according to the operational policy of the travel document Issuer.

This entity is commensurate with '*Personalization Agent*' in [CC_PP-0055].

Manufacturer (subject no. 5) Generic term for the IC *Manufacturer* producing integrated circuit and the travel document *Manufacturer* completing the IC to the travel document. The *Manufacturer* is the default user of the TOE during the *Manufacturing* life cycle phase. The TOE itself does not distinguish between the IC *Manufacturer* and travel document *Manufacturer* using this role *Manufacturer*.

[3] concretely, by a control officer

This entity is commensurate with '*Manufacturer*' in [CC_PP-0055].

Attacker A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by PACE PP, especially to change properties of the assets having to be maintained. (see below)

The attacker is assumed to possess an at most high attack potential.

Please note that the attacker might 'capture' any subject role recognized by the TOE.

This external entity is commensurate with 'Attacker' in [CC_PP-0055].

The following subjects additionally to those defined in PACE PP [CC_PP-0068-V2] are considered:

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

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

Terminal A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface. (see above)

Inspection system (IS) 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. (see above 'Basic Inspection System with PACE')

The Extended Inspection System (EIS) performs the Advanced Inspection Procedure (see figure 1 in [CC_PP-0056-V2]) and therefore (i) contains a terminal for the communication with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information. (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [BSI_TR-03110-1] and (v) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used. Optionally all the Inspection Systems can implement Active Authentication and PACE *Chip Authentication Mapping* (PACE-CAM).

Attacker Additionally to the definition above, the definition of an attacker is refined as followed: A threat agent trying (i) to manipulate the logical travel document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine travel document, or (iv) to trace a travel document. (see above)

3.2 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

A.Insp_Sys (Inspection Systems for global interoperability)

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [ICAO_SAC] and/or BAC [CC_PP-0055]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. If PACE *Chip Authentication Mapping* is used, Chip Authentication v.1 may be skipped. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. Optionally all the Inspection Systems can implement Active Authentication.

Justification:

The assumption A.Insp_Sys does not confine the security objectives of the [CC_PP-0068-V2] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality of the TOE.

A.Auth_PKI (PKI for Inspection Systems)

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

Justification:

This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [CC_PP-0068-V2] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

This ST includes the assumption from the PACE PP [CC_PP-0068-V2]:

A.Passive_Auth (PKI for Passive Authentication)

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical

travel document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations. It is assumed that the Personalization Agent ensures that the Document Security Object contains only the hash values of genuine User Data according to [ICAO_9303].

3.3 Threats

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

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

T.Read_Sensitive_Data (Read the sensitive biometric reference data)

Adverse action An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip.

The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (see below) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

Threat agent Having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document.

Asset Confidentiality of logical travel document sensitive User Data (i.e. biometric reference).

T.Counterfeit (Counterfeit of travel document chip data)

Adverse action An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveler by possession of a travel document.

The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

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

Asset authenticity of User Data stored on the TOE

This ST includes all threats from the PACE PP [CC_PP-0068-V2]:

T.Skimming (Skimming travel document / capturing card-terminal communication)

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

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

Asset Confidentiality of logical travel document data.

T.Eavesdropping (Eavesdropping on the communication between the TOE and the PACE terminal)

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

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

Asset Confidentiality of logical travel document data.

T.Tracing (Tracing travel document)

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

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

Asset Privacy of the travel document holder

Note 7: This Threat completely covers and extends "T.Chip-ID" from [CC_PP-0055].

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 Inspection System 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.

Note 8: T.Forgery from the PACE PP [CC_PP-0068-V2] is extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

T.Abuse-Func (Abuse of functionality)

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

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

Asset Integrity and authenticity of the travel document, availability of the functionality of the travel document

Note 9: Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage (Information leakage from travel document)

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

Threat agent Having high attack potential.

Asset Confidentiality of User Data and TSF data of the travel document.

Note 10: Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Phys-Tamper (Physical tampering)

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

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

Asset Integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF data of the travel document.

Note 11: 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.

T.Malfunction (Malfunction due to environmental stress)

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

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

Asset Integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF data of the travel document.

Note 12: 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.

3.4 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2).

P.Sensitive_Data (Privacy of sensitive biometric reference data)

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

even during transmission to the Extended Inspection System after Chip Authentication Version 1 or PACE *Chip Authentication Mapping*, respectively.

P.Personalization (Personalization of the travel document by issuing State or Organization only)

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

This ST includes all OSPs from the PACE PP [CC_PP-0068-V2]:

P.Manufact (Manufacturing of the travel document's chip)

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

P.Pre-Operational (Pre-operational handling of the travel document)

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

P.Card_PKI (PKI for Passive Authentication (issuing branch))

Note 13: The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

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

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

P.Trustworthy_PKI (Trustworthiness of PKI)

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

P.Terminal (Abilities and trustworthiness of terminals)

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

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

[4] This order is commensurate with [ICAO_SAC].

4 Security Objectives (ASE_OBJ.2)

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

4.1 Security Objectives for the TOE

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

OT.Sens_Data_Conf (Confidentiality of sensitive biometric reference data)

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

OT.Chip_Auth_Proof (Proof of the travel document's chip authenticity)

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organization by means of the Chip Authentication Version 1 as defined in [BSI_TR-03110-1] and by means of PACE *Chip Authentication Mapping* as defined in [ICAO_SAC, BSI_TR-03110-1]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Note 14: 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.

- In the case of Chip Authentication v.1: 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 [ICAO_9303] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

- In the case of PACE *Chip Authentication Mapping*: a certificate for the Public Key that matches the PACE-CAM Private Key of the travel document's chip. This certificate is provided by (i) the Public Key (EF.CardSecurity) in the LDS defined in [ICAO_SAC] and (ii) the hash value of EF.CardSecurity in the Document Security Object signed by the Document Signer.

OT.Active_Auth_Proof (Proof of travel document's chip authenticity)

The TOE shall support the Basic Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO_9303]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

This ST includes all Security Objectives for the TOE from the PACE PP [CC_PP-0068-V2]:

OT.Data_Integrity (Integrity of data)

The TOE must ensure integrity of the User Data and the TSF data stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized modifying).

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

OT.Data_Authenticity (Authenticity of data)

The TOE must ensure authenticity of the User Data and the TSF data stored on it by enabling verification of their authenticity at the terminal-side[1].

The TOE must ensure authenticity of the User Data and the TSF data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[2].

OT.Data_Confidentiality (Confidentiality of data)

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

OT.Tracing (Tracing travel document)

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

[1] verification of SO_D

[2] secure messaging after the PACE authentication, see also [ICAO_SAC].

OT.Prot_Abuse-Func (Protection against abuse of functionality)

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

OT.Prot_Inf_Leak (Protection against information leakage)

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

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE

Note 15: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Phys-Tamper (Protection against physical tampering)

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

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

with a prior

- reverse-engineering to understand the design and its properties and functionality.

OT.Prot_Malfunction (Protection against malfunctions)

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

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

OT.Identification (Identification of the TOE)

The TOE must provide means to store Initialization[3] and Pre-Personalization Data in its non-volatile memory. The Initialization Data must provide a unique identification

[3] amongst other, IC Identification data

of the IC during the *Manufacturing* and the *Card Issuing* life cycle phases of the travel document. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).

OT.AC_Pers (Access Control for personalization of logical MRTD)

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

4.2 Security Objectives for Operational Environment

Issuing State or Organization

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

OE.Auth_Key_Travel_Document (Travel document Authentication Key)

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

Justification:

This security objective for the operational environment is needed additionally to those from [CC_PP-0068-V2] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in EAC PP and not in [CC_PP-0068-V2].

OE.Authoriz_Sens_Data (Authorization for Use of Sensitive Biometric Reference Data)

The issuing State or Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of travel document holders to authorized receiving States or Organizations. The Country Verifying Certification Authority of the issuing State or Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

Justification:

This security objective for the operational environment is needed additionally to those from [CC_PP-0068-V2] in order to handle the Threat T.Read_Sensitive_Data, the Organizational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in EAC PP and not in [CC_PP-0068-V2].

OE.Active_Auth_Key_Travel_Document (Travel document Active Authentication Key)

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

Receiving State or Organization

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

OE.Exam_Travel_Document (Examination of the physical part of the travel document)

The inspection system of the receiving State or Organization must examine the travel document presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of PACE [ICAO_SAC] and/or the Basic Access Control [ICAO_9303]. Extended Inspection Systems perform additionally to these points PACE *Chip Authentication Mapping* or/and the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

Justification:

This security objective for the operational environment is needed additionally to those from [CC_PP-0068-V2] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [CC_PP-0068-V2] and therefore also counters T.Forgery and A.Passive_Auth from [CC_PP-0068-V2]. This is done because a new type of Inspection System is introduced in EAC PP as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

OE.Prot_Logical_Travel_Document (Protection of data from the logical travel document)

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

Justification:

This security objective for the operational environment is needed additionally to those from [CC_PP-0068-V2] in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

OE.Ext_Insp_Systems (Authorization of Extended Inspection Systems)

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

Justification:

This security objective for the operational environment is needed additionally to those from [CC_PP-0068-V2] in order to handle the Threat T.Read_Sensitive_Data, the Organizational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

This ST includes all Security Objectives of the TOE environment from the PACE PP [CC_PP-0068-V2]:

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

OE.Legislative_Compliance (Issuing of the travel document)

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

Travel document Issuer and CSCA: travel document's PKI (issuing) branch The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the *Note 13* above):

OE.Passive_Auth_Sign (Authentication of travel document by Signature)

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA

Public Key (C_{CSCA}). Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [ICAO_9303]. The *Personalization Agent* has to ensure that the Document Security Object contains only the hash values of genuine User Data according to [ICAO_9303]. The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

OE.Personalization (Personalization of travel document)

The travel document Issuer must ensure that the *Personalization Agents* acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enroll the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalization) and store them in the travel document (electronic personalization) for the travel document holder as defined in [ICAO_9303][4], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [ICAO_9303] (in the role of a DS).

Terminal operator: Terminal's receiving branch

OE.Terminal (Terminal operating)

The terminal operators must operate their terminals as follows:

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

[4] see also [ICAO_9303], sec. 10

[5] This order is commensurate with [ICAO_SAC]

Travel document holder Obligations

OE.Travel_Document_Holder (Travel document holder Obligations)

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

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage. Objectives, threats and assumptions marked in *italic letters* are taken from PACE-PP[CC_PP-0068-V2], those included for the Active Authentication functionality are underlined.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Tracing*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Identification*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfunction*	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Active_Auth_Key_Travel_Document	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	*OE.Personalization*	*OE.Passive_Auth_Sign*	*OE.Terminal*	*OE.Travel_Document_Holder*	*OE.Legislative_Compliance*
T.Read_Sensitive_Data	x														x				x					
T.Counterfeit		x	x											x		x	x							
T.Skimming					x	x	x																x	
T.Eavesdropping							x																	
T.Tracing								x															x	
T.Abuse-Func									x															
T.Information_Leakage										x														
T.Phys-Tamper												x												
T.Malfunction													x											
T.Forgery				x	x	x			x			x					x			x	x	x		
P.Sensitive_Data	x														x				x					
P.Personalization				x							x									x				
P.Manufact											x													
P.Pre-Operational				x							x									x				x
P.Terminal																	x					x		
P.Card_PKI																					x			
P.Trustworthy_PKI																					x			
A.Insp_Sys																	x	x						
A.Auth_PKI															x				x					
A.Passive_Auth																	x				x			

Table 4.1: Security Objective Rationale

A detailed justification required for *suitability* of the security objectives to coup with the security problem definition is given below.

