Security Target 'CardOS DI V5.3 EAC/PACE Version 1.0', Rev. 2.01, Edition 04/2016

Atos IT Solutions and Services GmbH
Otto-Hahn-Ring 6

D-81739 Munich
Germany

Disclaimer of Liability

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Contents

1 History and Indices

Revision History:

2.01	2016-04-19	Release Version

2 About this Document

2.1 References

2.1.1 General References

[BSI-AIS31-V3]

BSI, Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[BSI-AIS36-V4]

BSI, Anwendungshinweise und Interpretationen zum Schema, AIS36: Kompositionsevaluierung, Version 4, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[BSI-PP-0035]

BSI, Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-PP-0035

[BSI-TR-03110-1-V210]

BSI, Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents - Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20. March 2012

[BSI-TR-03110-3-V211]

BSI, Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents Part 3 - Common Specifications, Version 2.11, 12. July 2013

[BSI-TR-03111-V200-ECC]

BSI, Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.00, 2012-06-28

[BSI-TR-03116-2]

Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2 - Hoheitliche Ausweisdokumente, Stand 2014, Datum: 14.04.2014

[CC-3.1-P1]

Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 4 September 2012, CCMB-2012-09-001

[CC-3.1-P2]

Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-002

[CC-3.1-P3]

Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 4 September 2012, CCMB-2012-09-003

[CEM-3.1]

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004

[NIST-FIPS-PUB-186-4]

NIST, Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, July 2013

[NIST-FIPS-PUB-180-4]

Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, March 2012

[NIST-800-38A-2001]

NIST, Recommendation for Block Cipher Modes of Operation, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, December 2001

[ISO-IEC-7816-part-2]

ISO/IEC 7816: Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of contacts, Version Second Edition, 2008

[ISO-IEC-7816-part-3]

ISO/IEC 7816: Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electrical interface and transmission protocols Reference number: ISO/IEC 7816-3:2006(E)

[ISO-IEC-7816-part-4]

ISO/IEC 7816: Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange Reference number: ISO/IEC 7816-4:2005(E)

[ISO-IEC-7816-part-8]

ISO/IEC 7816: Identification cards - Integrated circuit cards - Part 8: Commands for security operations Reference number: ISO/IEC 7816-8:2004(E)

[ISO-IEC-9797-1-2011]

ISO/IEC, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2001-03

[RFC-5639-2010-03]

RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010

[RSA-PKCS-3-1993]

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

2.1.2 Common Evaluation Evidence

Note: The references in this are common for all evaluated configurations.

[AIS-V53DI-CardOS-Adm-Guid]

AIS, Administrator Guidance 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)', Atos IT Solutions and Services GmbH

[AIS-V53DI-CardOS-EPA]

AIS, ePassport Application 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)', Atos IT Solutions and Services GmbH

[AIS-V53DI-CardOS-LC-Support]

AIS, Life Cycle Support 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)', Atos IT Solutions and Services GmbH

[AIS-V53DI-CardOS-PR-Notes]

AIS, CardOS DI V5.3, Packages & Release Notes, Atos IT Solutions and Services GmbH

[AIS-V53DI-CardOS-PR-Notes-ICAO]

AIS, CardOS DI V5.3, ICAO Extension Packages & Release Notes, Atos IT Solutions and Services GmbH

[AIS-V53DI-CardOS-User-Guid]

AIS, User Guidance 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)', Atos IT Solutions and Services GmbH

[AIS-V53-CardOS-Users-Manual]

AIS, CardOS V5.3 Chipcard Operating System, User's Manual, Atos IT Solutions and Services GmbH, Edition

05/2014

[BSI-CC-PP-0035-2007]

BSI, Certification Report BSI-CC-PP-0035-2007 for Security IC Platform Protection Profile Version 1.0 from Atmel Secure Products, Infineon Technologies AG, NXP Semiconductors Germany GmbH, Renesas Technology Europe Ltd, STMicroelectronics

[BSI-CC-PP-0071]

BSI, Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application, prEN 14169-4:2012, Date: 2012-11, v1.0.1

[BSI-CC-PP-0071-2012]

BSI, BSI-CC-PP-0071-2012 for Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application, Version 1.0.1, V1.0, 12 December 2012

[BSI-DSZ-CC-0782-V2-2015]

BSI, Certification Report, BSI-DSZ-CC-0782-V2-2015, Infineon Security Controller M7892 B11 withoptional RSA2048/4096 v1.02.013, EC v1.02.013,SHA-2 v1.01 and Toolbox v1.02.013 libraries andwith specific IC dedicated software (firmware) from Infineon Technologies AG, 3 November 2015

[Infineon-ST-Chip-B11-2015-10-13]

Infineon, Security Target Lite, M7892 B11, Recertification, Including optional Software Libraries RSA - EC - SHA-2 - Toolbox, Common Criteria CC v3.1 EAL6 augmented (EAL6+), version 0.3 as of 2015-10-13

[Infineon-Chip-HW-Ref]

Infineon, M7892 Controller Family for Security Applications - Hardware Reference Manual Revision 1.6 2014-11-05 and Errata Sheet Revision 1.8 2014-12-01

[BSI-PP-0056-V2-2012-132]

BSI, Common Criteria Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, Version 1.3.2, 05th December 2012

[BSI-CC-PP-0056-V2-2012-MA-02]

BSI, Assurance Continuity Maintenance Report BSI-CC-PP-0056-V2-2012-MA-02 for Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE (EAC PP) Version 1.3.2, 21 December 2012

[BSI-CC-PP-0068-V2-2011]

BSI, Machine Readable Travel Document using Standard Inspection Procedure with PACE(PACE PP), BSI-CC-PP-0068-V2-2011, Version 1.0, 2nd November 2011

[BSI-CR-CC-PP-0068-V2-2011]

BSI, Certification Report BSI-CC-PP-0068-V2-2011 for Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP) Version 1.0, 10 November 2011

[BSI-CC-PP-0055-110]

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

[ICAO-9303-2006]

ICAO, International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents - Machine Readable Passports, 2006 (this includes the latest supplemental for ICAO Doc 9303 which also should be considered)

[ICAO-TR-101]

ICAO, Machine Readable Travel Documents, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version - 1.01, Date - November 11, 2010

[ICAO-TR-110]

ICAO, Machine Readable Travel Documents, TECHNICAL REPORT, Supplemental Access Control for Machine

Readable Travel Documents, Version - 1.10, Date - 15 April 2014

[ISO-IEC-7816-2008]

ISO/IEC 7816: Identification cards - Integrated circuit cards, Version Second Edition, 2008

[ISO-IEC-14443-2008-11]

ISO/IEC 14443 Identification cards - Contactless integrated circuit cards - Proximity cards, 2008-11

[ISO-IEC-11770-3]

ISO/IEC 11770-3: Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques, 2008

[PKCS3]

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

2.2 Tables

2.3 Acronyms

AA
: Active Authentication

AIP
: Advanced Inspection Procedure

APDU

Application Protocol Data Unit

BAC
: Basic Access Control

BIS
: Basic Inspection System

BIS-PACE
: Basic Inspection System with PACE

CA
: Chip Authentication

CAN
: Card Access Number

CC
: Common Criteria

CfPA
: Composite-fulfilled Platform Assumption

CSF
: CardOS Sequence Format

CVCA
: Country Verifying Certification Authority

DF
: Dedicated File

DH
: Diffie-Hellman

DPA
: Differential Power Analysis

DSA
: Digital Signature Algorithm

EAC
: Extended Access Control

EAL
: Evaluation Assurance Level

EC
: Elliptic Curve

ECDH
: Elliptic Curve DH

ECDSA
: EC DSA

EF
: Elementary File

EIS
: Extended Inspection System

eMRTD
: electronic MRTD

IC
: Integrated Circuit

ICAO
: International Civil Aviation Organization

ICC
: IC Card

ICCSN
: ICC Serial Number

IFD
: Interface Device

SLE78CLFX*P (M7892 B11)
: SLE78CLFX3000P/4000P or SLE78CLFX308AP/408AP (design step B11)

IP_SFR
: Irrelevant Platform SFR

IrPA
: Irrelevant Platform Assumption

IT
: Information Technology

LCS
: Life Cycle Status

LTD
: Logical Travel Document

MF
: Master File

MRTD
: Machine Readable Travel Documents

MRZ
: Machine readable zone

n.a.
: not applicable

OCR
: Optical Character Recognition

OSP
: Organizational security policy

PACE
: Password Authenticated Connection Establishment

PCD
: Proximity Coupling Device

PICC
: Proximity Integrated Circuit Chip

PP
: Protection Profile

PTRNG
: physical true RNG (short: physical RNG)

RP_SFR
: Relevant Platform SFR

PT
: Personalization Terminal

RF
: Radio Frequency

RSA
: Rivest Shamir Adleman

SAR
: Security assurance requirements

SCIC
: Smart Card IC

SE
: Security Environment

SFP
: Security Function Policy

SFR
: Security Functional Requirement

SgPA
: Significant Platform Assumption

SIP
: Standard Inspection Procedure

SM
: Secure Messaging

SPA
: Simple Power Analysis

SS
: Security Service

SSC
: Send Sequence Counter

ST
: Security Target

TA
: Terminal Authentication

TC
: Trust Center

TOE
: Target of Evaluation

TSF

TOE Security Functions

TSP
: TOE Security Policy (defined by the current document)

2.4 Terms and Definitions

2.4.1 Security Evaluation Terms

Common Criteria
: CC: set of rules and procedures for evaluating the security properties of a product

Evaluation Assurance Level
: EAL: a set of assurance requirements for a product, its manufacturing process and its security evaluation specified by Common Criteria

Protection Profile
: PP: document specifying security requirements for a class of products that conforms in structure and content to rules specified by common criteria

Security Target
: ST: document specifying security requirements for a particular product that conforms in structure and content to rules specified by common criteria, which may be based on one or more Protection Profiles

Target of Evaluation
: TOE: abstract reference in a document, such as a Protection Profile, for a particular product that meets specific security requirements

TOE Security Functions
: TSF: functions implemented by the TOE to meet the requirements specified for it in a Protection Profile or Security Target

2.4.2 Technical Terms

Note:

1. The following terms are taken over from [BSI-PP-0056-V2-2012-132]. References are adapted, e.g. [6] used by [BSI-PP-0056-V2-2012-132] is now [ICAO-9303-2006].

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-V210].

Advanced Inspection Procedure (with PACE)
: A specific order of authentication steps between a travel document and a terminal as required by [ICAO-TR-101], 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.

Agreement
: This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.

Active Authentication
: Security mechanism defined in [ICAO-9303-2006] 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
: Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Audit records
: Write-only-once non-volatile memory area of the travel document's chip to store the Initialization Data and Pre-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-9303-2006] by which means the travel document's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).

Basic Inspection System with PACE protocol (BIS-PACE)

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.

Biographic data (biodata)

The personalized details of the travel document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document. [ICAO-9303-2006]

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-9303-2006]

Country Signing CA Certificate (C.CSCA)

Certificate of the Country Signing Certification Authority Public Key (K.PuCSCA) issued by Country Signing Certification Authority 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-9303-2006], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [ICAO-9303-2006]) 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-V210].

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-V210]. 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 this PP. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO-9303-2006]) 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-V210].

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-V210].

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-9303-2006] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

PACE passwords

Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of

Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO-TR-101]

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 RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS). [ICAO-9303-2006]

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 (CDS), see [BSI-TR-03110-1-V210] and [ICAO-9303-2006]. 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-V210]. 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 PP. 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). The footnotes of this term made by [BSI-PP-0056-V2-2012-132] are as follows: Footnote 55: The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the current ST (adapted from 'current PP') in order to reflect an appropriate relationship between the parties involved. Footnote 56: 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.

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

Enrolment
: The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO-9303-2006]

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-V210].

Extended Access Control
: Security mechanism identified in [ICAO-9303-2006] 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 the portrait. [ICAO-9303-2006]

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-9303-2006]

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

IC Dedicated Support Software
: That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of

parts of the IC Dedicated Software might be restricted to certain phases.

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

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

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

Impostor
: A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO-9303-2006]

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-9303-2006]

Initialization
: Process of writing Initialization Data (see below) to the TOE (cf. ST chapter "TOE life-cycle", Phase 2, Step 3).

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

Inspection
: The act of a State examining an travel document presented to it by a traveller (the travel document holder) and verifying its authenticity. [ICAO-9303-2006]

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

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

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

Issuing Organization
: Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303-2006]

Issuing State
: The Country issuing the travel document. [ICAO-9303-2006]

Logical Data Structure (LDS)
: The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303-2006]. 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-9303-2006] as specified by ICAO on the contact-based/contactless integrated circuit. It presents contact-based/contactless 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-9303-2006]

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-9303-2006]. 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-9303-2006]

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

Metadata of a CV Certificate
: Data within the certificate body (excepting Public Key) as described in [BSI-TR-03110-1-V210]. The metadata of a CV certificate comprise the following elements: (i) Certificate Profile Identifier, (ii) Certificate Authority Reference, (iii) Certificate Holder Reference, (iv) Certificate Holder Authorization Template, (v) Certificate Effective Date, (vi) 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 (i) the file structure implementing the LDS [ICAO-9303-2006], (ii) 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 (iii) the TSF Data including the definition the authentication data but except the authentication data itself.

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

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

Password Authenticated Connection Establishment (PACE)
: A communication establishment protocol defined in [ICAO-TR-101]. 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 p). 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 "Enrolment" (cf. ST chapter "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-V210], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303-2006] (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 including (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Document Security Object). 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.

Personalization Agent Authentication Information
: TSF data used for authentication proof and verification of the Personalization Agent.

Personalization Agent Key
: Cryptographic authentication key used (i) by the Personalization Agent to prove his identity and to get access to the logical travel document and (ii) by the travel document's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/EAC.

Physical part of the travel document
: Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.

Pre-Personalization
: Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the travel document Application (cf. ST chapter "TOE life-cycle", Phase 2, Step 5)

Pre-personalization Data
: Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalized travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.

Pre-personalized travel document's chip
: travel document's chip equipped with a unique identifier.

Receiving State
: The Country to which the traveller is applying for entry. [ICAO-9303-2006]

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 [ISO-IEC-14443-2008-11].

Secondary image
: A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO-9303-2006]

Secure messaging in encrypted/combined mode
: Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4, [ISO-IEC-7816-2008]

Service Provider
: An official organization (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.

Skimming
: Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.

Standard Inspection Procedure
: A specific order of authentication steps between an travel document and a terminal as required by [ICAO-TR-101], namely (i) PACE or BAC and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.

Terminal
: A terminal is any technical system communicating with the TOE either through the contact-based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In this ST (adapted from 'this PP') the role 'Terminal' corresponds to any terminal being authenticated by the TOE. Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).

Terminal Authorization
: Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.

Terminal Authorization Level
: Intersection of the Certificate Holder Authorizations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.

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

Travel document
: Official document issued by a state or 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-9303-2006] (there "Machine readable travel document").

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.

Travel Document Holder
: The rightful holder of the travel document for whom the issuing State or organization personalized the travel document.

Travel document's Chip
: A contact-based/contactless integrated circuit chip complying with ISO/IEC 14443 [ISO-IEC-14443-2008-11] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO-9303-2006], sec III.

Travel document's Chip Embedded Software
: Software embedded in a travel document's chip and not being developed by the IC Designer. The travel document's chip Embedded Software is designed in Phase 1 and embedded into the travel document's chip in

Phase 2 of the TOE life-cycle.

Traveler
: Person presenting the travel document to the inspection system 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-3.1-P1]).

Unpersonalized travel document
: The travel document that contains the travel document chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.

User data
: All data (being not authentication data) (i) stored in the context of the ePassport application of the travel document as defined in [BSI-TR-03110-1-V210] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. 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-3.1-P1]). 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-3.1-P2]).

Verification
: The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO-9303-2006]

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.

3 Security Target Introduction (ASE_INT)

3.1 ST Reference

Title

Security Target 'CardOS DI V5.3 EAC/PACE Version 1.0'

Author

Atos IT Solutions and Services GmbH

Revision Number

2.01

General Status

Release

CC Version

3.1, Revision 4

Certification ID

BSI-DSZ-CC-967

Date

2016-04-19

The TOE is based on the Infineon Chip SLE78CLFX*P (M7892 B11) as ICC platform, which requires a composite evaluation.

This ST provides

- the introduction (ASE_INT), in this chapter,
- the conformance claims in 4 Conformance Claims (ASE_CCL),
- the security problem definition in 5 Security Problem Definition (ASE_SPD),
- the security objectives in 6 Security Objectives (ASE_OBJ)
- the extended components definition in 7 Extended Component Definition (ASE_ECD),
- the security and assurance requirements in 8 Security Requirements (ASE_REQ),
- the rationale in 8.3 Security Requirements Rationale, and
- the TOE summary specification (TSS) in 9 TOE summary specification (ASE_TSS).

3.2 TOE Reference

This ST refers to the TOE 'CardOS DI V5.3 EAC/PACE Version 1.0'.

The developer of the TOE is Atos IT Solutions and Services GmbH.

The underlying platform of the TOE is a Smart Card Integrated Circuit (SCIC), which can be used as wafer, module, smart card ("card" for short). The SCIC already contains the OS "CardOS DI V5.3" when delivered. The TOE as defined by this Composite Security Target consists of both the SCIC connected to the antenna and the ePassport Application. It is to be used as a travel document (passport). The SCIC is a SLE78CLFX*P (M7892 B11) from Infineon.

The Infineon chip SLE78CLFX*P (M7892 B11) and the libraries RSA v1.02.013, EC v1.02.013, SHA-2 v1.01, and Toolbox v1.02.013 are certified, see [Infineon-ST-Chip-B11-2015-10-13] and [BSI-DSZ-CC-0782-V2-2015].

SLE78CLFX*P (M7892 B11) is an abbreviation and denotes dual interface chips (design step B11) which differ only in flash size and input capacity (of the contactless interface):

- SLE78CLFX3000P with 300kByte flash, 27pF
- SLE78CLFX4000P with 404kByte flash, 27pF
- SLE78CLFX308AP with 300kByte flash, 78pF
- SLE78CLFX408AP with 404kByte flash, 78pF

The chips can be packaged in the modules M8.4, MCC8, MCS8 (27pF) or COM8.6, COM 10.6 (78pF) or other modules or packages.

Please note that all these derivates are covered by the certificate.

To be able to perform contactless connections the SLE78CLFX*P (M7892 B11) is provided with an antenna (inlay) which is done by a separate company, see [AIS-V53DI-CardOS-LC-Support].

3.3 TOE Overview

This ST defines the security objectives and requirements for the contact-based / contactless smart card of machine readable travel documents 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 **and optionally** the Active Authentication in 'ICAO Doc 9303' [ICAO-9303-2006].

The communication between terminal and chip is protected by Secure Messaging which is established after

i. Password Authenticated Connection Establishment (PACE) using Standard Inspection Procedure with PACE (BIS-PACE) according to BSI-CC-PP-0068-V2-2011]_
ii. Chip Authentication (CA) using a PACE authenticated terminal (BIS-PACE) according to [BSI-PP-0056-V2-2012-132]

The TOE protects

i. itself and the user data / cryptographic keys stored on it
ii. user data transferred between card and a terminal by securing the confidentiality and integrity
iii. itself against tracing.

The TOE utilizes the evaluation of the underlying platform, which includes the Infineon chip SLE78CLFX*P (M7892 B11), the IC Dedicated Software and the libraries RSA v1.02.013, EC v1.02.013, SHA-2 v1.01, and Toolbox v1.02.013. The security functionality TDES and AES supported by the Infineon chip SLE78CLFX*P (M7892 B11) are utilized by the TOE, too.

3.4 TOE Description

3.4.1 TOE Definition

The Target of Evaluation (TOE) addressed by this ST is an electronic travel document representing a contactless / contact-based smart card programmed according to International Civil Aviation Organization (ICAO) Technical Report "Supplemental Access Control" [ICAO-TR-101] (which means amongst others according to the Logical Data Structure (LDS) defined in [ICAO-9303-2006]) and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [ICAO-9303-2006] and BSI TR-03110 [BSI-TR-03110-1-V210]__, respectively. The communication between terminal and chip is protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 [BSI-CC-PP-0068-V2-2011].

The TOE comprises of at least

i. the circuitry of the travel document's chip (the integrated circuit, IC),
ii. the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
iii. the antenna,
iv. the IC Embedded Software (operating system),
v. the ePassport application and
vi. the associated guidance documentation.

Please note that the TOE is embedded into a document on which the holder data and other data are printed. This document and data printed on it are not part of the TOE.

The TOE provides contact-based and contactless interfaces and is able to connect itself

i. with terminals which provide a contactless interface
ii. with terminals which provide a contact-based interface.

3.4.2 TOE Usage and Security Features for Operational Use

A State or Organization issues travel documents to be used by the holder for international travel. The traveler presents a travel document to the inspection system to prove his or her identity. The travel document in context of this ST contains

(i) visual (eye readable) biographical data and portrait of the holder,

(ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and

(iii) data elements on the travel document's chip according to LDS in case of contactless machine reading.

The authentication of the traveler is based on

(i) the possession of a valid travel document personalized for a holder with the claimed identity as given on the biographical data page and

(ii) biometrics using the reference data stored in the travel document. The issuing State or Organization ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organization.

For this ST the travel document is viewed as unit of

(i) the physical part of the travel document in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder

(a) the biographical data on the biographical data page of the travel document surface,

(b) the printed data in the Machine Readable Zone (MRZ) and

(c) the printed portrait.

(ii) the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO-9303-2006] as specified by ICAO on the contact-based or contactless integrated circuit. It presents contact-based / contactless readable data including (but not limited to) personal data of the travel document holder

(d) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(e) the digitized portraits (EF.DG2),

(d) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both [1]

(g) the other data according to LDS (EF.DG5 to EF.DG16) and

(h) the Document Security Object (SO.D).

The issuing State or Organization implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and Organizational security measures (e.g. control of materials, personalization procedures) [ICAO-9303-2006]. 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

1 These biometric reference data are optional according to [ICAO-9303-2006]. This ST assumes that the issuing State or Organization uses this option and protects these data by means of extended access control.

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-9303-2006], and Password Authenticated Connection Establishment [ICAO-TR-101]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This ST 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 ST addresses the Chip Authentication Version 1 described in [BSI-TR-03110-1-V210] **and** the Active Authentication stated in [ICAO-TR-101].

BAC is supported by the composite product. It is not in the scope of this ST due to the fact that [BSI-CC-PP-0055-110] only considers extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

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)' [BSI-CR-CC-PP-0068-V2-2011]. Note that [BSI-CR-CC-PP-0068-V2-2011] considers high attack potential.

For the PACE protocol according to [ICAO-TR-101], the following steps shall be performed:

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

(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.

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

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

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [BSI-TR-03110-1-V210], [ICAO-TR-101].

The TOE implements the Extended Access Control [2] as defined in [BSI-TR-03110-1-V210]. The Extended Access Control consists of two parts

(i) the Chip Authentication Protocol Version 1 (v.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

2 more exactly "Extended Access Control Version 1.0"

(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.

Optionally the TOE implements Active Authentication (AA) according to [ICAO-9303-2006] part 1 vol. 2 NORMATIVE APPENDIX 4 using ECDSA or RSA for those terminals not able to perform EAC. (see also notes (1), (2), (3) and (4) below)

Notes:

1. PP [BSI-PP-0056-V2-2012-132] addresses the Chip Authentication Version 1 described in [BSI-TR-03110-1-V210] as an alternative to the Active Authentication stated in [ICAO-TR-101].
2. This ST refines PP [BSI-PP-0056-V2-2012-132] and adresses the Chip Authentication Version 1 described in [BSI-TR-03110-1-V210] **and** optionally the Active Authentication stated in [ICAO-TR-101].
3. Active Authentication is optional because the Active Authentication Public Key data can be stored in DG15 (EF.DG15) or not. If the Active Authentication Public Key data is not stored, Active Authentication is not available and vice versa.
4. Chip Authentication Version 1 protocol and Active Authentication protocol both authenticate the Travel document's Chip to the terminal.
5. A valid TOE uses only EC or only RSA for PACE, CA, TA and AA (if AA is configured). A mixed mode TOE (i.e. PACE, TA, AA with RSA and CA with EC) is **not** valid.

3.4.3 TOE Life-Cycle

The TOE life-cycle is described in terms of the four life-cycle phases. (With respect to the [BSI-CC-PP-0035-2007], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

Phase 1 "Development"

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

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the 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 the IC manufacturer. 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"

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and the the travel document's chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer 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. The IC is securely delivered from the IC manufacturer to the travel document manufacturer.