The OSP **P.Personalization** “Personalization of the travel document by issuing State or Organization only” addresses the (i) the enrollment of the logical travel document by

the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of logical travel document", and (ii) the access control for the User Data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalization of logical travel document". Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

The OSP **P.Sensitive_Data** "Privacy of sensitive biometric reference data" is fulfilled and the threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the TOE-objective **OT.Sens_Data_Conf** "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems".

The OSP **P.Terminal** "Abilities and trustworthiness of terminals" is countered by the security objective **OE.Exam_Travel_Document** additionally to the security objectives from PACE PP [CC_PP-0068-V2]. **OE.Exam_Travel_Document** enforces the terminals to perform the terminal part of the PACE protocol.

The threat **T.Counterfeit** "Counterfeit of travel document chip data" addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing State or Organization. The Public Key has to be written into EF.DG14 or, for PACE *Chip Authentication Mapping*, to EF.CardSecurity and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** "Travel document Authentication Key". According to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" the General Inspection system has to perform PACE *Chip Authentication Mapping* or the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document's chip. Additionally, this attack is thwarted through the chip by an identification and authenticity proof required by **OT.Active_Auth_Proof** "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing State or Organization. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Active_Auth_Key_Travel_Document** "Travel document Active Authentication Key".

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

The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a rightful terminal in order to gain the User Data transferred there. This threat is countered by the security objective **OT.Data_Confidentiality** through a trusted channel based on the PACE authentication.

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

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

The threats **T.Information_Leakage**, **T.Phys-Tamper** and **T.Malfunction** are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is obviously addressed by the directly related security objectives **OT.Prot_Inf_Leak**, **OT.Prot_Phys-Tamper** and **OT.Prot_Malfunction**, respectively.

The threat **T.Forgery** "Forgery of data" addresses the fraudulent, complete or partial alteration of the User Data or/and TSF data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective OT.AC_Pers requires the TOE to limit the write access for the travel document to the trustworthy *Personalization Agent* (cf. **OE. Personalization**). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF data as aimed by the security objectives **OT.Data_Integrity** and **OT.Data_ Authenticity**, respectively. The objectives **OT.Prot_Phys-Tamper** and **OT.Prot_Abuse-Func** contribute to protecting integrity of the User Data or/and TSF data stored on the TOE. A terminal operator operating his terminals according to OE.Terminal and performing the Passive Authentication using the Document Security Object as aimed by **OE.Passive_Auth_Sign** will be able to effectively verify integrity and authenticity of the data received from the TOE. Additionally, the examination of the presented MRTD passport book according to **OE.Exam_ Travel_Document** "Examination of the physical part of the travel document" shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

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

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

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

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

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

The examination of the travel document addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" which requires the inspection system to examine physically the travel document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform PACE *Chip Authentication Mapping* or the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip. The security objectives for the TOE environment **OE.Prot_Logical_Travel_ Document** "Protection of data from the logical travel document" require the Inspection System to protect the logical travel document data during the transmission and the internal handling.

The assumption **A.Passive_Auth** "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment **OE.Passive_Auth_Sign** "Authentication of travel document by Signature" from PACE PP [CC_PP-0068-V2] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs (see below). The implementation of the signature verification procedures is covered by **OE.Exam_Travel_ Document** "Examination of the physical part of the travel document".

From PACE PP [CC_PP-0068-V2]: The assumption **A.Passive_Auth** "PKI for Passive Authentication" is directly addressed by **OE.Passive_Auth_Sign** requiring the travel document issuer to establish a PKI for Passive Authentication, generating Document Signing private keys only for rightful organizations and requiring the Document Signer to sign exclusively correct Document Security Objects to be stored on travel document.

The assumption **A.Auth_PKI** "PKI for Inspection Systems" is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data" requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organizations only. The Document Verifier of the receiving State is required by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organization has to establish the necessary public key infrastructure.

5 Extended Components Definition (ASE_ECD.1)

This Security Target uses the components defined in chapter 5 of [CC_PP-0056-V2]. The security requirement FCS_RND.1 has been changed according to the security requirement FCS_RNG.1 defined in [CC_PP-0084] to meet [BSI_AIS31]. No other components are used.

6 Security Requirements (ASE_REQ.2)

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 of the CC [CC_Part1]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word “refinement” in bold text and that added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP author are denoted as underlined text. Selections filled in by the ST author are denoted as double-underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP author are denoted by showing as underlined text. Assignments filled in by the ST author are denoted as double-underlined text.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [CC_Part2]. The operation “load” is synonymous to “import” used in [CC_Part2].

Definition of security attributes:

Security attribute	Values	Meaning
Terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [BSI_TR-03110-1]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [BSI_TR-03110-1]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [BSI_TR-03110-1]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [BSI_TR-03110-1]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [BSI_TR-03110-1])
	DG3 (Fingerprint)	Read access to DG3: (cf. [BSI_TR-03110-1])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [BSI_TR-03110-1])

The following table provides an overview of the keys and certificates used. Further keys and certificates are listed in [CC_PP-0068-V2].

Name	Data
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying	The TOE stores the Country Verifying Certification Authority

Name	Data
Certification Authority Public Key (PK_{CVCA})	Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [5] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [ISO_11770-3].
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the User Data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Active Authentication Public Key Pair	The Active Authentication Public Key Pair (SK_{AA}, PK_{AA}) are used for Active Authentication according to [ICAO_9303].
Active Authentication Public Key (PK_{AA})	The Active Authentication Public Key (PK_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical travel document and used by the inspection system for Active Authentication of the travel document's chip. It is part of the User Data provided by the TOE for the IT environment.
Active Authentication Private Key (SK_{AA})	The Active Authentication Private Key (SK_{AA}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

Name	Data
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organization with the Document Signer Public Key.
Chip Authentication Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.
PACE *Chip Authentication Mapping* Public Key Pair	The PACE *Chip Authentication Mapping* Public Key Pair (SK_{CAM}, PK_{CAM}) are used for PACE *Chip Authentication Mapping* according to [ICAO_SAC, BSI_TR-03110-1].
PACE *Chip Authentication Mapping* Public Key (PK_{CAM})	The PACE *Chip Authentication Mapping* Public Key (PK_{CAM}) is stored in the EF.CardSecurity of the TOE's logical travel document and used by the inspection system for PACE *Chip Authentication Mapping* of the travel document's chip. It is part of the User Data provided by the TOE for the IT environment.
PACE *Chip Authentication Mapping* Private Key (SK_{CAM})	The PACE *Chip Authentication Mapping* Private Key (SK_{CAM}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

6.1 Security Functional Requirements for the TOE

6.1.1 Class FCS Cryptographic Support

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

6.1.1.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1/CA	Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys
Hierarchical to:	No other components.

Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm DH and specified cryptographic key sizes 112, 128, 192 and 256 bits that meet the following: based on the Diffie-Hellman key derivation protocol compliant to [NIST_SP800-56A] and [BSI_TR-03110-1] **and** in accordance with a specified cryptographic key generation algorithm ECDH and specified cryptographic key sizes 112, 128, 192 and 256 bits that meet the following: based on the Diffie-Hellman key derivation protocol compliant to [NIST_SP800-56A] and [BSI_TR-03110-1], based on an ECDH protocol compliant to [BSI_TR-03111]

Note 16: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [BSI_TR-03110-1].

Note 17: The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [CC_PP-0068-V2] 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.

Note 18: If PACE *Chip Authentication Mapping* is performed, the Secure Messaging session established by the PACE protocol is sustained. In this case FCS_CKM.1/DH_PACE applies instead of FCS_CKM.1/CA.

FCS_CKM.1/DH_PACE	**Cryptographic key generation – Diffie-Hellman for PACE session keys**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [BSI_TR-03111] and specified cryptographic key sizes 112, 128, 192 and 256 bits that meet the following: [ICAO_SAC].

Note 19: The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO_SAC]. 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 [ICAO_SAC] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Note 20: FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO_SAC].

FCS_CKM.4	Cryptographic key destruction – Session keys
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with the cryptographic key destruction method physical deletion of key value that meets the following: [FIPS_140-3].

Note 21: The TOE shall destroy the PACE or BAC 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.

6.1.1.2 Cryptographic Operation (FCS_COP.1)

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

FCS_COP.1/CA_ENC	Cryptographic operation – Symmetric Encryption / Decryption
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_ENC	The TSF shall perform secure messaging - encryption and decryption in accordance with a specified cryptographic algorithm AES in CBC mode and cryptographic key sizes 128, 192 and 256 bits **and** 3DES in CBC mode and cryptographic key sizes 112 bits that meet the following: [FIPS_197], [NIST_SP800-67] and [ISO_10116].

Note 22: 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.

FCS_COP.1/SIG_VER	Cryptographic operation – Signature verification by travel document
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ECDSA with SHA-224, SHA-256, SHA-384 or SHA-512 and cryptographic key sizes BP(r1): 224, 256, 320, 384, 512 bits, NIST: 224, 256, 384, 521 bits that meet the following: [ANSI_X9-62], sec. 7, [FIPS_180-4], section 6, and [BSI_TR-03110-3] **and** in accordance with a specified cryptographic algorithm RSA with SHA-1 or SHA-256 and cryptographic key sizes 1536 - 4096 bits that meet the following: [FIPS_180-4], section 6 and [RFC_8017] .

FCS_COP.1/CA_MAC	Cryptographic operation – MAC
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_MAC	The TSF shall perform secure messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC-AES and cryptographic key sizes128, 192 and 256 bits **and** Retail-MAC and cryptographic key sizes 112 bit that meet the following: [FIPS_197], [NIST_SP800-67], [NIST_SP800-38B] Section 6, and [ISO_9797-1], sec. 7.4.

Note 23: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with 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.

FCS_COP.1/AA	Cryptographic operation – Signature creation by travel document – AA
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AA	The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 and cryptographic key sizes 1536 - 4096 bits that meet the following: [FIPS_180-4], section 6, [ISO_9796-2], sec. 8 **and** in accordance with a specified cryptographic algorithm ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 and cryptographic key sizes BP(r1): 224, 256, 320, 384, 512 bits, NIST: 224, 256, 384, 521 bits that meet the following: [BSI_TR-03111], sec. 4.2.1, [ANSI_X9-62], sec. 7, [FIPS_180-4], section 6

FCS_COP.1/PACE_ENC	**Cryptographic operation – Encryption / Decryption AES/3DES**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/PACE_ENC	The TSF shall perform Secure Messaging - encryption and decryption in accordance with the cryptographic algorithm AES in CBC mode and cryptographic key sizes 128, 192 and 256 bits **and** 3DES in CBC mode and cryptographic key sizes 112 bits that meet the following: **[FIPS_197], [NIST_SP800-67] and [ISO_10116], sec. 7** compliant to [ICAO_SAC].

Note 24: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data. 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}). Although not explicitly worded within the SFR, it also applies to the encryption of the nonce in the first step of PACE.

Infomative: This SFR also applies to the usage of AES in CBC mode and cryptographic key sizes 128, 192 and 256 bits for Symmetric Authentication used for *Personalization*.

FCS_COP.1/PACE_MAC	**Cryptographic operation – MAC**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_COP.1.1/PACE_MAC	The TSF shall perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC-AES and cryptographic key sizes 128 bit, 192 bit and 256 bit **and** Retail-MAC and cryptographic key sizes 112 bit that meet the following: **[FIPS_197], [NIST_SP800-67], [NIST_SP800-38B] Section 6, and [ISO_9797-1], sec. 7.4** compliant to [ICAO_SAC].

Note 25: 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}).

Infomative: This SFR also applies to the usage of CMAC-AES and cryptographic key size 128, 192 and 256 bits for Symmetric Authentication used for *Personalization*.

6.1.1.3 Random Number Generation (FCS_RND.1)

FCS_RND.1	**Random number generation (Class PTG.3)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.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 is 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 has 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 nontolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time. (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_RND.1.2	The TSF shall provide octets of bits 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 none.[1] (PTG.3.8) The internal random numbers shall use PTRNG of class PTG.2 as random source for the postprocessing.