The IC manufacturer adds the IC Embedded Software in the non-volatile programmable FLASH memories.

(Step4) The travel document manufacturer combines the IC with hardware for the contact-based / contactless interface in the travel document.

(Step5) The travel document manufacturer

(i) creates the ePassport application, and

(ii) equips travel document's chips with pre-personalization Data.

Creation of the application implies:

- the creation of MF and ICAO.DF.

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"

(Step6) The personalization of the travel document includes

(i) the survey of the travel document holders biographical data,

(ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),

(iii) the personalization of the visual readable data onto the physical part of the travel document,

(iv) the writing of the TOE User Data and TSF Data into the logical travel document and

(v) configuration of the TSF.

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-9303-2006] finalizes the personalization of the genuine travel document for the travel document holder. The personalized travel document (together with appropriate guidance for TOE use) is handed over to the travel document holder for operational use.

The TSF data (data created by and for the TOE, that affects the operation of the TOE; cf. [CC-3.1-P1] § 92) comprise (but are not limited to) the Personalization Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key. (cf. Application note 2 of [BSI-PP-0056-V2-2012-132])

This ST distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [ICAO-9303-2006]. This approach allows but does not enforce the separation of these roles. (cf. Application note 3 of [BSI-PP-0056-V2-2012-132])

Phase 4 "Operational Use"

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

This ST considers at least the phases 1 and phase 2 (i.e. Step1 to **Step5**) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. (cf. Application note 4 of [BSI-PP-0056-V2-2012-132])

Note that the personalization process and its environment depends on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) are considered in the product evaluation process under AGD assurance class. Therefore, the Security Target outlines the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

3.4.4 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.

Note:

1. To be able to work as travel document the SCIC on which the TOE bases conforms to ISO 7816 and needs the usual IT environment for such smart cards, i.e. an RF-terminal.

3.4.5 Components of the TOE

The components of the TOE are

1. SLE78CLFX*P (M7892 B11) version M7892 B11
2. Antenna (inlay)
3. CardOS DI V5.3 for 300kByte flash and for 404kByte flash with EC-library version 1.02.013, RSA-library version 1.02.013, Toolbox version 1.02.013 and SHA-2-library v1.01
4. V53DI_ICAO_Package_L and V53DI_ICAO_Package_P (patches which contain amendments to CardOS DI V5.3)
5. Configuration scripts for initialization, for pre-personalization and for personalization
6. CardOS DI V5.3 User's Manual
7. CardOS DI V5.3 Packages & Release Notes
8. CardOS DI V5.3 ICAO Extension Packages & Release Notes
9. Administrator Guidance, User Guidance and ePassport Application description.

Note:

1. The patches are installed before delivery in the sense of CC.

3.4.6 Boundaries of the TOE

3.4.6.1 Physical boundaries

Figure 1 shows the ST scope from the structural perspective. The TOE limit is indicated by a shaded box with the label "TOE". The booklet (with printed MRZ or CAN) is not in the scope of the TOE. The SCIC product must not contain any applications besides the TOE (ePassport Application), e.g. a signature generating application.

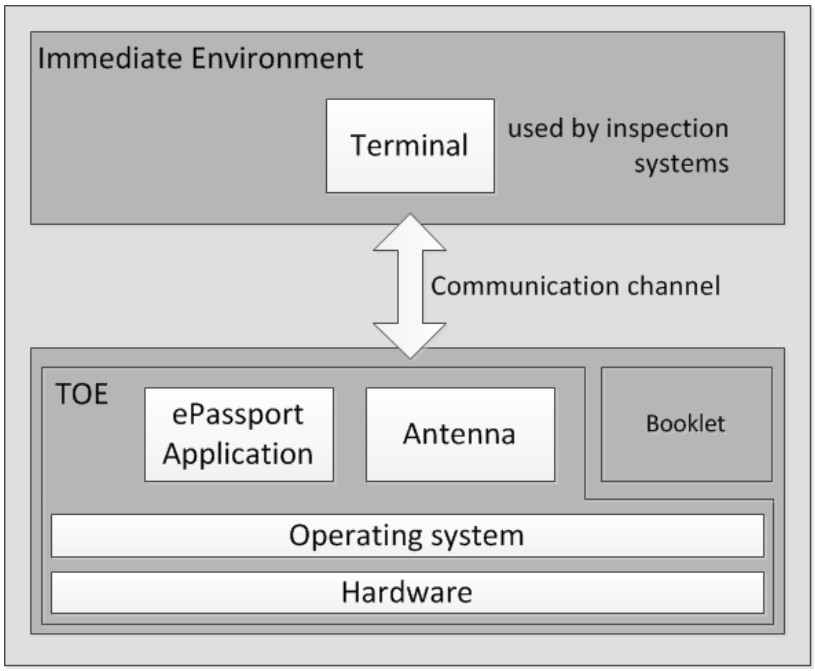

Figure 1: Scope of the MRTD, structural view

3.4.6.2 Logical boundaries

The communication between a terminal and the operating system CardOS DI V5.3 is done via the input and output interface of the operating system CardOS DI V5.3.

The logical boundaries of the TOE are given by all Application Protocol Data Unit (APDU) commands of the operating system CardOS DI V5.3.

An APDU command is received by the operating system CardOS DI V5.3 via its input interface. A Response APDU is sent by of the operating system CardOS DI V5.3 via its output interface.

The APDU commands and the Response APDU are transmitted physically over the the contact-based / contactless hardware interface which are connected to the chip SLE78CLFX*P (M7892 B11). The chip SLE78CLFX*P (M7892 B11) runs the operating system CardOS DI V5.3.

4 Conformance Claims (ASE_CCL)

The TOE is a composite product, as it is based on the Infineon Security Controller SLE78CLFX*P (M7892 B11), which has been evaluated and certified as being conformant to the Common Criteria version 3.1 (R4), CC Part 2 (R4) extended, and CC Part 3 (R4) conformant (cf. [BSI-DSZ-CC-0782-V2-2015]).

As required by [BSI-AIS36-V4], compatibility between this Composite Security Target and the platform Security Target [Infineon-ST-Chip-B11-2015-10-13] and of the Infineon chip SLE78CLFX*P (M7892 B11) is claimed. In chapter

- 9.2 Compatibility between the Composite ST and the Platform-ST

a detailed mapping shows the consistency of this ST and the Platform-ST.

4.1 CC Conformance Claim

This ST claims conformance to the Common Criteria version 3.1 Release 4, cf. [CC-3.1-P1], [CC-3.1-P2], and [CC-3.1-P3].

This ST claims conformance to [CC-3.1-P2] extended due to the use of

- FAU_SAS.1
- FCS_RND.1
- FMT_LIM.1
- FMT_LIM.2
- FPT_EMS.1
- FIA_API.1.

This ST claims conformance to [CC-3.1-P3]; no extended assurance components have been defined.

For the evaluation the following methodology is used:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, cf. [CEM-3.1].

4.2 PP Claim, Package Claim

This Security Target claims strict conformance to the Protection Profiles

- Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP) [BSI-PP-0056-V2-2012-132]
- Machine Readable Travel Document using Standard Inspection Procedure with PACE(PACE PP) [BSI-CC-PP-0068-V2-2011].

The assurance level for the ST is EAL4 augmented. Augmentation results from the selection of:

- ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in CC part 3 [CC-3.1-P3].

Notes:

1. The Protection Profile [BSI-PP-0056-V2-2012-132] has been certified by the Bundesamt fï¿½r Sicherheit in der Informationstechnik (BSI), cf [BSI-CC-PP-0056-V2-2012-MA-02].
2. The Protection Profile [BSI-CC-PP-0068-V2-2011] has been certified by the Bundesamt fï¿½r Sicherheit in der Informationstechnik (BSI), cf [BSI-CR-CC-PP-0068-V2-2011].

4.3 Conformance Rationale

The TOE type is a contactless / contact-based smart card and this type is consistent with the TOE type of the claimed PPs.

The chapter 5 Security Problem Definition (ASE_SPD) is taken over from the claimed PPs without changes.

The chapter 6 Security Objectives (ASE_OBJ) is taken over from the claimed PPs completely and extended by

- OT.AA_Proof Proof of the travel document's chip authenticity
- OE.AA_Key_Travel_Document "Travel document Authentication Key.

The chapter 7 Extended Component Definition (ASE_ECD) is taken over from the claimed PPs without changes

The chapter 8 Security Requirements (ASE_REQ) is taken over from the claimed PPs completely without changes but the the following security requirements

- FCS_CKM.1/CA_EC_KeyPair
- FCS_CKM.1/CA_RSA_KeyPair
- FCS_CKM.1/DH_PACE_RSA
- FCS_CKM.1/CA_RSA

are added and

- FCS_CKM.1/AA_EC_KeyPair
- FCS_CKM.1/AA_RSA_KeyPair
- FCS_COP.1/SIG_VER_RSA
- FCS_COP.1/AA_SGEN_EC
- FCS_COP.1/AA_SGEN_RSA
- FIA_API.1/AA

are added due to the fact that Active Authentication is introduced as an optional mechanism.

4.3.1 PP Claims Rationale for the OTs and OEs added to content of the PPs

With OT.AA_Proof Proof of the travel document's chip authenticity the Active Authentication functionality is introduced to this ST.

Active Authentication is a challenge-response protocol:

- the terminal sends a system challenge to the chip
- the chips sends a signature of this nonce to the terminal
- and the terminal verifies this signature.

Active Authentication prevents cloning of the chip and is an alternative to Chip Authentication which performs a public key exchange for the same purpose. The keys used for Active Authentication are different from the keys used by Chip Authentication.

Active Authentication may be performed if EAC can not be performed by the terminal.

With OE.AA_Key_Travel_Document Travel document Authentication Key the issuing State or Organization has to establish the necessary public key infrastructure to make the Active Authentication functionality possible.

Conclusion:

- The OT added to content of the PPs in the ST do not change the statement of Security Objectives of the PPs
- The statement of Security Objectives in this ST remains consistent with the statement of Security Objectives in the PPs.

4.3.2 PP Claims Rationale for the SFR added to content of the PPs

4.3.2.1 FCS_CKM.1/CA_EC_KeyPair

The SFR FCS_CKM.1/CA_EC_KeyPair is not iterated from a PP SFR.

The SFR introduces functionality to this ST which

- is foreseen in the PP [BSI-PP-0056-V2-2012-132], see application note 44
- and therefore does not affect the functionality as described by the statement of SFRs of the PP [BSI-PP-0056-V2-2012-132]
- does not affect the functionality as described by the statement of SFRs of the PP [BSI-CC-PP-0068-V2-2011] because PP [BSI-PP-0056-V2-2012-132] claims strict conformance to the PP [BSI-CC-PP-0068-V2-2011].

Application note 44 of [BSI-PP-0056-V2-2012-132] states:

"... The verb "create" means here that the Chip Authentication Private Key is generated by the TOE itself. In the latter case the ST writer shall include an appropriate instantiation of the component FCS_CKM.1/CA as SFR for this key generation. ..."

Conclusion:

- The SRF added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

4.3.3 FCS_CKM.1/CA_RSA_KeyPair

The SFR FCS_CKM.1/CA_RSA_KeyPair is iterated from FCS_CKM.1/CA_EC_KeyPair.

- adds no new functionality to this TOE
- uses RSA for key generation instead of EC for key generation used by FCS_CKM.1/CA_EC_KeyPair.

Conclusion:

- The SRF added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

4.3.4 FCS_CKM.1/DH_PACE_RSA

The SFR FCS_CKM.1/DH_PACE_RSA is iterated from FCS_CKM.1/DH_PACE_EC.

The SFR

- adds no new functionality to this TOE
- uses RSA for Diffie-Hellmann instead of ECDH used by FCS_CKM.1/DH_PACE_EC
- derives TDES and AES sessions keys with same bit lengths as FCS_CKM.1/DH_PACE_EC
- uses the same cryptographic primitives for the session keys as FCS_CKM.1/DH_PACE_EC
- uses the same SFR to clear the derived session keys as FCS_CKM.1/DH_PACE_EC.

Conclusion:

- The SRF added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

4.3.5 FCS_CKM.1/CA_RSA

The SFR FCS_CKM.1/CA_RSA is iterated from FCS_CKM.1/CA_EC.

The SFR

- adds no new functionality to this TOE

- uses RSA for Diffie-Hellmann instead of ECDH used by FCS_CKM.1/CA_EC
- derives TDES and AES sessions keys with same bit lengths as FCS_CKM.1/CA_EC
- uses the same cryptographic primitives for the session keys as FCS_CKM.1/CA_EC
- uses the same SFR to clear the derived session keys as FCS_CKM.1/CA_EC.

Conclusion:

- The SRF added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

4.3.6 FCS_CKM.1/AA_EC_KeyPair

The SFR FCS_CKM.1/AA_EC_KeyPair is not iterated from a PP SFR.

The SFR introduces functionality to this ST which

- adds the key generation functionality for Active Authentication to this TOE
- Active Authentication is an alternative mechanism to Chip Authentication
- works with its own key pair which is different from the CA key pair
- is used only if a terminal is not able to perform EAC after PACE.

Conclusion:

- The SRF added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

4.3.7 FCS_CKM.1/AA_RSA_KeyPair

The SFR FCS_CKM.1/AA_RSA_KeyPair is not iterated from a PP SFR.

The SFR FCS_CKM.1/AA_RSA_KeyPair is iterated from FCS_CKM.1/AA_EC_KeyPair, see above.

Since this SFR uses RSA cryptography instead of EC cryptography used by FCS_CKM.1/AA_EC_KeyPair the conclusion given for FCS_CKM.1/AA_EC_KeyPair holds also for this SFR.

4.3.8 FCS_COP.1/SIG_VER_RSA

The SFR FCS_COP.1/SIG_VER_RSA is iterated from SFR FCS_COP.1/SIG_VER_EC of [BSI-PP-0056-V2-2012-132].

The SFR introduces no new functionality to this ST

- it uses RSA cryptography instead of EC cryptography used by FCS_COP.1/SIG_VER_EC.

Conclusion:

- The SRF added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

4.3.9 FCS_COP.1/AA_SGEN_EC

The SFR FCS_COP.1/AA_SGEN_EC is not iterated from a PP SFR.

The SFR introduces functionality to this ST which

- adds the signature generation functionality for Active Authentication to this TOE which needs a private key generated by FCS_CKM.1/AA_EC_KeyPair, see above
- Active Authentication is an alternative mechanism to Chip Authentication

- is used only if a terminal is not able to perform EAC after PACE.

Conclusion:

- The SRF added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

4.3.10 FCS_COP.1/AA_SGEN_RSA

The SFR FCS_COP.1/AA_SGEN_RSA is not iterated from a PP SFR.

The SFR FCS_COP.1/AA_SGEN_RSA is iterated from FCS_COP.1/AA_SGEN_EC, see above.

Since this SFR uses RSA cryptography instead of EC cryptography used by FCS_COP.1/AA_SGEN_EC the conclusion given for FCS_COP.1/AA_SGEN_EC holds also for this SFR.

4.3.11 FIA_API.1/AA

The SFR FIA_API.1/AA is iterated from SFR FIA_API.1/CA of [BSI-PP-0056-V2-2012-132].

The SFR introduces functionality to this ST which

- adds the Active Authentication functionality to this TOE
- Active Authentication is a challenge-response protocol (the terminal sends a nonce to the chip, the chips sends a signature of this nonce to the terminal and the terminal verifies this signature)
- works with its own key pair which is different from the CA key pair
- is used only if a terminal is not able to perform EAC after PACE.

Conclusion:

- The SRF added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

5 Security Problem Definition (ASE_SPD)

Notes:

1. **This ST provides Active Authentication as an optional mechanism introduced to provide an alternative to Chip Authentication for those terminals not able to perform EAC.**
2. **There is no need to change the SPD since**
   - **for identifying the chip to the terminal Chip Authentication and Active Authentication are equivalent mechanisms**
   - **those parts taken over from** [BSI-PP-0056-V2-2012-132] **consider already the Chip Authentication mechanism**. [3]

5.1 Introduction

5.1.1 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 from the claimed PACE PP [BSI-CR-CC-PP-0068-V2-2011], chap 3.1.

The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in chapter 2.4 Terms and Definitions for the term definitions) are listed in the following table.

Table 1: Primary assets

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
1	user data stored on the TOE	All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [ICAO-TR-101] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-101]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [BSI-CC-PP-0055-110].	Confidentiality [4] Integrity Authenticity
2	user data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE)	All data (being not authentication data) being transferred in the context of the ePassport application of the travel document as defined in [ICAO-TR-101] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-101]). User data can be received and sent (exchange <=> {receive, send}).	Confidentiality [5] Integrity Authenticity
3	travel document	Technical information about the current and previous	unavailability [6]

3 REFINEMENT

4 Though not each data element stored on the TOE represents a secret, the specification [ICAO-TR-101] anyway requires securing their confidentiality: only terminals authenticated according to [ICAO-TR-101] can get access to the user data stored. They have to be operated according to P.Terminal.

5 Though not each data element being transferred represents a secret, the specification [ICAO-TR-101] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [ICAO-TR-101].

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
	tracing data	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.	
4	Logical document sensitive User Data	Sensitive biometric reference data (EF.DG3, EF.DG4) Application note 5 of PP [BSI-PP-0056-V2-2012-132]: Due to interoperability reasons the 'ICAO Doc 9303' [ICAO-9303-2006] 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 the document data DG1, DG2, DG5 to DG16 are accessed using BAC [ICAO-9303-2006] [7].	Confidentiality Integrity Authenticity
5	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.	Authenticity

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

The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

Table 2: Secondary assets

Object No.	Asset	Definition	Property to be maintained by the current security policy
6	Accessibility to the TOE functions and data only for authorized subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.	Availability
7	Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD's chip' in [BSI-CC-PP-0055-110].	Availability
8	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
9	TOE internal non-	Permanently or temporarily stored non-secret	Integrity

6 represents a prerequisite for anonymity of the travel document holder.
7 Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [BSI-CC-PP-0055-110]).
If supported, it is therefore recommended to used 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.

Object No.	Asset	Definition	Property to be maintained by the current security policy
	secret cryptographic material	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.	Authenticity
10	travel document communication establishment authorization data	Restricted-revealable [8] 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.	Confidentiality Integrity

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

5.1.2 Subjects and external entities

This ST considers the following external entities and subjects:

Please note, that the table Table 3: Subjects and external entities defines external entities and subjects in the sense of [CC-3.1-P1]. Subjects can be recognized by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates -for each of the respective external entity- an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC-3.1-P1]). From this point of view, the TOE itself perceives only 'subjects' and, for them, does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognized by the TOE.

Table 3: Subjects and external entities

External Entity No.	Subject No.	Role	Definition
1	1	travel document holder	A person for whom the travel document Issuer has personalized the travel document [9]. This entity is commensurate with 'MRTD Holder' in [BSI-CC-PP-0055-110]. Please note that a travel document holder can also be an attacker (s. below).
2	-	travel document presenter (traveler)	A person presenting the travel document to a terminal [10] and claiming the identity of the travel document holder. This external entity is commensurate with 'traveler' in [BSI-CC-PP-0055-110]. Please note that a travel document presenter can also be an attacker (s. below).
3	2	Terminal	A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface. The role 'Terminal' is the default role for any terminal being recognized by the TOE as not being PACE authenticated ('Terminal' is used by the

8 The travel document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorized person or device who definitely act according to respective regulations and are trustworthy.
9 i.e. this person is uniquely associated with a concrete electronic Passport
10 in the sense of [ICAO-TR-101]

External Entity No.	Subject No.	Role	Definition
			travel document presenter. This entity is commensurate with 'Terminal' in [BSI-CC-PP-0055-110].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority [11] and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.
5	-	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 (CDS), see [ICAO-9303-2006]. This role is usually delegated to a Personalization Agent.
6	-	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 (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO-9303-2006], 5.5.1.
7	4	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 [ICAO-9303-2006], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303-2006] (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 [BSI-CC-PP-0055-110].
8	5	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

11 concretely, by a control officer

External Entity No.	Subject No.	Role	Definition
			between the IC Manufacturer and Travel Document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [BSI-CC-PP-0055-110].
9	-	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.
10	-	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.
11	6	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. The Extended Inspection System (EIS) performs the Advanced Inspection Procedure (figure 1) 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-V210] 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. Application note 6 of PP [BSI-PP-0056-V2-2012-132]: For definition of Basic Inspection System (BIS) resp. Basic Inspection System with PACE (BIS-PACE) see PACE PP [BSI-CR-CC-PP-0068-V2-2011].
12	-	Attacker	AA threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, (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. 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. Application note 7 of PP [BSI-PP-0056-V2-2012-132]: An impostor is

External Entity No.	Subject No.	Role	Definition
			attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged travel document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

Figure 3: Advanced Inspection Procedure

5.2 Assumptions

This ST includes the assumption from the PACE PP [BSI-CC-PP-0068-V2-2011], chapter 3.4:

- A.Passive_Auth.

5.2.1 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-9303-2006] and/or BAC [BSI-CC-PP-0055-110].

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. 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 the Inspection Systems implements Active Authentication.** [12]

Note:

1. The assumption A.Insp_Sys does not confine the security objectives of the [BSI-CC-PP-0068-V2-2011] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality **and Active Authentication functionality** [13] of the TOE.

5.2.2 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.

Note:

1. 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 [BSI-CC-PP-0068-V2-2011] 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.

12 REFINEMENT
13 REFINEMENT

5.2.3 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-9303-2006].

5.3 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.

This ST includes all threats from the PACE PP [BSI-CC-PP-0068-V2-2011]:

- T.Skimming,
- T.Eavesdropping,
- T.Tracing,
- T.Abuse-Func,
- T.Information_Leakage,
- T.Phys-Tamper,
- T.Forgery
- T.Malfunction.

The application notes for the threats from the PACE PP [BSI-CC-PP-0068-V2-2011]_are also included. The numbers of these application notes are the numbers of [BSI-CC-PP-0068-V2-2011].

5.3.1 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 (cf. [BSI-CC-PP-0055-110]) 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).

5.3.2 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.

5.3.3 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.

Notes:

1. This TOE does not support BAC.
2. A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST. (cf. application note 10 of [BSI-CC-PP-0068-V2-2011]).
3. MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder. (cf. application note 11 of [BSI-CC-PP-0068-V2-2011]).

5.3.4 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.

Notes:

1. This TOE does not support BAC.
2. A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST (cf. application note 12 of [BSI-CC-PP-0068-V2-2011]).

5.3.5 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

Notes:

1. This threat completely covers and extends "T.Chip-ID" from BAC PP [BSI-CC-PP-0055-110]. (cf. application note 13 of [BSI-CC-PP-0068-V2-2011]).
2. A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this ST. (cf. application note 14 of [BSI-CC-PP-0068-V2-2011]).

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

5.3.6 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

(i) the PACE authenticated BIS-PACE or

(ii) the authenticated Extended Inspection System [14]

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.

14 T.Forgery is extended by (ii) due to PP [BSI-PP-0056-V2-2012-132] Application note 8.

5.3.7 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

1. to manipulate or to disclose the *User Data stored in the TOE*,
2. to manipulate or to disclose the *TSF-data stored in the TOE* or
3. 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:

1. 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 (cf. application note 16 of [BSI-CC-PP-0068-V2-2011]).

5.3.8 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:

1. 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). (cf. application note 17 of [BSI-CC-PP-0068-V2-2011]).

5.3.9 T.Phys-Tamper Physical Tampering

Adverse action:

An attacker may perform physical probing of the travel document in order

1. to disclose the TSF-data, or
2. to disclose/reconstruct the TOE's Embedded Software.

An attacker may physically modify the travel document in order to alter

1. its security functionality (hardware and software part, as well),

2. 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:

1. 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. (cf. application note 18 of [BSI-CC-PP-0068-V2-2011]).

5.3.10 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

1. deactivate or modify security features or functionality of the TOE's hardware or to
2. 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:

1. 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. (cf. application note 19 of [BSI-CC-PP-0068-V2-2011]).

5.4 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-3.1-P1], sec. 3.2).

This PP includes all OSPs from the PACE PP [BSI-CC-PP-0068-V2-2011], chapter 3.3:

- P.Pre-Operational,
- P.Card_PKI,
- P.Trustworthy_PKI,
- P.Manufact

- P.Terminal.

5.4.1 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.

5.4.2 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.

5.4.3 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.