Note 26: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocols (PACE) as required by FIA_UAU.4/PACE.

Note 27: This SFR has been changed according to [CC_PP-0084] (FCS_RNG.1), justified in [KiSch-RNG] chapter 3 (PTG.3) and [NIST_SP800-90A], sec. 10.2, 10.3.2 to meet [BSI_AIS31] and [BSI_TR-03116-2].

6.1.2 Class FIA Identification and Authentication

Table 6.1 provides an overview of the authentication mechanisms used.

Name	SFR for the TOE
Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE
Chip Authentication Protocol v.1	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE
Active Authentication (specified in addition [CC_PP-0056-V2])	FIA_API.1/AA

Table 6.1: Overview on authentication SFR

Note the Chip Authentication Protocol Version 1 as defined in this protection profile 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.

[1] See [KiSch-RNG] Section 2.4.4.

Note 28: If PACE *Chip Authentication Mapping* is used, the secure messaging keys established by the PACE protocol are sustained. A subsequent Terminal Authentication Protocol v.1 uses the PACE-CAM public key verified during the PACE protocol.

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

FIA_UID.1/PACE	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/PACE	The TSF shall allow 1. to establish the communication channel 2. carrying out the PACE Protocol according to [ICAO_SAC] 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 [BSI_TR-03110-1] 5. to carry out the Terminal Authentication Protocol v.1 according to [BSI_TR-03110-1] 6. to carry out the PACE *Chip Authentication Mapping* Protocol according to [ICAO_SAC] 7. 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.

Note 29: The SFR FIA_UID.1/PACE covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.

Note 30: 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).

Note 31: 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).

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

FIA_UAU.1/PACE	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1/PACE	The TSF shall allow 1. to establish the communication channel 2. carrying out the PACE Protocol according to [ICAO_SAC] 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 v.1 according to [BSI_TR-03110-1] 6. to carry out the Terminal Authentication Protocol v.1 according to [BSI_TR-03110-1] 7. to carry out the PACE *Chip Authentication Mapping* Protocol according to [ICAO_SAC] 8. 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.

Note 32: The SFR FIA_UAU.1/PACE in EAC PP covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.

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

FIA_UAU.4/PACE	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1/PACE	The TSF shall prevent reuse of authentication data related to 1. PACE Protocol according to [ICAO_SAC], 2. Authentication Mechanism based on Triple-DES **or** AES, 3. Terminal Authentication Protocol v.1 according to [BSI_TR-03110-1].

Note 33: The SFR FIA_UAU.4.1 covers the definition in PACE PP [CC_PP-0068-V2] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. 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 [CC_PP-0068-V2].

Note 34: 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.

Note 35: Authentication data related to PACE Protocol according to [ICAO_SAC] include authentication data related to PACE *Authentication Mapping*.

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

FIA_UAU.5/PACE	Multiple authentication mechanisms
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1/PACE	The TSF shall provide 1. PACE Protocol according to [ICAO_SAC], 2. Passive Authentication according to [ICAO_9303], 3. Secure messaging in MAC-ENC mode according to [ICAO_SAC], 4. Symmetric Authentication Mechanism based on Triple-DES **or** AES, 5. Terminal Authentication Protocol v.1 according to [BSI_TR-03110-1]. 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 Symmetric Authentication Mechanism with *Personalization Agent* Keys. 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 v.1. 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. If PACE *Chip Authentication Mapping* has been performed instead of Chip Authentication Protocol Version 1 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 PACE *Chip Authentication Mapping* and the secure messaging established by the PACE Protocol. 6. none

Note 36: The SFR FIA_UAU.5.1/PACE covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspects 2), 3), 4)and 5). These extensions do not conflict with the strict conformance to PACE PP.

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

FIA_UAU.6/PACE	**Re-authenticating – Re-authenticating of Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/PACE	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.

Note 37: The SFR FIA_UAU.6/PACE also includes PACE *Chip Authentication Mapping*.

FIA_UAU.6/EAC	Re-authenticating – Re-authenticating of Terminal by the TOE
Hierarchical to:	No other components.
Dependencies:	No dependencies.
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.

Note 38: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO_9303] 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.

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

FIA_API.1	Authentication Proof of Identity
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a Chip Authentication Protocol Version 1 according to [BSI_TR-03110-1] to prove the identity of the TOE.

Note 39: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [BSI_TR-03110-1]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO_9303]. 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).

The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1)” as specified below (Common Criteria Part 2 extended [CC_Part2]).

FIA_API.1/AA	Authentication Proof of Identity – AA
Hierarchical to:	No other components.

Dependencies:	No dependencies.
FIA_API.1.1/AA	The TSF shall provide an Active Authentication Mechanism according to [ICAO_9303] to prove the identity of the TOE.

FIA_AFL.1/PACE	**Authentication failure handling – PACE authentication using non-blocking authorization data**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1/PACE	The TSF shall detect when 1 unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password for PACE.
FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall wait for an administrator configurable time greater 10 seconds between the reception of the authentication command and its processing.

6.1.3 Class FDP User Data Protection

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

FDP_ACC.1/TRM	**Subset access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/TRM	The TSF shall enforce the Access Control SFP on terminals gaining access to the user data and data stored in EF.SOD of the logical travel document.

Note 40: The SFR FIA_ACC.1.1 covers the definition in PACE PP [CC_PP-0068-V2] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to PACE PP.

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

FDP_ACF.1/TRM	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/TRM

The TSF shall enforce the Access Control SFP to objects based on the following:

1. Subjects:
   (a) Terminal
   (b) BIS-PACE
   (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.
3. Security attributes:
   (a) PACE Authentication,
   (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: A BIS-PACE is allowed to read data objects from FDP_ACF.1/TRM according to [ICAO_SAC] 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

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 DG3 (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 DG4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) 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.

Note 41: The SFR FDP_ACF.1.1/TRM covers the definition in PACE PP [CC_PP-0068-V2] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM cover the definition in PACE PP [CC_PP-0068-V2]. The SFR FDP_ACF.1.4/TRM covers the definition in PACE PP [CC_PP-0068-V2] and extends it by 3) to 6). These extensions do not conflict with the strict conformance to PACE PP.

Note 42: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [BSI_TR-03110-1]. 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.

Note 43: 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).

FDP_RIP.1	**Subset residual information protection**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: 1. Session keys (immediately after closing related communication session), 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K)[2] 3. none

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

FDP_UCT.1/TRM	**Basic data exchange confidentiality – MRTD**
Hierarchical to:	No other components.

[2] according to [ICAO_SAC]

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

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

FDP_UIT.1/TRM	**Data exchange integrity**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]: fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/TRM
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

FTP_ITC.1/PACE	**Inter-TSF trusted channel after PACE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal.

6.1.5 Class FAU Security Audit

FAU_SAS.1	Audit storage
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer with the capability to store the Initialization and Pre-personalization Data in the audit records.

Note 44: 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.

6.1.6 Class FMT Security Management

Note 45: The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data.

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

FMT_SMR.1/PACE	Security roles
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1/PACE	The TSF shall maintain the roles: 1. Manufacturer, 2. Personalization Agent, 3. Terminal, 4. PACE authenticated BIS-PACE, 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

Note 46: The SFR FMT_SMR.1.1/PACE in EAC PP covers the definition in PACE PP [CC_PP-0068-V2] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

FMT_SMF.1	**Specification of Management Functions**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Pre-personalization, 3. Personalization, 4. Configuration.

Note 47: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below (Common Criteria Part 2 extended).

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with ’Limited availability (FMT_LIM.2)’ the following policy is enforced: Deploying test features after TOE delivery do not allow 1. User data to be manipulated and disclosed, 2. TSF data to be disclosed or manipulated, 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.

The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below (Common Criteria Part 2 extended).

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced: Deploying test features after TOE delivery 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.

Note 48: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

FMT_MTD.1/CVCA_INI	Management of TSF data – Initialization of CVCA Certificate and Current Date
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
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 Verifier Certification Authority Certificate, 3. Initial Current Date, 4. none. to the Personalization Agent

FMT_MTD.1/CVCA_UPD	Management of TSF data – Country Verifier Certification Authority
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_UPD	The TSF shall restrict the ability to update the 1. Country Verifying Certification Authority Public Key, 2. Country Verifier Certification Authority Certificate, to Country Verifier Certification Authority

Note 49: 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. [BSI_TR-03110-1]). 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. [BSI_TR-03110-1]).

FMT_MTD.1/DATE	**Management of TSF data – Current date**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
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.

Note 50: The authorized roles are identified in their certificate (cf. [BSI_TR-03110-1]) 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 [BSI_TR-03110-1]).

FMT_MTD.1/CAPK	**Management of TSF data – Chip Authentication Private Key**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/CAPK	The TSF shall restrict the ability to create **and** load the Chip Authentication Private Key to the Personalization Agent

Note 51: 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.

FMT_MTD.1/AAPK	**Management of TSF data – Active Authentication Private Key – AA**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MTD.1.1/AAPK	The TSF shall restrict the ability to create **and** load the Active Authentication Private Key to the Personalization Agent

Note 52: The verb "load" means here that the Active Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb "create" means here that the Active Authentication Private Key is generated by the TOE itself.

FMT_MTD.1/KEY_READ	**Management of TSF data – Key Read**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
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.

Note 53: The SFR FMT_MTD.1/KEY_READ in EAC PP covers the definition in PACE PP [CC_PP-0068-V2] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.

FMT_MTD.1/ KEY_READ_AA	**Management of TSF data – Key Read – AA**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ_AA	The TSF shall restrict the ability to read the Active Authentication Private Key to none

FMT_MTD.1/ KEY_READ_PACE_CAM	**Management of TSF data – Key Read – PACE *Chip Authentication Mapping***
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ_PACE_CAM	The TSF shall restrict the ability to read the PACE *Chip Authentication Mapping* Private Key to none

The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below (Common Criteria Part 2):

FMT_MTD.3	Secure TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of 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.

Note 54: 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.

FMT_MTD.1/INI_ENA	Management of TSF data – Writing Initialization and Pre-personalization Data
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
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
Hierarchical to:	No other components.

Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to read out the Initialization Data and the Pre-personalization Data to Personalization Agent

FMT_MTD.1/PA	**Management of TSF data – Personalization Agent**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/PA	The TSF shall restrict the ability to write to the Document Security Object (SO_D) to the Personalization Agent

6.1.7 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for the user data and TSF data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of the TOE security functionality.

The TOE shall meet the requirement “TOE Emanation (FPT_EMS.1)” as specified below (Common Criteria Part 2 extended):

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_EMS.1.1	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information 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. Manufacturer Authentication Key, 5. Administration keys, 6. Personalization Agent Keys, 7. Chip Authentication Private Key, 8. Active Authentication Private Keys, 9. PACE *Chip Authentication Mapping* Private Keys.
FPT_EMS.1.2	The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to 1. Chip Authentication Session Keys, 2. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. Manufacturer Authentication Key, 5. Administration keys, 6. Personalization Agent Keys, 7. Chip Authentication Private Key, 8. Active Authentication Private Keys, 9. PACE *Chip Authentication Mapping* Private Keys.

Note 55: The SFR FPT_EMS.1.1 covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in EAC PP covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspects 4) and 5). Active Authentication is taken into account in aspect 9 of FPT_EMS.1.1 and FPT_EMS.1.2. These extensions do not conflict with the strict conformance to PACE PP.

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

FPT_FLS.1	**Failure with preservation of secure state**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions causing a TOE malfunction, 2. Failure detected by TSF according to FPT_TST.1, 3. none

FPT_TST.1	**TSF testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up and at the condition 'request of random numbers' 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.