Note:

1. OSP P.Manufact covers OSP "P.Process-TOE" of [Infineon-ST-Chip-B11-2015-10-13] which inherits OSP "P.Process-TOE" from PP [BSI-CC-PP-0035-2007].

5.4.4 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, see Table 1: Primary assets and Table 2: Secondary assets.
3. The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. 3.4.3 TOE Life-Cycle above.
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.

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

Note:

1. 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. (cf. application note 20 of [BSI-CC-PP-0068-V2-2011]).

1. The travel document Issuer shall establish a public key infrastructure for the passive

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

2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the

   CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [ICAO-9303-2006], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [ICAO-9303-2006], 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.

5.4.6 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.

5.4.7 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-9303-2006].
2. They shall implement the terminal parts of the PACE protocol [ICAO-TR-101], of the Passive Authentication [ICAO-9303-2006] and use them in this order [15]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [ICAO-9303-2006]).
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.

Note:

1. **REFINEMENT P.Terminal holds also for Extended Inspection System with PACE**.

15 This order is commensurate with [ICAO-TR-101].

6 Security Objectives (ASE_OBJ)

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.

6.1 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.

This PP includes all Security Objectives for the TOE from the PACE PP [BSI-CR-CC-PP-0068-V2-2011], chapter 4.1:

- OT.Data_Integrity,
- OT.Data_Authenticity,
- OT.Data_Confidentiality,
- OT.Tracing,
- OT.Prot_Abuse-Func,
- OT.Prof_Inf_Leak,
- OT.Prot_Phys-Tamper,
- OT.Identification,
- OT.AC_Pers and
- OT.Prot_Malfunction.

6.1.1 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.

6.1.2 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-V210]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Note:

1. The OT.Chip_Auth_Proof implies the travel document's chip to have
   i. a unique identity as given by the travel document's Document Number,
   ii. a secret to prove its identity by knowledge i.e. a private authentication key as TSF data.
   The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by
   i. the Chip Authentication Public Key (EF.DG14) in the LDS defined in [ICAO-9303-2006] and
   ii. the hash value of DG14 in the Document Security Object signed by the Document Signer.

6.1.3 OT.AA_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 Active Authentication as defined in [ICAO-9303-2006]. **The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.** [16]

6.1.4 OT.Data_Integrity Integrity of Data

The TOE must ensure integrity of the User Data and the TSF-data [17] 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.

Note:

1. **REFINEMENT OT.Data_Integrity holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication**.

6.1.5 OT.Data_Authenticity Authenticity of Data

The TOE must ensure authenticity of the User Data and the TSF-data [18] stored on it by enabling verification of their authenticity at the terminal-side [19]. 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) [20].

Note:

1. **REFINEMENT OT.Data_Authenticity holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication**.

6.1.6 OT.Data_Confidentiality Confidentiality of Data

The TOE must ensure confidentiality of the User Data and the TSF-data [21] 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.

Note:

1. **REFINEMENT OT.Data_Confidentiality holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication**.

6.1.7 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.

Note:

1. Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity) cannot be achieved by the current TOE. (cf. application note 21 of [BSI-CC-PP-0068-V2-2011]).

16 REFINEMENT
17 where appropriate, see Table 2: Secondary assets above
18 where appropriate, see Table 2: Secondary assets above
19 verification of SO.D
20 secure messaging after the PACE authentication, see also [ICAO-TR-101]
21 where appropriate, see Table 2: Secondary assets above

6.1.8 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

1. to manipulate or to disclose the User Data stored in the TOE,
2. to manipulate or to disclose the TSF-data stored in the TOE,
3. to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

6.1.9 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:

1. This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker (cf. application note 2 of [BSI-CC-PP-0068-V2-2011]).

6.1.10 OT.Prot_Phys-Tamper Protection against Physical Tampering

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

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

with a prior

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

6.1.11 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.

6.1.12 OT.Identification Identification of the TOE

The TOE must provide means to store Initialization [22] and Pre-Personalization Data in its non-volatile memory. The Initialization Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).

22 amongst other, IC Identification data

6.1.13 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-9303-2006] 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.

Note:

1. The OT.AC_Pers implies that the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalization. (cf. application note 23 of [BSI-CC-PP-0068-V2-2011]).

6.2 Security Objectives for the Operational Environment

This St includes all Security Objectives of the TOE environment from the PACE PP [BSI-CR-CC-PP-0068-V2-2011], chap. 4.2, namely OE.Legislative_Compliance, OE.Passive_Auth_Sign, OE.Personalization, OE.Terminal, and OE.Travel_Document_Holder.

6.2.1 Issuing State or Organization

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

6.2.1.1 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

1. generate the travel document's Authentication Key Pair,
2. sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and
3. 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.

6.2.1.2 OE.AA_Key_Travel_Document Travel document Authentication Key

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

1. **generate the travel document's Active Authentication Key Pair,**
2. **sign and store the Active Authentication Public Key data in EF.DG15 and**
3. **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 Active Authentication Public Key by means of the Document Security Object.** [23]

6.2.1.3 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.

6.2.2 Receiving State or Organization

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

23 REFINEMENT

6.2.2.1 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

1. includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and
2. implements the terminal part of PACE [ICAO-TR-101] and/or the Basic Access Control [ICAO-9303-2006].

Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

Inspection Systems not able to perform EAC perform additionally to these points Active Authentication (if optionally available and the terminal's ability allows to perform AA) to verify the Authenticity of the presented travel document's chip. [24]

6.2.2.2 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.

6.2.2.3 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 themselves 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.

6.2.3 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:

6.2.3.1 OE.Legislative_Compliance Issuing of the travel document

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

6.2.4 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 note 1. in section 5.4.5 P.Card_PKI PKI for Passive Authentication (issuing branch) above):

6.2.4.1 OE.Passive_Auth_Sign Authentication of travel document by Signature

The travel document Issuer has to establish the necessary public key infrastructure as follows:

the CSCA acting on behalf and according to the policy of the travel document Issuer must

1. generate a cryptographically secure CSCA Key Pair,
2. ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and
3. publish the Certificate of the CSCA Public Key (CCSCA).

24 REFINEMENT

Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must

1. generate a cryptographically secure Document Signing Key Pair,
2. ensure the secrecy of the Document Signer Private Key,
3. hand over the Document Signer Public Key to the CSCA for certification,
4. 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-9303-2006]. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO-9303-2006]. 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.

6.2.4.2 OE.Personalization Personalization of travel document

The travel document Issuer must ensure that the Personalization Agents acting on his behalf

1. establish the correct identity of the travel document holder and create the biographical data for the travel document,
2. enrol the biometric reference data of the travel document holder,
3. 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-9303-2006] (see also [ICAO-9303-2006], sec. 10),
4. write the document details data,
5. write the initial TSF data,
6. sign the Document Security Object defined in [ICAO-9303-2006] (in the role of a DS).

6.2.5 Terminal operator: Terminal's receiving branch

6.2.5.1 OE.Terminal Terminal operating

The terminal operators must operate their terminals as follows:

1. The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [ICAO-9303-2006].
2. The related terminals implement the terminal parts of the PACE protocol [ICAO-TR-101], of the Passive Authentication [ICAO-TR-101] (by verification of the signature of the Document Security Object) and use them in this order (This order is commensurate with [ICAO-TR-101]). The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) 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-9303-2006]).
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.

Note:

1. OE.Terminal completely covers and extends
   "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD"

   from BAC PP [BSI-CC-PP-0055-110]. (cf. application note 24 of [BSI-CC-PP-0068-V2-2011]).

6.2.6 Travel document holder Obligations

6.2.6.1 OE.Travel_Document_Holder Travel document holder Obligations

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

6.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for sufficiency and necessity of the objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

Table 4: Security Objective Rationale

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AA_Proof (3)	OT.AC_Pers (1)	OT.Data_Integrity (1)	OT.Data_Authenticity (1)	OT.Datt_Confidentiality (1)	OT.Tracing (1)	OT.Prot_Abuse-Func (1)	OT.Prot_Inf_Leak (1)	OT.Identification (1)	OT.Prot_Phys-Tamper (1)	OT.prot_Malfunction (1)	OE.Auth_Key_Travel_Document	OE.AA_Key_Travel_Document (3)	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Exp_Insp_systems	OE.Personalisation (1)	OE.Passive_Auth_Sign (1)	OE.Terminal (1)	OE.Travel_Document_Holder (1)	OE.Legislative_Compliance (1)
T.Read_Sensitive_Data	x															x			x					
T.Counterfeit		x	x											x	x		x							
T.Skimming (2)					x	x	x																x	
T.Eavesdropping (2)							x																	
T.Tracing (2)								x															x	
T.Tracing (2)									x															
T.Information_Leakage (2)										x														
T.Phys-Tamper (2)												x												
T.Malfunction (2)													x											

T.Forgery (2)				x	x	x			x			x					x			x	x	x		
P.Sensitive_Data	x															x			x				
P.Personalization				x							x									x				
P.Manufact (2)											x													
P.Pre-Operational (2)				x							x									x				x
P.Terminal (2)																	x					x		
P.Card_PKI (2)																					x			
P.Trustworthy_PKI (2)																					x			
A.Insp_Sys															x		x	x						
A.Auth_PKI																x			x					
A.Passive_Auth (2)																	x				x			

Notes:

1. The Objectives marked with "(1)" are included from the claimed PACE-PP [BSI-CR-CC-PP-0068-V2-2011]. They are listed for the complete overview of the security objectives.
2. Threats and assumptions included from the claimed PACE-PP [BSI-CR-CC-PP-0068-V2-2011] are marked "(2)". They are listed for the complete overview of threats and assumptions.
3. **The Objectives marked with "(3)" are introduced due to optional Active Authentication.** [25]

The OSP **P.Personalization** "Personalization of the travel document by issuing State or Organization only" addresses the

i. the enrolment 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 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 Systems2.

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 [BSI-CR-CC-PP-0068-V2-2011]. **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

25 REFINEMENT

reproduction of the genuine travel document's chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** "Travel document Authentication Key". According to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document's chip.

Please note that paragraph "The threat" **T.Counterfeit** ..." **above is copied due to optional Active Authentication because a refined copy can be read easier**.

The threat **T.Counterfeit** "Counterfeit of travel document chip data" addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.AA_Proof** [26] "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing State or Organization. The Public **Active** [27] Authentication Key has to be written into **EF.DG15** [28] and signed by means of Documents Security Objects as demanded by **OE.AA_Key_Travel_Document** [29] "Travel document Authentication Key". According to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" the General Inspection system has to perform the **Active Authentication Protocol** [30] to verify the authenticity of the travel document's chip.

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. Additionally to the security objectives from PACE PP [BSI-CR-CC-PP-0068-V2-2011] which counter this threat, the examination of the presented MRTD passport book according to **OE.Exam_Travel_Document** "Examination of the physical part of the 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 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 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 optional Active Authentication functionality is covered by the security objective for the TOE environment OE.AA_Key_Travel_Document "Travel document Authentication Key"**. [31]

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 [BSI-CR-CC-PP-0068-V2-2011] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_Travel_Document** "Examination of the physical part of the 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.

26 REFINEMENT OT.Chip_Auth_Proof
27 REFINEMENT Chip
28 REFINEMENT EF.DG14
29 OE.Auth_Key_Travel_Document
30 Chip Authentication Protocol Version 1
31 REFINEMENT

7 Extended Component Definition (ASE_ECD)

This ST includes all Extended Component Definitions from the PACE PP [BSI-CR-CC-PP-0068-V2-2011], chap. 5, namely

- FAU_SAS,
- FCS_RND,
- FMT_LIM,
- FPT_EMS.

These definitions are taken over as described in [BSI-CR-CC-PP-0068-V2-2011].

7.1 Definition of the Family FIA_API

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

Note:

1. The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [CC-3.1-P3], chapter "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behaviour

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

Component levelling:

FIA_API Authentication Proof of Identity	1

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1

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

7.2 Definition of the Family FAU_SAS

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

The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behaviour

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

Component levelling

FAU_SAS Audit data storage	1

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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components

Dependencies: No dependencies

FAU_SAS.1.1

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

7.3 Definition of the Family FCS_RND

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

The family 'Generation of random numbers (FCS_RND)' is specified as follows:

FCS_RND Generation of random numbers

Family behaviour

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

Component levelling:

FCS_RND Generation of random numbers	1

FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RND.1.1

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

7.4 Definition of the Family FMT_LIM

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

The family 'Limited capabilities and availability (FMT_LIM)' is specified as follows:

FMT_LIM Limited capabilities and availability

Family behaviour

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

Component levelling:

FMT_LIM Limited capabilities and availability	1
	2

FMT_LIM.1

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

FMT_LIM.2

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1

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

FMT_LIM.2 Limited availability

Hierarchical to:

No other components

Dependencies:

FMT_LIM.1 Limited capabilities

FMT_LIM.2.1

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

Note:

1. The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that
   (i) the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced
   or conversely
   (ii) the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.
   The combination of both the requirements shall enforce the related policy.