FPT_PHP.3	**Resistance to physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

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

6.2 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level EAL5 and augmented by taking the following components:

- ALC_DVS.2 (Sufficiency of security measures) and
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The table 6.2 provides The following table provides an overview for security functional requirements coverage. SFRs and security objectives from PACE PP [CC_PP-0068-V2] are marked in *italic letters*, SFRs from PACE PP [CC_PP-0068-V2] which are extended in EAC PP [CC_PP-0056-V2] are marked in **bold letters**. SFRs and security objectives included in addition for key pair generation, Active Authentication and PACE *Chip Authentication Mapping* are underlined.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Identification*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Tracing*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfunction*
FAU_SAS.1				x				x					
FCS_CKM.1/DH_PACE					x	x	x						
FCS_CKM.1/CA	x	x		x	x	x	x						
FCS_CKM.4	x			x	x	x	x						
FCS_COP.1/PACE_ENC							x						
FCS_COP.1/CA_ENC	x	x		x	x		x						
FCS_COP.1/PACE_MAC					x	x							
FCS_COP.1/CA_MAC	x	x		x	x								
FCS_COP.1/SIG_VER	x			x									
FCS_COP.1/AA			x										
FCS_RND.1	x			x	x	x	x						
FIA_AFL.1/PACE											x		
FIA_UID.1/PACE	x			x	x	x	x						
FIA_UAU.1/PACE	x			x	x	x	x						
FIA_UAU.4/PACE	x			x	x	x	x						
FIA_UAU.5/PACE	x			x	x	x	x						
FIA_UAU.6/PACE					x	x	x						
FIA_UAU.6/EAC	x			x	x	x	x						
FIA_API.1		x											
FIA_API.1/AA			x										
FDP_ACC.1/TRM	x			x	x		x						
FDP_ACF.1/TRM	x			x	x		x						
FDP_RIP.1					x	x	x						
FDP_UCT.1/TRM	x				x		x						
FDP_UIT.1/TRM					x		x						

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Identification*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Tracing*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfunction*
FMT_SMF.1		x		x	x	x	x	x					
FMT_SMR.1/PACE		x		x	x	x	x	x					
FMT_LIM.1									x				
FMT_LIM.2									x				
FMT_MTD.1/INI_ENA				x				x					
FMT_MTD.1/INI_DIS				x				x					
FMT_MTD.1/CVCA_INI	x												
FMT_MTD.1/CVCA_UPD	x												
FMT_MTD.1/DATE	x												
FMT_MTD.1/CAPK	x	x			x								
FMT_MTD.1/AAPK			x										
FMT_MTD.1/PA				x	x	x	x						
FMT_MTD.1/KEY_READ	x	x		x	x	x	x						
FMT_MTD.1/KEY_READ_AA			x										
FMT_MTD.1/KEY_READ_PACE_CAM		x											
FMT_MTD.3	x												
FPT_EMS.1				x						x			
FPT_TST.1										x			x
FPT_FLS.1										x			x
FPT_PHP.3					x					x		x	
FTP_ITC.1/PACE					x	x	x				x		

Table 6.2: Coverage of Security Objectives for the TOE by SFR

The security objective **OT.Identification** “Identification of the TOE” addresses the storage of Initialization and Pre-Personalization Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE’s chip. This will be ensured by TSF according to SFR FAU_SAS.1. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalization Agent to disable access to Initialization and Pre-personalization Data in the life cycle phase ’operational use’.

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

The security objective **OT.AC_Pers** “Access Control for Personalization of logical travel document” addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalization Data. The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE,

FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SO_D and, in generally, personalization data). The SFR FMT_SMR.1/PACE lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The SFRs FMT_MTD.1/KEY_READ and FPT_EMS.1 restrict the access to the Personalization Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalization Terminal wants to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/ CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication). If the Personalization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The security objective **OT.Data_Integrity** “Integrity of personal data” requires the TOE to protect the integrity of the logical travel document stored on the travel document’s chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D containing signature over the user data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered as trustworthy. The Personalization Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorized modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/ PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_ UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/ PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).

The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/ TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_ CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself.

This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).

FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key.

FMT_MTD.1/PA requires that SO_D containing signature over the user data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered as trustworthy.

The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

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

The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged.

This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/ TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/ TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for K_{enc}). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the user data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered trustworthy.

The SFR FCS_RND.1 represents the general support for cryptographic operations needed.

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

The security objective **OT.Sens_Data_Conf** "Confidentiality of sensitive biometric reference data" is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER.

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 or PACE *Chip Authentication Mapping* before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/ KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

The security objective **OT.Chip_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 proving the identity of the TOE or by or PACE *Chip Authentication Mapping*. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/ CAPK and FMT_MTD.1/KEY_READ resp. FMT_MTD.1/KEY_READ_PACE_CAM. The Chip Authentication Protocol v.1 [BSI_TR-03110-1] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).

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

The security objective **OT.Active_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Active Authentication Protocol provided by FIA_ API.1/AA proving the identity of the TOE. The Active Authentication Protocol defined by FIA_API.1/AA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ_AA. The Active Authentication Protocol [ICAO_9303] requires additional TSF according to FCS_COP.1/AA.

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

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

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).

This objective is achieved as follows:(i) while establishing PACE communication with CAN or MRZ (non-blocking authorization data) – by FIA_AFL.1/PACE; (ii) for listening to PACE communication (is of importance for the current PP, since SO_D is card-individual) – FTP_ITC.1/PACE.

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

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

6.3.2 Dependency Rationale

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

Table 6.3 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1/ DH_PACE	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation],	justification 1 for non-satisfied dependencies
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/CA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation],	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC,
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_CKM.4 from [CC_PP-0068-V2]	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1/DH_PACE and FCS_CKM.1/CA
FCS_COP.1/ PACE_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by FCS_CKM.1/DH_PACE,
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by FCS_CKM.1/CA,
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/ PACE_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by FCS_CKM.1/DH_PACE
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by FCS_CKM.1/CA
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/ SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by FCS_CKM.1/CA,
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/AA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	justification 2 for non-satisfied dependencies

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

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/ CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/ CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/ KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/ KEY_READ_AA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/ KEY_READ_ PACE_CAM	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD

SFR	Dependencies	Support of the Dependencies
FPT_EMS.1	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FTP_ITC.1/PACE	No dependencies	n.a.

Table 6.3: Dependencies between the SFR for the TOE

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

No. 1 A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

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

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

6.3.3 Security Assurance Requirements Rationale

The selection of assurance components is based on the underlying PP [CC_PP-0056-V2]. This Security Target uses the same augmentations as the PP, but chooses a higher assurance level. The level EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL5 is applicable in those circumstances where developers or users require a very high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs. Additionally, the requirement of the PP [CC_PP-0056-V2] to choose at least EAL4 is fulfilled.

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

The selection of the component ATE_DPT.2 as augmentation from the PP is made obsolete by the selection of EAL5 because the component ATE_DPT.3 as part of EAL5 already exceeds ATE_DPT.2.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an at-

tacker possessing a high attack potential. This vulnerability analysis is necessary to fulfill the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 has the following dependencies:

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

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The analysis of the TOE's security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in section 6.3.2 'Dependency Rationale for the security functional requirements' shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. This is also true for the augmentations defined in Table 2.1. All dependencies between the chosen functional components are analyzed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behavior of these 'shared' items.

The assurance class EAL5 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 'Security Assurance Requirements Rationale' shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.3.2 'Rationale for SFR's Dependencies' and 6.3.3 'Security Assurance Requirements Rationale'. Furthermore, as also discussed in section 6.3.3 'Security Assurance Requirements Rationale', the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specification (ASE_TSS.1)

This chapter describes the TOE security functions and the assurance measures covering the requirements of the previous chapter.

7.1 TOE Security Functions

This chapter gives the overview description of the different TOE Security Functions composing the TSF.

7.1.1 TOE Security Functions from Hardware (IC) and Cryptographic Library

7.1.1.1 F.IC_CL: Security Functions of the Hardware (IC) and Cryptographic Library

This security function covers the security functions of the hardware and the cryptographic library. The Security Target of the hardware [NXP_P71_ST] defines the following security functionalities, which are grouped in TSF portions:

TSF portion	Used by TOE	
TSF.Service	x	Service functionality beside cryptographic operations
		Functionality:
	x	TOE identification
	–	Trusted channel for usage of the Flash Loader (optional)
	x	Self-test functionality
	x	Hardware RNG following PTG.2
	–	Hybrid-deterministic RNG following DRG.4
	x	Hybrid-physical RNG following PTG.3
TSF.Protection	x	General security measures to protect the TSF
		Functionality:
	x	Integrity protection of memories

TSF portion	Used by TOE	
	x	Protection against physical manipulations
	x	Logical protection
	–	Flash Loader data confidentiality and integrity protection (optional)
	x	Cryptographic coprocessors and cryptographic library
	x	Protection of the general purpose I/O interface against misuse
TSF.Control	x	Operating conditions, memory and hardware access control
		Functionality:
	x	Control of operating conditions
	x	Mode control
	x	Access control to memories
	x	Access control to special function registers
	x	Secure User Mode Box firewall
	–	Access control to Flash Loader functionality
TSF.Crypto	x	Crypto Service
		Functionality:
	x	Hardware support for Triple-DES encryption/decryption
	x	Library support for Triple-DES encryption/decryption (optional)
	x	Hardware support for AES encryption/decryption
	x	Library support for AES encryption/decryption (optional)
	–	PUF functionality
	x	Library support for RSA (optional)
	x	Library support for ECC (optional)
	x	Library support for hashing (optional)

Table 7.1: Security functionality provided by the hardware and cryptographic library.

7.1.2 TOE Security Functions from Embedded Software (ES) – Operating system

7.1.2.1 F.Access_Control

This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. This function consists of following elements:

1. Access to objects is controlled based on subjects, objects (any file) and security attributes.
2. No access control policy allows reading of any key.
3. Any access not explicitly allowed is denied.

4. Access Control in the **manufacturing** phase (phase 2): Configuration and initialization of the TOE, configuring of Access Control policy and doing key management only by the *Manufacturer* or on behalf of him (see F.Management).
5. Access Control in the **personalization** phase (phase 3): Personalization including the writing of user and dedicated TSF data and reading of initialization data only by the *Personalization Agent* identified with its authentication key (see F.Management).
6. Access Control in **operational use** phase (phase 4): Reading of user data (except DG3 and DG4) only by a PACE Terminal (PCT) after a successful PACE authentication and using Secure Messaging; reading of optional biometrics (EF.DG3, EF.DG4) by authenticated and authorized EIS.

7.1.2.2 F.Identification_Authentication

This function provides identification/authentication of the user roles

- Manufacturer (Initialization/Pre-personalization Agent)
- Personalization Agent
- Terminal (for BAC authentication mechanism)
- PACE Terminal (PCT)
- Country Verifier Certification Authority
- Document Verifier
- Extended Inspection System (domestic/foreign)

by the methods:

1. **Personalization** phase:
   - Symmetric authentication [FIPS_197, NIST_SP800-38B] with following properties:
     - It uses a challenge from the TOE.
     - The cryptographic method for confidentiality is AES-128/CBC provided by F.Crypto and F.IC_CL.
     - The cryptographic method for authenticity is CMAC provided by F.Crypto and F.IC_CL.
     - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
     - After three consecutive failed authentication attempts the authentication method is blocked and the key is no longer usable (retry counter with a value of 3). Upon a successful authentication, the retry counter is reset to three unless the key is blocked.
     - A usage counter of 50.000 prevents the unlimited usage of the key. The counter cannot be reset. After the limit is reached, the key is irreversibly blocked.
     - On success the session keys are created and stored for Secure Messaging.
     - Keys and data in transient memory are overwritten after usage.
   - Secure Messaging with following properties:
     - The cryptographic method for confidentiality is AES-128/CBC provided by F.Crypto and F.IC_CL.

  - The cryptographic method for authenticity is CMAC provided by F.Crypto.
  - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
  - The initialization vector is an encrypted Send Sequence Counter (SSC) for encryption and MAC.
  - A session key is used.
  - The Secure Messaging session is limited by a Secure Messaging counter of 500.000; the decrease of the counter is depending on the length of the command and response APDUs. If a new Secure Messaging session is started, the counter is reset to 500.000.
  - Upon any command that is not protected correctly with the session keys these are overwritten according to FIPS 140-3 [FIPS_140-3] (or better) and a new authentication is required.
  - Keys and data in transient memory are overwritten after usage.

2. **Operational use** phase:
   - PACE authentication method [BSI_TR-03110-1] with following properties:
     - It uses an MRZ or a Card Access Number.
     - The cryptographic method for confidentiality is AES/CBC or 3DES/CBC provided by F.Crypto and F.IC_CL.
     - The cryptographic method for authenticity is CMAC or Retail-MAC provided by F.Crypto.
     - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
     - On success the session keys are created and stored for Secure Messaging.
     - Keys and data in transient memory are overwritten after usage.
   - Secure Messaging with following properties:
     - The cryptographic method for confidentiality is AES/CBC or 3DES/CBC provided by F.Crypto and F.IC_CL.
     - The cryptographic method for authenticity is CMAC for Retail-MAC provided by F.Crypto.
     - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
     - The Secure Messaging session is limited by a Secure Messaging counter of 500.000; the decrease of the counter is depending on the length of the command and response APDUs. If a new Secure Messaging session is started, the counter is reset to 500.000.
     - The initialization vector is a zero-IV for 3DES encryption and an encrypted Send Sequence Counter (SSC) for AES encryption and CMAC and Retail-MAC.
     - A session key is used.
     - On any command that is not protected correctly with the session keys these are overwritten according to FIPS 140-3 [FIPS_140-3] (or better) and a new PACE authentication is required.
     - Keys and data in transient memory are overwritten after usage.
     - PACE *Chip Authentication Mapping* can optionally be used to authenticate the chip.
3. Active Authentication with following properties:
   - According to [ICAO_9303] using RSA or ECDSA from F.IC_CL.

4. Chip Authentication with following properties:
   - According to TR-03110 [BSI_TR-03110-1] using DH or ECDH from F.IC_CL.
   - A usage counter of 50.000 prevents the unlimited usage of the key. After the limit is reached, the key is irreversibly blocked.
   - Session keys are created and stored for Secure Messaging replacing existing session keys.
   - The Secure Messaging session is limited by a Secure Messaging counter of 500.000; the decrease of the counter is depending on the length of the command and response APDUs. If a new Secure Messaging session is started, the counter is reset to 500.000.
   - Keys and data in transient memory are overwritten after usage.
5. Terminal Authentication with following properties:
   - According to TR03110 [BSI_TR-03110-1] checking certificates with RSA or ECDSA from F.IC_CL.
   - It uses a challenge from the MRTD.
   - Usable only in a Secure Messaging session with Chip Authentication key or after PACE *Chip Authentication Mapping* with Secure Messaging established by the PACE protocol.
   - It distinguishes between the roles:
     - Country Verifier Certification Authority.
     - Domestic and foreign Document Verifier.
     - Domestic and foreign Extended Inspection System.
   - Update of CVCA certificate is allowed for CVCA.
   - Update of current date is allowed for CVCA, domestic and foreign Document Verifier and domestic Extended Inspection System.
   - Only with a public key from an IS certificate the challenge-response authentication itself is performed.
   - The bitwise AND of the Certificate Holder Authorizations of a certificate chain is used for Terminal Authorization.
   - Verifying validity of certificate chain:
     - Certificates must be in the sequence: known CVCA [> CVCA...] > DV > IS.
     - Expiration dates must not be before the current date with the exception of CVCA.

7.1.2.3 F.Management

In phase 2 the Manufacturer (Initialization/Pre-personalization Agent) performs the initialization and configures the file layout including security attributes. In any case the layout determines that the parameters given in F.Access_Control for phases 3 and 4 are enforced. The agent can also do key management and other administrative tasks.

In phase 3 the Personalization Agent performs the following steps:

- Formatting of all data to be stored in the TOE.
- Writing of all the required data to the appropriate files.
- Changing the TOE into the end-usage mode for phase 4 where reading of the initialization data is prevented.

7.1.2.4 F.Crypto

This function provides the implementation or, if the functionality of the cryptographic library (F.IC_CL) is used, the high level interface to

- DES (supplied by F.IC_CL)
- AES (supplied by F.IC_CL)
- CMAC
- 3DES/CBC (supplied by F.IC_CL)
- DES/Retail MAC
- ECC (supplied by F.IC_CL)
- RSA (supplied by F.IC_CL)
- DH (supplied by F.IC_CL)

This function implements the hash algorithms according to FIPS 180-4 [FIPS_180-4]

- SHA-1 (supplied by F.IC_CL)
- SHA-224 (supplied by F.IC_CL)
- SHA-256 (supplied by F.IC_CL)
- SHA-384 (supplied by F.IC_CL)
- SHA-512 (supplied by F.IC_CL)

Note 56: In **phase 3** the Personalization Agent can use the ECC functionality to generate the Chip Authentication key pair and the Active Authentication key pair or the RSA functionality the generate the Active Authentication key pair.

7.1.2.5 F.Verification

TOE internal functions ensures correct operation.

7.2 Assurance Measures

The assurance measures fulfilling the requirements of EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 are given in table 7.2.

Measure	Description
ADV_ARC.1	Security architecture description
ADV_FSP.5	Complete semi-formal functional specification with additional error information
ADV_IMP.1	Implementation representation of the TSF
ADV_INT.2	Well-structured internals
ADV_TDS.4	Semiformal modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures

Measure	Description
ALC_CMC.4	Production support, acceptance procedures, automation
ALC_CMS.5	Development tools CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.2	Compliance with implementation standards
ATE_COV.2	Analysis of coverage
ATE_DPT.3	Testing: modular design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.5	Advanced methodical vulnerability analysis

Table 7.2: Assurance Measures

7.3 TOE Summary Specification Rationale

Table 7.3 shows the coverage of the SFRs by TSFs.

SFR	TSFs
FCS_CKM.1/DH_PACE	F.IC_CL
FCS_CKM.1/CA	F.IC_CL
FCS_CKM.4	F.Identification_Authentication
FCS_COP.1/PACE_ENC	F.IC_CL, F.Crypto
FCS_COP.1/CA_ENC	F.IC_CL, F.Crypto
FCS_COP.1/PACE_MAC	F.Crypto
FCS_COP.1/CA_MAC	F.Crypto
FCS_COP.1/SIG_VER	F.IC_CL
FCS_COP.1/AA	F.IC_CL
FCS_RND.1	F.IC_CL
FIA_AFL.1/PACE	F.Identification_Authentication
FIA_UID.1/PACE	F.Access_Control
FIA_UAU.1/PACE	F.Access_Control
FIA_UAU.4/PACE	F.Identification_Authentication
FIA_UAU.5/PACE	F.Access_Control, F.Identification_Authentication
FIA_UAU.6/PACE	F.Identification_Authentication
FIA_UAU.6/EAC	F.Identification_Authentication
FIA_API.1	F.Identification_Authentication

SFR	TSFs
FIA_API.1/AA	F.Identification_Authentication
FDP_ACC.1/TRM	F.Access_Control
FDP_ACF.1/TRM	F.Access_Control
FDP_RIP.1	F.Identification_Authentication, F.Management
FDP_UCT.1/TRM	F.Access_Control
FDP_UIT.1/TRM	F.Access_Control
FAU_SAS.1	F.IC_CL
FMT_SMF.1	F.Management
FMT_SMR.1/PACE	F.Identification_Authentication
FMT_LIM.1	F.IC_CL
FMT_LIM.2	F.IC_CL
FMT_MTD.1/INI_ENA	F.IC_CL, F.Access_Control
FMT_MTD.1/INI_DIS	F.Access_Control, F.Management
FMT_MTD.1/CVCA_INI	F.Access_Control
FMT_MTD.1/CVCA_UPD	F.Identification_Authentication
FMT_MTD.1/DATE	F.Identification_Authentication
FMT_MTD.1/CAPK	F.Access_Control
FMT_MTD.1/AAPK	F.Access_Control
FMT_MTD.1/PA	F.Identification_Authentication
FMT_MTD.1/KEY_READ	F.Access_Control
FMT_MTD.1/KEY_READ_AA	F.Access_Control
FMT_MTD.1/KEY_READ_PACE_CAM	F.Access_Control
FMT_MTD.3	F.Identification_Authentication
FPT_EMS.1	F.IC_CL
FPT_FLS.1	F.IC_CL
FPT_TST.1	F.IC_CL, F.Verification
FPT_PHP.3	F.IC_CL
FTP_ITC.1/PACE	F.Access_Control, F.Identification_Authentication

Table 7.3: Coverage of SFRs for the TOE by TSFs.

The SFR **FCS_CKM.1/DH_PACE** requires the ECDH algorithm. This is provided by **F.IC_CL (TSF.Crypto)**.

The SFR **FCS_CKM.1/CA** requires the DH and the ECDH algorithm. This is provided by **F.IC_CL (TSF.Crypto)**.

The SFR **FCS_CKM.4** requires the destroying of cryptographic keys. This is done in **F.Identification_Authentication** (“Overwrites keys in transient memory after usage”).

The SFR **FCS_COP.1/PACE_ENC** requires AES and 3DES in CBC mode. **F.IC_CL**

(TSF.Crypto) and **F.Crypto** provide this algorithm.

The SFR **FCS_COP.1/CA_ENC** requires AES and 3DES in CBC mode. **F.IC_CL (TSF.Crypto)** and **F.Crypto** provide this algorithm.

The SFR **FCS_COP.1/PACE_MAC** requires AES and 3DES in CBC mode. **F.Crypto** provides this algorithm.

The SFR **FCS_COP.1/CA_MAC** requires AES and 3DES in CBC mode. **F.Crypto** provides this algorithm.

The SFR **FCS_COP.1/SIG_VER** requires ECDSA and cryptographic key sizes BP(r1): 224, 256, 320, 384, 512 bits, NIST: 224, 256, 384, 521 bits and RSA and cryptographic key sizes 1536 - 4096 bits to perform digital signature verification. **F.IC_CL (TSF.Crypto)** provides these functions.

The SFR **FCS_COP.1/AA** requires ECDSA and RSA. **F.IC_CL (TSF.Crypto)** provides these functions.

The SFR **FCS_RND.1** requires the generation of random numbers which is provided by **F.IC_CL (TSF.Service)**. The provided random number generator produces cryptographically strong random numbers which are used at the appropriate places as written in the addition there.

The SFR **FIA_AFL.1/PACE** requires the detection of an unsuccessful authentication attempt and the waiting for a specified time between the reception of an authentication command and its processing. **F.Identification_Authentication** detects unsuccessful authentication attempts.

The SFR **FIA_UID.1/PACE** requires timing of identification. It is handled by **F.Access_Control** which enforces identification of a role before access is granted. Also all policies prevent reading sensitive or user dependent data without user identification.

The SFR **FIA_UAU.1/PACE** requires timing of authentication. It is handled by **F.Access_Control** which enforces authentication of a role before access is granted. Also all policies prevent reading sensitive or user dependent data without user authentication.

The SFR **FIA_UAU.4/PACE** requires prevention of authentication data reuse. This is in particular fulfilled by using changing initialization vectors in Secure Messaging. Secure Messaging is provided by **F.Identification_Authentication**.