7.5 Definition of the Family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [CC-3.1-P3].

The family 'TOE Emanation (FPT_EMS)' is specified as follows:

FPT_EMS TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation	1

FPT_EMS.1 TOE Emanation has two constituents:

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if **FAU_GEN** (Security audit data generation) is included in a PP or ST using FPT_EMS.1.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

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

FPT_EMS.1.2

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

8 Security Requirements (ASE_REQ)

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

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 [CC-3.1-P1] of the CC. 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 by the ST authors is denoted by

- the "new" words in **bold text** and
- a footnote which starts with **Refinement** followed by the "old" words if any.

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 ST authors are denoted as **bold text** and the original text of the component is given by a footnote.

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 ST authors are denoted as **bold text** and the original text of the component is given by a footnote.

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 5 Security Problem Definition (ASE_SPD). Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 2.4 Terms and Definitions 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-3.1-P2]. The operation "load" is synonymous to "import" used in [CC-3.1-P2].

Definition of security attributes:

Table 5: Definition of security attributes

security attribute	values	meaning
Terminal Authentication Status [32]	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-V210]); 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-V210]); 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-V210]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [BSI-TR-03110-1-V210]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1

32 **REFINEMENT** terminal authentication status

security attribute	values	meaning
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [BSI-TR-03110-1-V210])
	DG3 (Fingerprint)	Read access to DG3: (cf. [BSI-TR-03110-1-V210])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [BSI-TR-03110-1-V210])

Notes:

1. Security attribute Terminal Authentication Status is spelled differently in PP [BSI-PP-0056-V2-2012-132], e.g. FDP_ACF.1/TRM spells it Terminal Authentication v.1.
2. Security attribute Terminal Authorization is spelled differently in PP [BSI-PP-0056-V2-2012-132], e.g. FDP_ACF.1/TRM spells it Authorization of the Terminal.
3. These diffent spellings are corrected by refinements to read always Terminal Authentication Status or Terminal Authorization.

The following table provides an overview of the keys and certificates used including further keys and certificates from [BSI-CR-CC-PP-0068-V2-2011].

Note:

1. Where PP [BSI-CR-CC-PP-0068-V2-2011] is more specific than PP [BSI-PP-0056-V2-2012-132] name and data are taken from PP [BSI-CR-CC-PP-0068-V2-2011].

Table 6: Keys and certificates

Name	Data
keys and certificates taken from [BSI-PP-0056-V2-2012-132]	
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material by the TOE in order to enforce its security functionality.
Receiving PKI branch	
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 Certification Authority Public Key (PK.CVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PK.CVCA) as part of the TSF data to verify the Document Verifier Certificates. The PK.CVCA 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. [BSI-TR-03110-1-V210] 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

Name	Data
	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.
Issuing PKI branch	
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/IEC 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.
Session keys	
Chip Authentication Session Keys (CA-K.MAC, CA-K.Enc)	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System as result of the Chip Authentication Protocol Version 1.
keys and certificates taken from [BSI-CR-CC-PP-0068-V2-2011]	
Issuing PKI branch	
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the travel document Issuer signs the Document Signer Public Key Certificate (C.DS) with the Country Signing Certification Authority Private Key (SK.CSCA) and the signature will be verified by receiving terminal with the Country Signing Certification Authority Public Key (PK.CSCA). The CSCA also issues the self-signed CSCA Certificate (CCSCA) to be distributed by strictly secure diplomatic means, see. [ICAO-9303-2006], 5.5.1.
Document Signer Key Pairs and Certificates	The Document Signer Certificate C.DS is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK.DS) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object (SO.D) of the travel document with the Document Signer Private Key (SK.DS) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK.DS).
Session keys	
PACE Session Keys (PACE-K.MAC, PACE-K.Enc)	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or 3DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol, see [ICAO-TR-101].
Ephemeral keys	

Name	Data
PACE authentication ephemeral key pair (ephem-SK.PICC.PACE, ephem-PK.PICC.PACE)	The ephemeral PACE Authentication Key Pair {ephem-SK.PICC.PACE, ephem-PK.PICC-PACE } is used for Key Agreement Protocol: Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 [BSI-TR-03111-V200-ECC], cf. [ICAO-TR-101].
Refinements (cf note 2 below)	
Issuing PKI branch	
Active Authentication Key Pair	The Active Authentication Key Pair (KPr.AA, KPu.AA) are used for Active Authentication Protocol according to [ICAO-9303-2006] part 1 vol. 2 chapter "7.2.2 Inspection process flow" section "Active Authentication (Optional)" using EC or RSA.
Active Authentication Public Key (KPu.AA)	The Active Authentication Public Key (KPu.AA) is stored in the EF.DG15 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 (KPr.AA)	The Active Authentication Private Key (KPr.AA) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

Notes:

1. The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From travel document's point of view the domestic Document Verifier belongs to the issuing State or Organization.
2. With the optional Active Authentication a key pair is stored in the chip.
3. According to OE.AA_Key_Travel_Document the hash value of ACTIVE AUTHENTICATION PUBLIC KEY INFO (cf. [ICAO-9303-2006] part 1 vol.2 chapter NORMATIVE APPENDIX 4) is stored in the Document Security Object (SO.D) for verifying the key using Passive Authentication.

8.1 Security Functional Requirements for the TOE

8.1.1 Overview

In order to give an overview of the security functional requirements in the context of the security services offered by the TOE, the author of the ST defines the security functional groups and allocated the functional requirements described in the following sections to them:

Table 7: Security functional groups vs. SFRs

Security Functional Groups	Security Functional Requirements concerned
Access control to the User Data stored in the TOE	▶ {FDP_ACC.1/TRM, FDP_ACF.1/TRM} Supported by: ▶ FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE)
Secure data exchange between the travel document and the terminal connected	▶ FTP_ITC.1/PACE: trusted channel Supported by: ▶ FCS_COP.1/CA_ENC: encryption/decryption ▶ FCS_COP.1/CA_MAC: MAC generation/verification

Security Functional Groups	Security Functional Requirements concerned
	▶ FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE) ▶ FIA_API.1/CA ▶ FDP_UCT.1/TRM ▶ FDP_UIT.1/TRM
Identification and authentication of users and components	▶ FIA_UID.1/PACE: PACE Identification (PACE authenticated BIS-PACE) ▶ FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE) ▶ FIA_UAU.4/PACE: single-use of authentication data ▶ FIA_UAU.5/PACE: multiple authentication mechanisms ▶ FIA_UAU.6/EAC: Re-authentication of Terminal ▶ FIA_AFL.1/PACE: reaction to unsuccessful authentication attempts for establishing PACE communication using non-blocking authentication and authorization data ▶ FIA_API.1/CA ▶ FIA_API.1/AA
	Supported by: ▶ FCS_CKM.1/DH_PACE_EC **and** FCS_CKM.1/DH_PACE_RSA [33]: PACE authentication (PACE authenticated BIS-PACE) ▶ FCS_CKM.4: session keys destruction (authentication expiration) ▶ FCS_RND.1: random numbers generation ▶ FMT_SMR.1/PACE: security roles definition ▶ FCS_COP.1/SIG_VER_EC or FCS_COP.1/SIG_VER_RSA ▶ FCS_CKM.1/CA_EC or FCS_CKM.1/CA_RSA ▶ FCS_CKM.1/CA_EC_KeyPair or FCS_CKM.1/CA_RSA_KeyPair ▶ FCS_CKM.1/AA_EC_KeyPair or FCS_CKM.1/AA_RSA_KeyPair
Audit	▶ FAU_SAS.1: Audit storage
	Supported by: ▶ FMT_MTD.1/INI_ENA: Writing Initialization and Pre-personalization ▶ FMT_MTD.1/INI_DIS: Disabling access to Initialization and Pre-personalization Data in the operational phase
Management of and access to TSF and TSF-data	▶ The entire class FMT.
	Supported by: ▶ the entire class FIA: user identification /authentication
Accuracy of the TOE security functionality / Self-protection	▶ The entire class FPT. ▶ FDP_RIP.1
	Supported by: ▶ the entire class FMT.

8.1.2 Elliptic curves used

This TOE uses the following elliptic curves:

1. for 224 bits:
   1.a P-224 ([NIST-FIPS-PUB-186-4], chapter D.2.2 "Curve P-224", aka secp224r1)

33 REFINEMENT

1.b brainpoolP224r1 ([RFC-5639-2010-03] chapter 3.3
2. for 256 bits:
   2.a P-256 ([NIST-FIPS-PUB-186-4], chapter D.2.3 "Curve P-256", aka secp256r1)
   2.b brainpoolP256r1 ([RFC-5639-2010-03] chapter 3.4)
3. for 384 bits:
   3.a P-384 ([NIST-FIPS-PUB-186-4], chapter D.2.4 "Curve P-384", aka secp256r1)
   3.b brainpoolP384r1 ([RFC-5639-2010-03] chapter 3.6)
4. for 512 bits:
   brainpoolP512r1 ([RFC-5639-2010-03] chapter 3.7)

Notes:

1. EC curves above are taken from [BSI-TR-03110-3-V211] Table 4: Standardized Domain Parameters.
2. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CLFX*P (M7892 B11).
3. For "ECDH" see [Infineon-ST-Chip-B11-2015-10-13] section "7.1.4.9 Elliptic Curve Diffie-Hellman (ECDH) key agreement".
4. For the "digital signature generation" see [Infineon-ST-Chip-B11-2015-10-13], 8.5.4 Elliptic Curves EC, section "Signature Generation".
5. For the "cryptographic key generation algorithm" see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.8 Elliptic Curve (EC) key generation"
6. For the "digital signature verification" see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.7 Elliptic Curve DSA (ECDSA) operation", section "Signature Verification".

8.1.3 Hash functions implemented

This TOE provides the following hash algorithms

1. SHA-1
2. SHA-{224, 256, 384, 512}.

Notes:

1. The hash algorithm SHA-1 is provided by CardOS DI V5.3 according to [NIST-FIPS-PUB-180-4] section 6.1.
2. This TOE uses for SHA-{256, 512} the SHA crypto library v1.01 of the underlying chip SLE78CLFX*P (M7892 B11). For the hash algorithms SHA-{256, 512} see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.10 SHA-2 Operation".
3. The hash algorithm SHA-224 is provided by CardOS DI V5.3 using a SHA-256 value according to [NIST-FIPS-PUB-180-4] section 6.3.
4. The hash algorithm SHA-384 is provided by CardOS DI V5.3 using a SHA-512 value according to [NIST-FIPS-PUB-180-4] section 6.5.

8.1.4 Class Cryptographic support (FCS)

8.1.4.1 FCS_CKM.1/CA_EC Cryptographic key generation - EC 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_EC

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH** [34] and specified cryptographic key sizes **112 bits (for TDES) and 128, 192, 256 bits (for AES)** [35] that meet the following:

(1) **based on an ECDH protocol compliant to** [BSI-TR-03111-V200-ECC]

34 [assignment: cryptographic key generation algorithm]
35 [assignment: cryptographic key sizes]

using curves

(2) **see section** 8.1.2 Elliptic curves used. [36]

Notes:

1. FCS_CKM.1/CA_EC implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [BSI-TR-03110-1-V210], section 3.1.
2. The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [BSI-TR-03110-1-V210] chapter "3.4 Chip Authentication Version 1". The protocol used by this TOE bases on the Diffie-Hellman-Protocol compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [BSI-TR-03111-V200-ECC], for details). The shared secret value is used to derive the Chip Authentication Session Keys (CA-K.MAC, CA-K.Enc) used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [BSI-TR-03110-1-V210]).
3. The TOE implements the hash function SHA-1 and SHA-256 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms according to [BSI-TR-03110-3-V211] chapter "A.2.3.1. DES" and "A.2.3.2. AES".
4. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011] 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 destroys the PACE Session Keys after generation of a Chip Authentication Session Keys and changes the secure messaging to the Chip Authentication Session Keys. (iv) The TOE clears 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_EC.
5. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.
6. See also section 8.1.3 Hash functions implemented.