The SFR **FIA_UAU.5/PACE** requires Passive Authentication protocol, Secure Messaging in encrypt-then-authenticate mode and PACE protocol based on 3DES or AES. In addition SFR **FIA_UAU.5** also requires the authentication of any user's claimed identity. **F.Identification_Authentication** and **F.Access_Control** fulfill these requirements.

The SFR **FIA_UAU.6/PACE** requires re-authentication for each command after successful authentication (PACE authentication in *operational use* phase). This is done by **F.Identification_Authentication** providing Secure Messaging.

The SFR **FIA_UAU.6/EAC** requires re-authentication for each command after successful authentication (EAC authentication in *operational use* phase). This is done by **F.Identification_Authentication** providing Secure Messaging.

The SFR **FIA_API.1** requires the proving of the identity of the TOE. The Chip Authentication is done by **F.Identification_Authentication**.

The SFR **FIA_API.1/AA** requires the proving of the identity of the TOE. The Active Authentication is done by **F.Identification_Authentication**.

The SFR **FDP_ACC.1/TRM** requires the enforcement of the terminal access control policy on terminals gaining write, read, modification and usage access to user data stored in the ePass. This is done by **F.Access_Control**.

The SFR **FDP_ACF.1/TRM** requires the enforcement of the terminal access control policy on objects which is done by **F.Access_Control**.

The SFR **FDP_RIP.1** requires residual information protection. This is done by **F.Identification_Authentication** and **F.Management**.

The SFR **FDP_UCT.1/TRM** requires data exchange confidentiality. This is done by **F.Access_ Control**.

The SFR **FDP_UIT.1/TRM** requires data exchange integrity. This is done by **F.Access_ Control**.

The SFR **FAU_SAS.1** requires the storage of the chip identification data which is addressed in **F.IC_CL (TSF.Service)**.

The SFR **FMT_SMF.1** requires security management functions for initialization, personalization and configuration. This is done by **F.Management**.

The SFR **FMT_SMR.1/PACE** requires the maintenance of roles. The roles are managed by **F.Identification_Authentication**.

The SFR **FMT_LIM.1** requires limited capabilities of test functions which is provided by **F.IC_CL (TSF.Control)** which controls what commands can be executed thereby preventing external usable test functions to do harm. The IC Dedicated Test Software only is available in the test mode.

The SFR **FMT_LIM.2** requires limited availabilities of test functions which is provided by **F.IC_CL (TSF.Control)** which controls what commands can be executed thereby preventing external usable test functions to do harm and the access to memory and special function registers. The IC Dedicated Test Software only is available in the test mode.

The SFR **FMT_MTD.1/INI_ENA** requires writing of initialization data and pre-personalization data to the *Manufacturer*. Writing of pre-personalization and installation data only by the *Manufacturer* is enforced by **F.Access_Control**. In addition **F.IC_CL (TSF.Control)** stores this data in the User Read Only Area which cannot be changed afterwards.

The SFR **FMT_MTD.1/INI_DIS** requires only the *Personalization Agent* to be able to read out and use the initialization data. This is provided by **F.Management** and **F.Access_Control**.

The SFR **FMT_MTD.1/CVCA_INI** requires only *Personalization Agent* to be able to write initial Country Verifying Certification Authority public key, initial Country Verifier Certification Authority certificate and initial date. This is provided by **F.Access_Control**.

The SFR **FMT_MTD.1/CVCA_UPD** requires only *Country Verifier Certification Authority* to be able to update Country Verifier Certification Authority public key and Country Verifier Certification Authority certificate. This is provided by **F.Identification_Authentication** (properties of terminal authentication).

The SFR **FMT_MTD.1/DATE** requires only *Country Verifier Certification Authority*, *Document Verifier* and domestic *Extended Inspection System* to be able to modify the current date. This is provided by **F.Identification_Authentication** (properties of terminal authentication).

The SFR **FMT_MTD.1/CAPK** requires the *Personalization Agent* to be able to create or load the Chip Authentication private key. This is provided by **F.Access_Control** allowing the *Personalization Agent* in phase 3 to write all necessary data.

The SFR **FMT_MTD.1/AAPK** requires the *Personalization Agent* to be able to create or load the Active Authentication private key. This is provided by **F.Access_Control** allowing the *Personalization Agent* in phase 3 to write all necessary data.

The SFR **FMT_MTD.1/PA** requires only the *Personalization Agent* to write the document security object. This is provided by **F.Identification_Authentication**.

The SFR **FMT_MTD.1/KEY_READ**, **FMT_MTD.1/KEY_READ_AA** and **FMT_MTD.1/KEY_READ_PACE_CAM** require that no read access to secret keys is given to anyone. This is provided by **F.Access_Control**.

The SFR **FMT_MTD.3** requires only secure values of the certificate chain are accepted for data of the Terminal Authentication protocol and the access control. This is done by **F.Identification_Authentication** (Terminal Authentication properties).

The SFR **FPT_EMS.1** requires limiting of emanations. This is provided by **F.IC_CL (TSF.Control)**.

The SFR **FPT_FLS.1** requires failure detection and preservation of a secure state. This is provided by **F.IC_CL (TSF.Protection, TSF.Control)**. The security functions audit continually and react to environmental and other problems by bringing the IC into a secure state.

The SFR **FPT_TST.1** requires testing for (a) correct operation, (b) integrity of data and (c) integrity of executable code. **F.Verification** does this testing. **F.IC_CL (TSF.Protection)** controls all NVM and FLASH content for integrity.

The SFR **FPT_PHP.3** requires resistance to physical manipulation and probing. This is provided by **F.IC_CL (TSF.Protection)** which is provided by the hardware to resist attacks.

The SFR **FTP_ITC.1/PACE** requires the usage of a trusted channel. This is done by **F.Access_Control** and **F.Identification_Authentication**.

7.4 Statement of Compatibility

This is a statement of compatibility between this composite Security Target and the Security Target of P71D352 (N7121) [NXP_P71_ST].

7.4.1 Relevance of Hardware TSFs

All security functions of the hardware and cryptographic library that are used by the TOE (as indicated in Table 7.1) are relevant for the composite Security Target.

7.4.2 Compatibility: TOE Security Environment

7.4.2.1 Security Objectives

Table 7.4 gives a mapping of the hardware security objectives to those of the composite ST. Those taken from the [CC_PP-0068-V2] are given in *italic*, those that are given in the ST in addition to [CC_PP-0068-V2] and [CC_PP-0056-V2] are underlined.

HW objective	Matches TOE objective	Remarks
O.Leak-Inherent (protection against inherent information leakage)	*OT.Prot_Inf_Leak*	
O.Phys-Probing (protection against physical probing)	*OT.Prot_Phys-Tamper*	
O.Malfunction (protection against malfunctions)	*OT.Prot_Malfunction*	
O.Phys-Manipulation (protection against physical manipulation)	*OT.Prot_Phys-Tamper*	
O.Leak-Forced (protection against forced information leakage)	*OT.Prot_Inf_Leak*	
O.Abuse-Func (protection against abuse of functionality)	*OT.Prot_Abuse-Func*	
O.Identification (TOE identification)	*OT.Identification*	
O.RND (random numbers)	–	no conflicts
O.Cap_Avail_Loader (capability and availability of the loader)	–	not applicable (the loader is deactivated before delivery)
O.Ctrl_Auth_Loader (optional) (access control and authenticity for the loader)	–	not applicable (the loader is deactivated before delivery)
O.TDES (cryptographic service Triple-DES)	*OT.Data_Confidentiality* OT.Sens_Data_Conf	
O.AES (cryptographic service AES)	*OT.Data_Confidentiality* OT.Sens_Data_Conf	
O.SHA (cryptographic service hash function)	–	no conflict
O.NVM-Integrity (integrity support of data stored to NVM)	*OT.Data_Integrity*	

HW objective	Matches TOE objective	Remarks
O.Access-Control (access control to memories and special function registers)	*OT.Data_Confidentiality* OT.Sens_Data_Conf *OT.Prot_Abuse-Func*	
O.Self-Test (self-test)	–	no conflict
O.PUF (optional) (sealing/unsealing user data)	–	no conflict
O.Secure-User-Mode-Box (optional) (secure user mode box firewall)	–	no conflict
O.RSA (RSA functionality (optional))	*OT.Data_Confidentiality* OT.Sens_Data_Conf OT.Active_Auth_Proof	
O.ECC (elliptic-curve cryptography over GF(p) (optional))	*OT.Data_Confidentiality* OT.Sens_Data_Conf OT.Active_Auth_Proof	
OE.Resp-Appl (treatment of user data)	–	no conflict
OE.Process-Sec-IC (protection during composite product manufacturing)	–	no conflict
OE.Lim_Block_Loader (limitation of capability and blocking the loader)	–	not applicable (the loader is deactivated before delivery)
OE.Loader_Usage (optional) (secure communication and usage of the Loader)	–	not applicable (the loader is deactivated before delivery)
OE.Check-Init (check of initialization data by the security IC embedded software)	–	no conflict

Table 7.4: Mapping of hardware to TOE security objectives including those of the environment.

7.4.2.2 Security Requirements

Table 7.5 addresses the platform security requirements and their relevance for the TOE. Those taken from the PACE-PP [CC_PP-0068-V2] are given in *italic*, those taking Active Authentication into account are underlined. Neither the SFRs that can be mapped to the platform SFRs nor those that are application specific (and thus not listed in the table) show any conflicts with the platform SFRs.

HW SFRs	Matches TOE SFR	Remarks
FRU_FLT.2 (limited fault tolerance)	*FPT_FLS.1* *FPT_TST.1*	
FPT_FLS.1 (failure with preservation of secure state)	*FPT_FLS.1*	
FMT_LIM.1 (limited capabilities)	FMT_LIM.1	
FMT_LIM.2 (limited availability)	FMT_LIM.2	
FAU_SAS.1 (audit storage)	*FAU_SAS.1*	
FDP_SDC.1 (stored data confidentiality)	–	used implicitly, no conflict
FDP_SDI.2 (stored data integrity monitoring and action)	–	used implicitly, no conflict
FPT_PHP.3 (resistance to physical attack)	*FPT_PHP.3*	
FDP_ITT.1 (basic internal transfer protection)	FPT_EMS.1	
FPT_ITT.1 (basic internal TSF data transfer protection)	FPT_EMS.1	
FDP_IFC.1 (subset information flow control)	FPT_EMS.1	
FCS_RNG.1/PTG.2 (random number generation – PTG.2)	*FCS_RND.1*	
FMT_LIM.1/Loader (limited capabilities – loader)	–	not applicable (loader deactivated before delivery)
FMT_LIM.2/Loader (limited availability – loader)	–	not applicable (loader deactivated before delivery)
FTP_ITC.1/Loader (inter-TSF trusted channel (optional))	–	not applicable (loader deactivated before delivery)
FDP_UCT.1/Loader (basic data exchange confidentiality (optional))	–	not applicable (loader deactivated before delivery)
FDP_UIT.1/Loader (data exchange integrity (optional))	–	not applicable (loader deactivated before delivery)
FDP_ACC.1/Loader (subset access control – loader (optional))	–	not applicable (loader deactivated before delivery)

HW SFRs	Matches TOE SFR	Remarks
FDP_ACF.1/Loader (security attribute based access control – loader (optional))	–	not applicable (loader deactivated before delivery)
FCS_COP.1/TDES (cryptographic operation – TDES)	–	used implicitly with crypto library, no conflict
FCS_CKM.4/TDES (cryptographic key destruction – TDES)	–	used implicitly, no conflict
FCS_COP.1/AES (cryptographic operation – AES)	–	used implicitly with crypto library, no conflict
FCS_CKM.4/AES (cryptographic key destruction – AES)	–	used implicitly, no conflict
FCS_COP.1/TDES_LIB (cryptographic operation – TDES – crypto library (optional))	*FCS_COP.1/PACE_ENC* FCS_COP.1/CA_ENC *FCS_COP.1/PACE_MAC* FCS_COP.1/CA_MAC	
FCS_CKM.4/TDES_LIB (cryptographic key destruction – crypto library (optional))	–	used implicitly, no conflict
FCS_COP.1/AES_LIB (cryptographic operation – AES – crypto library (optional))	*FCS_COP.1/PACE_ENC* FCS_COP.1/CA_ENC *FCS_COP.1/PACE_MAC* FCS_COP.1/CA_MAC	
FCS_CKM.4/AES_LIB (cryptographic key destruction – crypto library (optional))	–	used implicitly, no conflict
FCS_RNG.1/DRG.4 (random number generation – hybrid deterministic (optional))	–	not used by the TOE, no conflict
FCS_RNG.1/PTG.3 (random number generation – hybrid physical (optional))	*FCS_RND.1*	
FCS_COP.1/RSA (cryptographic operation – RSA (optional))	FCS_CKM.1/CA FCS_COP.1/SIG_VER FCS_COP.1/AA	FCS_CKM.1/CA is mapped because of DH key agreement
FCS_COP.1/RSA_PAD (cryptographic operation – RSA message encoding (optional))	–	not used by the TOE, no conflict
FCS_COP.1/RSA_PubExp (cryptographic operation – RSA public key computation (optional))	–	not used by the TOE, no conflict
FCS_CKM.1/RSA (cryptographic key generation – RSA (optional))	–	not used by the TOE, no conflict

HW SFRs	Matches TOE SFR	Remarks
FCS_CKM.4/RSA (cryptographic key destruction – RSA (optional))	–	not used by the TOE, no conflict
FCS_COP.1/ECDSA (cryptographic operation – ECDSA (optional))	FCS_COP.1/SIG_VER FCS_COP.1/AA	
FCS_COP.1/ECC_DHKE (cryptographic operation – Diffie-Hellman key exchange (optional))	*FCS_CKM.1/DH_PACE* FCS_CKM.1/CA	
FCS_CKM.1/ECDSA (cryptographic key generation – ECDSA (optional))	–	not used by the TOE, no conflict
FCS_CKM.4/ECDSA (cryptographic key destruction – ECDSA (optional))	–	used implicitly, no conflict
FCS_COP.1/SHA (cryptographic operation – hashing (optional))	FCS_COP.1/SIG_VER FCS_COP.1/AA	
FCS_COP.1/AES_PUF (cryptographic operation – PUF based AES)	–	not used by the TOE, no conflict
FCS_COP.1/MAC_PUF (cryptographic operation – PUF based MAC)	–	not used by the TOE, no conflict
FCS_CKM.1/PUF (cryptographic key generation – PUF)	–	not used by the TOE, no conflict
FCS_CKM.4/PUF (cryptographic key destruction – PUF)	–	not used by the TOE, no conflict
FPT_TST.1 (subset TOE testing)	*FPT_TST.1*	
FMT_SMF.1 (specification of management functions)	*FMT_SMF.1*	
FDP_ACC.1/ACP (subset access control – access control policy)	FDP_ACC.1/TRM	
FDP_ACF.1/ACP (security attribute based access control – access control policy)	FDP_ACF.1/TRM	
FMT_MSA.1/ACP (management of security attributes – access control policy)	*FMT_SMF.1*	

HW SFRs	Matches TOE SFR	Remarks
FMT_MSA.3/ACP (static attribute initialization – access control policy)	*FMT_SMF.1*	

Table 7.5: Mapping of hardware to TOE SFRs.

7.4.2.3 Assurance Requirements

The level of assurance of the

- TOE is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
- Hardware is EAL6 augmented with ALC_FLR.1 and ASE_TSS.2

This shows that the assurance requirements of the TOE is matched or exceeded by the assurance requirements of the hardware. There are no conflicts.

7.4.3 Conclusion

Overall no contradictions between the Security Targets of the TOE and the hardware can be found.

8 Glossary and Acronyms

Accurate Terminal Certificate A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [BSI_TR-03110-1].

Advanced Inspection Procedure (with PACE) A specific order of authentication steps between a travel document and a terminal as required by [ICAO_SAC], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE and EIS-AIP-BAC.

Agreement This term is used in BSI-CC-PP-0056-V2-2011 [CC_PP-0056-V2] in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.

Active Authentication Security mechanism defined in [ICAO_9303] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organization.

Application note / Note Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Audit records Write-only-once non-volatile memory area of the travel document's chip to store the Initialization Data and Pre-personalization Data.

Authenticity Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organization

Basic Access Control (BAC) Security mechanism defined in [ICAO_9303] by which means the travel document's chip proves and the basic inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).

Basic Inspection System with PACE protocol (BIS-PACE) A technical system being used by an inspecting authority and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder).

The Basic Inspection System with PACE is a PACE Terminal additionally supporting/ applying the Passive Authentication protocol and is authorized by the travel document

Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.

Basic Inspection System (BIS) An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.

Biographical data (biodata) The personalized details of the travel document holder appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO_9303]

Biometric reference data Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.

Card Access Number (CAN) Password derived from a short number printed on the front side of the data-page.

Certificate chain A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.

Counterfeit An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_9303]

Country Signing CA Certificate (C_{CSCA}) Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority and stored in the inspection system.

Country Signing Certification Authority (CSCA) 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.

The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO_9303], 5.5.1.

The Country Signing Certification Authority issuing certificates for Document Signers (cf. [ICAO_9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [BSI_TR-03110-1].

Country Verifying Certification Authority (CVCA) 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, see [BSI_TR-03110-1].

Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a CVCS as a subject; hence, it merely represents an organizational entity within BSI-CC-PP-0056-V2-2012.

The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO_9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [BSI_TR-03110-1].

Current date The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.

CV Certificate Card Verifiable Certificate according to [BSI_TR-03110-1].

CVCA link Certificate Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.

Document Basic Access Key Derivation Algorithm The [ICAO_9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

PACE passwords Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO_SAC].

Document Details Data Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.

Document Security Object (SO_D) A RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS). [ICAO_9303]

Document Signer (DS) An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication.

A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS})(CDS), see [BSI_TR-03110-1] and [ICAO_9303].

This role is usually delegated to a Personalization Agent.

Document Verifier (DV) 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, see [BSI_TR-03110-1].

Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a DV as a subject; hence, it merely represents an organizational entity within this ST.

There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a

policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer and a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy).[1],[2]

Eavesdropper A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.

Enrollment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]

Travel document (electronic) The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.

ePassport application A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [BSI_TR-03110-1].

Extended Access Control Security mechanism identified in [ICAO_9303] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.

Extended Inspection System (EIS) A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.

Forgery Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait. [ICAO_9303]

Global Interoperability The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all travel documents. [ICAO_9303]

IC Dedicated Software Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life cycle phases.

[1] The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in BSI-CC-PP-0068-V2-2011 in order to reflect an appropriate relationship between the parties involved.

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

IC Dedicated Support Software That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

IC Dedicated Test Software That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

IC Embedded Software Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.

IC Identification Data The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.

Impostor A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_9303]

Improperly documented person A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_9303]

Initialization Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).

Initialization Data Any data defined by the TOE manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are, for instance, used for traceability and for IC identification as travel document's material (IC identification data).

Inspection The act of State examining an travel document presented to it by a traveler (the travel document holder) and verifying its authenticity. [ICAO_9303].

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

Integrated circuit (IC) Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.

Integrity Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organization.

Issuing Organization Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]

Issuing State The Country issuing the travel document. [ICAO_9303]

Logical Data Structure (LDS) The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the travel document's chip.

Logical travel document Data of the travel document holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contactless/contact integrated circuit. It presents contactless or contact based readable data including (but not limited to)

1. personal data of the travel document holder
2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
3. the digitized portraits (EF.DG2),
4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and
5. the other data according to LDS (EF.DG5 to EF.DG16).
6. EF.COM and EF.SOD

Machine readable travel document (MRTD) Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_9303].

Machine readable zone (MRZ) Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1,the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303].

The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.

Machine-verifiable biometrics feature A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_9303]

Manufacturer Generic term for the IC manufacturer producing integrated circuit and the travel document manufacturer completing the IC to the travel document. The *Manufacturer* is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC manufacturer and travel document manufacturer using this role manufacturer.

Metadata of a CV Certificate Data within the certificate body (excepting Public Key) as described in [BSI_TR-03110-1].

The metadata of a CV certificate comprise the following elements:

- Certificate Profile Identifier,
- Certificate Authority Reference,
- Certificate Holder Reference,
- Certificate Holder Authorization Template,
- Certificate Effective Date,
- Certificate Expiration Date.

ePassport application Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes

- the file structure implementing the LDS [ICAO_9303],

- the definition of the user data, but does not include the user data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and
- the TSF Data including the definition the authentication data but except the authentication data itself.

Optional biometric reference data Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.

Passive authentication Security mechanism implementing (i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.

Password Authenticated Connection Establishment (PACE) A communication establishment protocol defined in [ICAO_SAC]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.

PACE password A password needed for PACE authentication, e.g. CAN or MRZ.

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 "Enrollment" (cf. sec. 1.2, TOE life-cycle, Phase 3, Step 6).

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:

i establishing the identity of the travel document holder for the biographic data in the travel document,
ii enrolling the biometric reference data of the travel document holder,
iii writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [BSI_TR-03110-1],
iv writing the document details data,
v writing the initial TSF data,
vi signing the Document Security Object defined in [ICAO_9303] (in the role of DS).

Please note that the role '*Personalization Agent*' may be distributed among several institutions according to the operational policy of the travel document Issuer.

Generating signature key pair(s) is not in the scope of the tasks of this role.

Personalization Data A set of data incl. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalization data are gathered and then written into

the non-volatile memory of the TOE by the *Personalization Agent* in the life cycle phase *card issuing*.

Pre-personalization Data Any data that is injected into the non-volatile memory of the TOE by the *Manufacturer* for traceability of the non-personalized travel document and/or to secure shipment within or between the life cycle phases *Manufacturing* and *card issuing*.

Pre-personalized travel document's chip Travel document's chip equipped with a unique identifier and a unique Authentication Key Pair of the chip.

Receiving State The Country to which the travel document holder is applying for entry; see [ICAO_9303].

Reference data Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

RF-terminal A device being able to establish communication with an RF-chip according to ISO/IEC 14443.

Rightful equipment (rightful terminal or rightful Card) A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either BIS-PACE (see *Inspection System*).

Secondary image A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [ICAO_9303]

Secure messaging in combined mode Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.

Skimming Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact communication channel of the TOE without knowledge of the printed PACE password.

Standard Inspection Procedure A specific order of authentication steps between an travel document and a terminal as required by [ICAO_SAC], namely (i) PACE and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.

Supplemental Access Control A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.

Terminal A Terminal is any technical system communicating with the TOE through a contactless/contact interface.

TOE tracing data Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognizing the travel document.

Travel document Official document issued by a state or organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO_9303] (there "Machine readable travel document").

Travel document (electronic) The contactless/contact smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.

Travel document holder A person for whom the ePass Issuer has personalized the travel document.

Travel document Issuer (issuing authority) Organization authorized to issue an electronic Passport to the travel document holder.

Travel document presenter A person presenting the travel document to a terminal and claiming the identity of the travel document holder.

TSF data Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC_Part1]).

Unpersonalized travel document Travel document material prepared to produce a personalized travel document containing an initialized and pre-personalized travel document's chip.

User data All data (being not authentication data)

i stored in the context of the ePassport application of the travel document as defined in [ICAO_9303] and
ii being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_SAC]).

CC give the following generic definitions for user data:
Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC_Part1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC_Part2]).