8.1.4.2 FCS_CKM.1/CA_RSA Cryptographic key generation - RSA DH 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_RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **DH** [37] and specified cryptographic key sizes **112 bits (for TDES) and 128, 192, 256 bits (for AES)** [38] that meet the following:

(1) based on the Diffie-Hellman key derivation protocol compliant **to** [RSA-PKCS-3-1993] **and** [BSI-TR-03110-1-V210]. [39]

Notes:

1. FCS_CKM.1/CA_RSA is iterated from FCS_CKM.1/CA_EC.
2. For computing the shared secret the modular exponentation function (cryptorsasignexp) of the RSA crypto library of the Infineon chip SLE78CLFX*P (M7892 B11) is used. Function "cryptorsasignexp" of RSA crypto library is used also for signing.
3. FCS_CKM.1/CA_RSA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [BSI-TR-03110-1-V210], section 3.1.
4. The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [BSI-TR-03110-1-V210] chapter "3.4 Chip Authentication Version 1". The protocol used by this TOE bases on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [RSA-PKCS-3-1993]). The shared secret value is used to derive the Chip Authentication Session Keys (CA-K.MAC, CA-K.Enc) used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [BSI-TR-03110-1-V210]).

36 [selection: based on the Diffie-Hellman key derivation protocol compliant to [12] and [5] , based on an ECDH protocol compliant to [13]]
37 [assignment: cryptographic key generation algorithm]
38 [assignment: cryptographic key sizes]
39 [selection: based on the Diffie-Hellman key derivation protocol compliant to [12] and [5] , based on an ECDH protocol compliant to [13]]

5. The TOE implements the hash function SHA-1 and SHA-256 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms according to [BSI-TR-03110-3-V211] chapter "A.2.3.1. DES" and "A.2.3.2. AES".
6. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011] 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 destroys the PACE Session Keys after generation of a Chip Authentication Session Keys and changes the secure messaging to the Chip Authentication Session Keys. (iv) The TOE clears 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_RSA.
7. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.
8. See also section 8.1.3 Hash functions implemented.

8.1.4.3 FCS_CKM.1/DH_PACE_EC Cryptographic key generation - EC 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_EC

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to [BSI-TR-03111-V200-ECC]** [40] and specified cryptographic key sizes **112 bits (for TDES) and 128, 192, 256 bits (for AES)** [41] that meet the following:

(1) [ICAO-TR-101]

using curves

(2) **see section** 8.1.2 Elliptic curves used. [42]

Notes:

1. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.
2. The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO-TR-101]. 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-TR-101] for the TSF required by FCS_COP.1/PACE_ENC (see FCS_COP.1/CA_ENC Note 5) and FCS_COP.1/PACE_MAC (see FCS_COP.1/CA_MAC Note 5).
3. FCS_CKM.1/DH_PACE_EC implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO-TR-101].
4. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011] after
   i. detection of an error in a received command by verification of the MAC and
   ii. The TOE clears 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.
5. See also section 8.1.3 Hash functions implemented.
6. If a configuration of the TOE uses FCS_CKM.1/DH_PACE_RSA for PACE seesion key, it must not use this SFR additionally.

40 [selection: Diffie- Hellman-Protocol compliant to PKCS#3, ECDH compliant to [BSI-TR-03111-V200-ECC]]
41 [assignment: cryptographic key sizes]
42 REFINEMENT

8.1.4.4 FCS_CKM.1/DH_PACE_RSA Cryptographic key generation - RSA 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_RSA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Diffie- Hellman-Protocol compliant to PKCS#3** [43] and specified cryptographic key sizes **112 bits (for TDES) and 128, 192, 256 bits (for AES)** [44] that meet the following:

(1) [ICAO-TR-101] (section 4.1 Key Agreement Algorithms, table 2)

using bit lengths

(2) **(p component) 1024 and q component with 160 bits**

(3) **(p component) 2048 and q component with 224 bits**

(4) **(p component) 2048 and q component with 256 bits**. [45]

Notes:

1. FCS_CKM.1/DH_PACE_RSA is iterated from FCS_CKM.1/DH_PACE_EC.
2. For computing the shared secret the modular exponentation function (cryptorsasignexp) of the RSA crypto library of the Infineon chip SLE78CLFX*P (M7892 B11) is used. Function "cryptorsasignexp" of RSA crypto library is used also for signing.
3. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.
4. The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO-TR-101]. 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-TR-101] for the TSF required by FCS_COP.1/PACE_ENC (see FCS_COP.1/CA_ENC Note 5) and FCS_COP.1/PACE_MAC (see FCS_COP.1/CA_MAC Note 5).
5. FCS_CKM.1/DH_PACE_RSA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO-TR-101].
6. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011] after
   i. detection of an error in a received command by verification of the MAC and
   ii. The TOE clears 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.
7. See also section 8.1.3 Hash functions implemented.
8. If a configuration of the TOE uses FCS_CKM.1/DH_PACE_EC for PACE seesion key, it must not use this SFR additionally.

8.1.4.5 FCS_CKM.4 Cryptographic key destruction - Session keys, CA + AA 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_EC **and**

43 [selection: Diffie- Hellman-Protocol compliant to PKCS#3, ECDH compliant to [BSI-TR-03111-V200-ECC]]
44 [assignment: cryptographic key sizes]
45 REFINEMENT

FCS_CKM.1/DH_PACE_RSA [46].

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with zeros** [47] that meets the following: **none** [48].

Note:

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

8.1.4.6 FCS_CKM.1/CA_EC_KeyPair Cryptographic key generation - EC key pair for CA

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_EC_KeyPair

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 15946-1:2002** [49] and specified cryptographic key sizes **224, 256, 384 and 512 bits** [50] that meet the following:

ECDSA Key Generation:

(1) **According to the appendix A4.3 in ANSI X9.62-2005 the cofactor h is not supported.**

(2) **According to section 6.1 (not 6.1.1) in ISO/IEC 15946-1:2002**

using curves

(3) **see section** 8.1.2 Elliptic curves used. [51]

Notes:

1. FCS_CKM.1/CA_EC_KeyPair is added to contents of PPs [BSI-PP-0056-V2-2012-132] and [BSI-CC-PP-0068-V2-2011].
2. With FCS_CKM.1/CA_EC_KeyPair the TOE is able to create an EC key pair for Chip Authentication.
3. With FMT_MTD.1/CA_AA_PK only the Personalization Agent is able to create a key pair.
4. The EC key pair for CA can be generated only once.
5. If a configuration of the TOE uses FCS_CKM.1/CA_RSA_KeyPair for CA key generation, it must not use this SFR additionally.

8.1.4.7 FCS_CKM.1/CA_RSA_KeyPair Cryptographic key generation - RSA key pair for CA

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_RSA_KeyPair

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key

46 REFINEMENT
47 [assignment: cryptographic key destruction method]
48 [assignment: list of standards]
49 [assignment: cryptographic key generation algorithm]
50 [assignment: cryptographic key sizes]
51 [assignment: list of standards]

generation algorithm **RSA key generation** [52] and specified cryptographic key sizes **2048 bits** [53] that meet the following:

According to section 3.2(2) in PKCS v2.1 RFC3447 for u=2, i.e., without any (r_i, d_i, t_i), i > 2. For p x q < 2 power 2048 additionally according to section 3.2(1). [54]

Notes:

1. FCS_CKM.1/CA_RSA_KeyPair is iterated from FCS_CKM.1/CA_EC_KeyPair.
2. With FCS_CKM.1/CA_RSA_KeyPair the TOE is able to create an RSA key pair for Chip Authentication.
3. With FMT_MTD.1/CA_AA_PK only the Personalization Agent is able to create a key pair.
4. The RSA key pair for CA can be generated only once.
5. If a configuration of the TOE uses FCS_CKM.1/CA_EC_KeyPair for CA key generation, it must not use this SFR additionally.

8.1.4.8 FCS_CKM.1/AA_EC_KeyPair Cryptographic key generation - EC key pair for AA

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/AA_EC_KeyPair

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curve EC specified in ANSI X9.62-2005 and ISO/IEC 15946-1:2002** [55] and specified cryptographic key sizes **224, 256, 384 and 512 bits** [56] that meet the following:

ECDSA Key Generation:

(1) **According to the appendix A4.3 in ANSI X9.62-2005 the cofactor h is not supported.**

(2) **According to section 6.1 (not 6.1.1) in ISO/IEC 15946-1:2002**

using curves

(3) **see section** 8.1.2 Elliptic curves used. [57]

Notes:

1. FCS_CKM.1/AA_EC_KeyPair is added to contents of PPs [BSI-PP-0056-V2-2012-132] and [BSI-CC-PP-0068-V2-2011].
2. With FCS_CKM.1/AA_EC_KeyPair the TOE is able to create an EC key pair for Active Authentication.
3. With FMT_MTD.1/CA_AA_PK only the Personalization Agent is able to create a key pair.
4. The EC key pair for AA can be generated only once.
5. If a configuration of the TOE uses FCS_CKM.1/AA_RSA_KeyPair for AA, it must not use this SFR additionally.

8.1.4.9 FCS_CKM.1/AA_RSA_KeyPair Cryptographic key generation - RSA key pair for AA

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/AA_RSA_KeyPair

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key

52 [assignment: cryptographic key generation algorithm]
53 [assignment: cryptographic key sizes]
54 [assignment: list of standards]
55 [assignment: cryptographic key generation algorithm]
56 [assignment: cryptographic key sizes]
57 [assignment: list of standards]

generation algorithm **RSA key generation** [58] and specified cryptographic key sizes **2048 bits** [59] that meet the following:

According to section 3.2(2) in PKCS v2.1 RFC3447 for u=2, i.e., without any (r_i, d_i, t_i), i > 2. For p x q < 2 power 2048 additionally according to section 3.2(1). [60]

Notes:

1. FCS_CKM.1/AA_RSA_KeyPair is iterated from SFR FCS_CKM.1/AA_EC_KeyPair.
2. This TOE uses the RSA key generation provided by the underlying chip SLE78CLFX*P (M7892 B11).
3. For the "RSA key generation" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.5 Rivest-Shamir-Adleman (RSA) key generation.
4. With FCS_CKM.1/AA_RSA_KeyPair the TOE is able to create a RSA key pair for Active Authentication.
5. With FMT_MTD.1/CA_AA_PK only the Personalization Agent is able to create a key pair.
6. The RSA key pair for AA can be generated only once.
7. If a configuration of the TOE uses FCS_CKM.1/AA_EC_KeyPair for AA, it must not use this SFR additionally.

8.1.5 Cryptographic operation (FCS_COP.1)

8.1.5.1 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 TDES in CBC mode** [61] and cryptographic key sizes **using AES with 128, 192, 256 bits and using TDES with 112 bits** [62] that meet the following:

1. **(for CBC:) [NIST-800-38A-2001], chapter 6.2 THE CIPHER BLOCK CHAINING MODE.**
2. **(for TDES:) National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-67, Version 1.1**.
3. **(for AES:) U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197**. [63]

Notes:

1. This TOE uses the Triple-DES provided by the underlying chip SLE78CLFX*P (M7892 B11).
2. For the "secure messaging - encryption and decryption" using TDES see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.2 Triple-DES Operation.
3. This TOE uses the AES provided by the underlying chip SLE78CLFX*P (M7892 B11).
4. For the "Advanced Encryption Standard (AES)" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.3 AES Operation.
5. 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_EC (and FCS_CKM.1/CA_RSA).

58 [assignment: cryptographic key generation algorithm]
59 [assignment: cryptographic key sizes]
60 [assignment: list of standards]
61 [assignment: cryptographic algorithm]
62 [assignment: cryptographic key sizes]
63 [assignment: list of standards]

8.1.5.2 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 **(for TDES) Retail-MAC and (for AES) CMAC** [64] and cryptographic key sizes **using TDES with 112 bits and using AES with 128, 192, 256 bits** [65] that meet the following:

1. **(for Retail-MAC:) [ISO-IEC-9797-1-2011], algorithm 3 and padding method 2**.
2. **(for TDES:) National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-67, Version 1.1**.
3. **(for CMAC:) [ISO-IEC-9797-1-2011], algorithm 5 and padding method 2**.
4. **(for AES:) U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197**. [66]

Notes:

1. This TOE uses the Triple-DES provided by the underlying chip SLE78CLFX*P (M7892 B11).
2. For the "Triple-DES encrypting and decrypting" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.2 Triple-DES Operation.
3. This TOE uses the AES provided by the underlying chip SLE78CLFX*P (M7892 B11).
4. For the "Advanced Encryption Standard (AES)" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.3 AES Operation.
5. This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by PACE Protocol according to the FCS_CKM.1/DH_PACE_EC and FCS_CKM.1/DH_PACE_RSA. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the authentication mechanism.