Verification data Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [CC_PP-0055])
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority
EAC	Extended Access Control

Acronym	Term
EF	Elementary file
ICCSN	Integrated circuit card serial number
MF	Master file
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity coupling device
PICC	Proximity integrated circuit chip
PP	Protection Profile
PT	Personalization terminal
RF	Radio frequency
SAC	Supplemental Access Control
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure, see [BSI_TR-03110-1], sec. 3.1.1
TA	Terminal Authentication
TOE	Target of evaluation
TSF	TOE security functionality
TSP	TOE security policy (defined by the current document)

Bibliography

[AGD] User Guidance – MTCOS Pro 2.5 ePassport / P71D352 (N7121), MaskTech International GmbH, Version 1.1, 2020-10-12.

[ANSI_X9-62] ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-11-16.

[BSI_AIS31] Anwendungshinweise und Interpretationen zum Schema – Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, AIS 31, Version 3, 2013-05-15.

[BSI_TR-03110-1] TR-03110-1, Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015-02-26.

[BSI_TR-03110-3] TR-03110-3, Technical Guideline 03110: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 – Common Specifications, BSI, Version 2.21, 2016-12-21.

[BSI_TR-03111] TR-03111, Technical Guideline TR-03111: Elliptic Curve Cryptography, BSI, Version 2.1, 2018-06-01.

[BSI_TR-03116-2] TR-03116-2, Technische Richtlinie – Kryptographische Verfahren für Projekte der Bundesregierung - Teil 2 – Hoheitliche Ausweisdokumente, BSI, Stand 2020, 2020-01-27.

[CC_Part1] CCMB-2017-04-001, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, 2017-04.

[CC_Part2] CCMB-2017-04-002, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, 2017-04.

[CC_Part3] CCMB-2017-04-003, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, 2017-04.

[CC_PartEM] CCMB-2017-04-004, Version 3.1, Revision 5, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC_PP-0055] BSI-CC-PP-0055-2009, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Basic Access Control, BSI, Version 1.10, 2009-03-25.

[CC_PP-0056-V2] BSI-CC-PP-0056-V2-2012-MA-02, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Extended Access Control with PACE, BSI, Version 1.3.2, 2012-12-05.

[CC_PP-0068-V2] BSI-CC-PP-0068-V2-2011-MA-01, Common Criteria Protection Profile / Machine Readable Travel Document using Standard Inspection Procedure with PACE (ePass_PACE PP), BSI, Version 1.01, 2014-07-22.

[CC_PP-0084] BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages, EUROSMART, Version 1.0, 2014-01-13.

[FIPS_140-3] FIPS PUB 140-3, Security Requirements for Cryprographic Modules, National Institute of Standards and Technology, 2019-03.

[FIPS_180-4] FIPS PUB 180-4, Secure Hash Standard (SHS), National Institute of Standards and Technology, 2015-08.

[FIPS_186-4] FIPS PUB 186-4, DIGITAL SIGNATURE STANDARD (DSS), National Institute of Standards and Technology, 2013-07.

[FIPS_197] FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), National Institute of Standards and Technology, 2001-11.

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, ICAO, 2015.

[ICAO_SAC] Technical Report: Supplemental Access Control for Machine Readable Travel Documents, ICAO, TR-SAC V1.1, 2014-04-15.

[ISO_10116] ISO/IEC 10116-2017, Information technology – Security techniques - Modes of operation for an n-bit block cipher, ISO/IEC, 2017-07.

[ISO_11770-3] ISO/IEC 11770-3:2015, Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, ISO/IEC, 2015-08-01.

[ISO_7816] ISO/IEC 7816, Identification cards – Integrated circuit cards – Multipart Standard, ISO/IEC, 2008.

[ISO_9796-2] ISO/IEC 9796-2:2010, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, ISO/IEC, 2010-12.

[ISO_9797-1] ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO/IEC, 2011.

[KiSch-RNG] Version 2.0, A proposal for: Functionality classes for random number generators, W. Killmann and W. Schindler, 2011-09-18.

[MT_Manual] MTCOS Pro 2.5 on P71D352 (N7121) – Manual, MaskTech GmbH, 2020-10-02. Version 1.0.

[NIST_SP800-38B] NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology, 2005-05.

[NIST_SP800-56A] NIST SP 800-56A Rev. 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology, 2018-04.

[NIST_SP800-67] NIST SP 800-67 Rev. 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST, 2017-11.

[NIST_SP800-90A] NIST SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, 2015-06.

[NXP_P71_ST] NXP Semiconductors, Security Target Lite 'NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library', BSI-DSZ-CC-1040-2019, Rev. 1.1, 2019-05-31.

[RFC_8017] RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2, K. Moriarty (Ed.), B. Kaliski, J. Johnson, and A. Rusch, 2016-11.

[SC_HID] BSI-DSZ-CC-S-0114-2018, HID Global GmbH, Site Security Target Lite of HID Global Ireland Teoranta in Galway, Ireland, Doc. No: F-10-138d, Rev. B, 2018-09-13.

[SC_HID_MY] BSI-DSZ-CC-S-0156-2020, HID Global GmbH, Site Security Target Lite for HID Global Malaysia, Rev. D, 2020-04-17.

[SC_Linxens] BSI-DSZ-CC-S-0143-2019, Linxens (Thailand) Co Ltd., Site Security Target LITE for AY1, Version 2.3, 2019-11-25.

[SOGIS_CRYPTO] SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms, SOG-IS Crypto Working Group, Version 1.2, 2020-01.

9 Revision History

Version	Date	Author	Changes
1.0	2020-10-02	Gudrun Schürer	Public version based on v0.6 of the confidential ST
1.1	2020-10-12	Gudrun Schürer	Amended note in table A.1

10 Contact

MaskTech GmbH – **Headquarters**

Nordostpark 45	Phone	+49 911 955149 0
D-90411 Nuernberg	Fax	+49 911 955149 7
Germany	Email	info@masktech.de

MaskTech GmbH – **Support**

Bahnhofstr. 13	Phone	+49 911 955149 0
D-87435 Kempten	Fax	+49 831 5121077 5
Germany	Email	support@masktech.de

MaskTech GmbH – **Sales**

Lauenburger Str. 15	Phone	+49 4151 8990858
D-21493 Schwarzenbek	Fax	+49 4151 8995462
Germany	Email	stimm@masktech.de

A Overview Cryptographic Algorithms

The following cryptographic algorithms are used by the TOE to enforce its security policy:

	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments ST-Reference
1	Authenticated Key Agreement / Authentication	PACEv2 (Generic Mapping), PACE-CAM (Chip Authentication Mapping), PACE (key agreement, authentication), Elliptic Curve Diffie-Hellman, Nonce Encryption, Authentication Token	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303] [BSI_TR-03111] sec. 4.3.2.1 also cf. line 9	| MRZ| = 160 | Nonce| = 128 BP(r1): 224, 256, 320, 384, 512 NIST: 224, 256, 384, 521 Session keys: 3DES: 112 AES: 128, 192, 256	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303]	FCS_CKM.1/DH_PACE FCS_COP.1/PACE_ENC FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE
2	Authentication	Chip Authentication V1 DH ECDH	[ICAO_9303] [ICAO_SAC] [BSI_TR-03110-1] [NIST_SP800-56A] sec. 5.5 [NIST_SP800-56A] sec. 5.5 [BSI_TR-03111] also cf. line 9	 2048/224 or 2048/256 BP(r1): 224, 256, 320, 384, 512 NIST: 224, 256, 384, 521 Session keys: 3DES: 112 AES: 128, 192, 256	[ICAO_9303] [ICAO_SAC] [BSI_TR-03110-1]	FCS_CKM.1/CA FIA_UAU.5/PACE FIA_UAU.6/EAC FIA_API.1
3	Authentication	Active Authentication RSA signature creation using SHA-[1, 224, 256, 384, 512] ECDSA signature creation using SHA-[1, 224, 256, 384, 512]	[ICAO_9303] [ICAO_SAC] [BSI_TR-03110-1] [ISO_9796-2], sec. 8 [FIPS_180-4] sec. 6 [FIPS_186-4] sec. 5 [BSI_TR-03111] sec. 4.2.1 [ANSI_X9-62] sec. 7 [FIPS_180-4] sec. 6 also cf. line 13	 1536 - 4096[1] 32 Bit steps. BP(r1): 224, 256, 320, 384, 512 NIST: 224, 256, 384, 521	[ICAO_9303] [ICAO_SAC] [BSI_TR-03110-1]	FCS_COP.1/AA FIA_API.1/AA
4	Authentication	Terminal Authentication V1 (signature verification)	[ICAO_9303] [ICAO_SAC] [BSI_TR-03110-1] [BSI_TR-03110-3]		[ICAO_9303] [ICAO_SAC] [BSI_TR-03110-1] [BSI_TR-03110-3]	FCS_COP.1/SIG_VER FIA_UAU.5/PACE

[1]Technical range. Usual values: 1536, 1792 (max. short APDU), 2048 bits; recommended acc. [SOGIS_CRYPTO]: > 3000 bits).

	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments ST-Reference
		ECDSA using SHA-[224, 256, 384, 512] RSA using SHA-[1, 256]	[ANSI_X9-62] sec. 7 [FIPS_180-4] sec. 6 [RFC_8017] sec. 5.2, 8 [FIPS_180-4] sec. 6 also cf. line 13	BP(r1): 224, 256, 320, 384, 512 NIST: 224, 256, 384, 521 1536 - 4096 1 32 Bit steps.		
5	Confidentiality	3DES in CBC mode for Secure Messaging	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303] [NIST_SP800-67] (3DES) [ISO_10116] sec. 7 (CBC)	112	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303]	FCS_COP.1/CA_ENC FCS_COP.1/PACE_ENC FDP_UCT.1/TRM
6	Confidentiality	AES in CBC mode for Secure Messaging	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303] [FIPS_197] (AES), [ISO_10116] sec. 7 (CBC)	128, 192, 256	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303]	FCS_COP.1/CA_ENC FCS_COP.1/PACE_ENC FDP_UCT.1/TRM
7	Integrity	3DES in Retail-MAC mode for Secure Messaging	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303] [NIST_SP800-67] (3DES) [ISO_9797-1] sec. 7.4 (Retail-MAC)	112	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303]	FCS_COP.1/PACE_MAC FCS_COP.1/CA_MAC FDP_UIT.1/TRM
8	Integrity	CMAC-AES for Secure Messaging	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303] [FIPS_197] (AES) [NIST_SP800-38B] sec. 6 (CMAC)	128, 192, 256	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303]	FCS_COP.1/PACE_MAC FCS_COP.1/CA_MAC FDP_UIT.1/TRM
9	Key Derivation	Chip Authentication V1, PACE, Key derivation using SHA-[1, 256]	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303] [FIPS_180-4] sec. 6 [BSI_TR-03111] sec. 4.3.3	3DES: 112 AES: 128, 192, 256	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303]	FCS_CKM.1/CA FCS_CKM.1/DH_PACE
10	Trusted Channel	Secure Messaging in ENC/MAC mode (PACE)	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303] also cf. lines 5 - 9	-	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303]	FTP_ITC.1/PACE FDP_UCT.1/TRM FDP_UIT.1/TRM
11	Trusted Channel	Secure Messaging in ENC/MAC mode (CA, after PACE)	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303] also cf. lines 5 - 9	-	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_SAC] [ICAO_9303]	FCS_CKM.1/CA FDP_UCT.1/TRM FDP_UIT.1/TRM
12	Cryptographic Primitive	PTG.3 Random number generator (PTG.2 and cryptographic post-processing)	[BSI_AIS31] [NIST_SP800-90A] sec. 10.2, 10.3.2	-	[BSI_TR-03116-2]	FCS_RND.1
13	Cryptographic Primitive	SHA-[1, 224, 256, 384, 512]	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303] [ICAO_SAC] [FIPS_180-4] sec. 6	-	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303] [ICAO_SAC]	Signature Creation, Signature Verification Key Derivation

Table A.1: Overview Cryptographic Algorithms