8.1.5.3 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_EC **and** FCS_CKM.1/DH_PACE_RSA [67]
- 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 a specified cryptographic algorithm **3DES and AES** [68] in CBC mode and cryptographic key sizes **112 (for 3DES) and 128, 192, 256 (for AES)** [69] bit that meet the following:

64 [assignment: cryptographic algorithm]
65 [assignment: cryptographic key sizes]
66 [assignment: list of standards]
67 REFINEMENT
68 [selection: AES, 3DES]
69 [selection: 112, 128, 192, 256]

compliant to [ICAO-TR-101].

Note:

1. This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE_EC (PACE-K.Enc) and FCS_CKM.1/DH_PACE_RSA.

8.1.5.4 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_EC **and** FCS_CKM.1/DH_PACE_RSA [70]
- 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 **(for 3DES) Retail-MAC and for (AES) CMAC** [71] and cryptographic key sizes **112 (for 3DES) and 128, 192, 256 (for AES)** bit that meet the following:

compliant to [ICAO-TR-101].

Note:

1. 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_EC (PACE-K.MAC) and FCS_CKM.1/DH_PACE_RSA. Note that in accordance with [ICAO-TR-101] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

8.1.5.5 FCS_COP.1/SIG_VER_EC Cryptographic operation - Signature verification by travel document with EC

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_EC

The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **ECDSA** [72] and cryptographic key sizes **224, 256, 384 and 512 bits** [73] that meet the following:

1. **According to section 7.4.1 in ANSI X9.62-2005 Not implemented is step b) and c) thereof. The output of step c) has to be provided as input to our function by the caller. Deviation of step d): Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder n to the calculated values u1 and u2.**

70 REFINEMENT
71 [selection: CMAC, Retail-MAC]
72 [selection: 112, 128, 192, 256]
73 [assignment: cryptographic algorithm]

2. **According to sections 6.4 (6.4.1. + 6.4.3 + 6.4.4) in ISO/IEC 15946-2:2002. Not implemented is section 6.4.2: The output of 5.4.2 has to be provided by the caller as input to the function.**

using curves

(3) **see section** 8.1.2 Elliptic curves used. [74]

Note:

1. Due to the fact that there is a SFR added to this ST using RSA for signature verification the SFR "FCS_COP.1/SIG_VER" of [BSI-PP-0056-V2-2012-132] is renamed to "FCS_COP.1/SIG_VER_EC" for mnemonic reason.
2. The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.
3. The TOE implements ECDSA (and RSA cf. FCS_COP.1/SIG_VER_RSA) for the Terminal Authentication Protocol v.1 (cf. [BSI-TR-03110-1-V210] A.6.4.Terminal Authentication with ECDSA).
4. See also section 8.1.3 Hash functions implemented.
5. If a configuration of the TOE uses FCS_COP.1/SIG_VER_RSA, it must not use this SFR additionally.

8.1.5.6 FCS_COP.1/SIG_VER_RSA Cryptographic operation - Signature verification by travel document with RSA

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_RSA

The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **RSA** [75] and cryptographic key sizes **1024, 1280, 1536, 2048 and 3072 bits** [76] (cf. [BSI-TR-03110-3-V211] section A.6.3.2.Public Key Format) that meet the following:

1. **According to section 5.2.2 RSAVP1 in PKCS v2.1 RFC3447.**
2. **Padding according to RSASSA-PSS or**
3. **Padding according to RSASSA-PKCS1-v1_5**. [77]

Notes:

1. SFR FCS_COP.1/SIG_VER_RSA is iterated from PP SFR FCS_COP.1/SIG_VER_EC ("FCS_COP.1/SIG_VER").
2. This TOE uses the RSA (Signature Verification) provided by the underlying chip SLE78CLFX*P (M7892 B11).
3. For the "digital signature verification" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation, section "Signature Verification:".
4. The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge
5. See also section 8.1.3 Hash functions implemented.
6. The bit lengths for TA are taken over from [BSI-TR-03110-3-V211] section A.6.3.2. Public Key Format.
7. The TOE implements RSA (and ECDSA cf. FCS_COP.1/SIG_VER_EC) for the Terminal Authentication Protocol v.1 (cf. [BSI-TR-03110-3-V211] section A.6.3.Terminal Authentication with RSA).
8. If a configuration of the TOE uses FCS_COP.1/SIG_VER_EC, it must not use this SFR additionally.

74 [assignment: cryptographic key sizes]
75 [assignment: list of standards]
76 [assignment: cryptographic algorithm]
77 [assignment: cryptographic key sizes]

8.1.5.7 FCS_COP.1/AA_SGEN_EC Cryptographic operation - Signature generation for AA with EC

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_SGEN_EC

The TSF shall perform **digital signature generation** [78] in accordance with a specified cryptographic algorithm **ECDSA** [79] and cryptographic key sizes **224, 256, 384 and 512 bits** [80] that meet the following:

1. **According to section 7.3 in ANSI X9.62 - 2005 Not implemented is step d) and e) thereof. The output of step e) has to be provided as input to our function by the caller. Deviation of step c) and f): The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.**
2. **According to sections 6.2 (6.2.2. + 6.2.3) in ISO/IEC 15946-2:2002 Not implemented is section 6.2.1: The output of 5.4.2 has to be provided by the caller as input to the function**.

using curves

(3) **see section** 8.1.2 Elliptic curves used. [81]

Notes:

1. SFR FCS_COP.1/AA_SGEN_EC is added to contents of PPs [BSI-PP-0056-V2-2012-132] and [BSI-CC-PP-0068-V2-2011].
2. See also section 8.1.3 Hash functions implemented.
3. The signature generation is used to perform Active Authentication.
4. The TOE implements ECDSA and RSA (cf. FCS_COP.1/AA_SGEN_RSA) for the Active Authentication Protocol (cf. [BSI-TR-03110-3-V211] section 1.2 Active Authentication).
5. If a configuration of the TOE uses FCS_COP.1/AA_SGEN_RSA, it must not use this SFR additionally.

8.1.5.8 FCS_COP.1/AA_SGEN_RSA Cryptographic operation - Signature generation for AA with RSA

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_SGEN_RSA

The TSF shall perform **digital signature generation** [82] in accordance with a specified cryptographic algorithm **RSA** [83] and cryptographic key sizes **2048 bits** [84] that meet the following:

1. **Signature Generation (with or without CRT): According to section 5.2.1 RSASP1 in PKCS v2.1 RFC3447 for u = 2, i.e., without any (r_i, d_i, t_i), i >2, therefore without**

78 [assignment: list of standards]
79 [assignment: list of cryptographic operations]
80 [assignment: cryptographic algorithm]
81 [assignment: cryptographic key sizes]
82 [assignment: list of standards]
83 [assignment: list of cryptographic operations]
84 [assignment: cryptographic algorithm]

5.2.1.2.b (ii)&(v), without 5.2.1.1. 5.2.1.2.a, only supported up to n < 2 power 2048.

2. **Padding according ISO/IEC 9796-2 Digital Signature scheme 1 according to [ICAO-9303-2006]_ part 1 vol 2 section "A4.2 Active Authentication Mechanism"**. [85]

Notes:

1. SFR FCS_COP.1/AA_SGEN_RSA is iterated from SFR FCS_COP.1/AA_SGEN_EC.
2. This TOE uses the RSA (Signature Generation) provided by the underlying chip SLE78CLFX*P (M7892 B11).
3. For the "digital signature generation" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation, section "Signature Generation (with or without CRT):".
4. See also section 8.1.3 Hash functions implemented.
5. The signature generation is used to perform Active Authentication.
6. The TOE implements RSA and ECDSA (cf. FCS_COP.1/AA_SGEN_EC) for the Active Authentication Protocol (cf. [BSI-TR-03110-3-V211] section 1.2 Active Authentication).
7. If a configuration of the TOE uses FCS_COP.1/AA_SGEN_EC, it must not use this SFR additionally.

8.1.6 Random Number Generation (FCS_RND.1)

8.1.6.1 FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1

The TSF shall provide a mechanism to generate random numbers that meet

1. **(for PACE) random numbers generation Class PTG.2 chip according to [BSI-AIS31-V3] additionally processed according to algorithm "Nachbearbeitung bei PACE"** [BSI-TR-03116-2] **section 1.3.3.1**
2. **(for other purposes) random numbers generation Class PTG.2 according to [BSI-AIS31-V3]** [86].

Notes:

1. This TOE uses the random numbers generation provided by the underlying chip SLE78CLFX*P (M7892 B11).
2. For the "random numbers generation Class PTG.2 according to [BSI-AIS31-V3]" see [Infineon-ST-Chip-B11-2015-10-13] "7.1.1.1 FCS_RNG".
3. This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE (1).
4. This SFR requires the TOE to generate random numbers (random nonce) used also for Terminal Authentication Protocol v.1 as required by FIA_UAU.4/PACE (3).

8.1.7 Class FIA Identification and Authentication

The Table 8: Overview on authentication SFR provides an overview on the authentication mechanisms used

Table 8: Overview on authentication SFR

Name	SFR for the TOE
Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE
Chip Authentication Protocol v.1	FIA_API.1/CA FIA_UAU.5/PACE

85 [assignment: cryptographic key sizes]
86 [assignment: list of standards]

Name	SFR for the TOE
	FIA_UAU.6/EAC
Active Authentication Protocol	FIA_API.1/AA FIA_UAU.5/PACE
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol [87]	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_UAU.6/PACE [88] FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE

Note the Chip Authentication Protocol Version 1 as used by this TOE 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.

8.1.7.1 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-TR-101]
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-V210]
5. to carry out the Terminal Authentication Protocol v.1 according to [BSI-TR-03110-1-V210]
6. **to carry out the Active Authentication Protocol according to** [ICAO-TR-101]
7. **to run self tests according to** FPT_TST.1 [89].

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.

87 [assignment: a defined quality metric]
88 Only listed for information purposes
89 not listed in PP [BSI-CC-PP-0056-V2-2012-MA-02]

Notes:

1. The SFR FIA_UID.1/PACE in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.
2. 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-personalisation Data in the audit records of the IC. The travel document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 "Personalisation of the travel document". The users in role Personalisation Agent identify themselves by means of selecting the authentication key. After personalisation 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 Personalisation Agent (using the Personalisation Agent Key).
3. User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).
4. In the life-cycle phase "Manufacturing" the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC.Please note that a Personalisation Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation 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 "Personalisation Agent", when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).
5. See FIA_AFL.1/PACE how skimming is prevented by the TOE.

8.1.7.2 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-TR-101] [90],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to identify themselves by selection of the authentication key
5. to carry out the Chip Authentication Protocol Version 1 according to [BSI-TR-03110-1-V210]
6. to carry out the Terminal Authentication Protocol Version 1 according to [BSI-TR-03110-1-V210]
7. **to carry out the Active Authentication Protocol according to** [ICAO-TR-101]
8. **to run self tests according to** FPT_TST.1 [91]

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.

Notes:

1. The SFR FIA_UID.1/PACE in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.
2. The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither

90 [assignment: list of TSF-mediated actions]
91 travel document identifies itself within the PACE protocol by selection of the authentication key ephem-PK.PICC-PACE

CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorized other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K.MAC, PACE-K.Enc), cf. FTP_ITC.1/PACE.

3. See FIA_AFL.1/PACE how skimming is prevented by the TOE.

8.1.7.3 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-TR-101]
2. Authentication Mechanism based on **TDES and AES** [92]
3. Terminal Authentication Protocol v.1 according to [BSI-TR-03110-1-V210].

Note:

1. The SFR FIA_UAU.4.1/PACE in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011] 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 [BSI-CC-PP-0068-V2-2011].
2. 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 Personalisation Agent relies also on other mechanisms ensuring protection against replay attacks, the use of an internal counter as a diversifier.

8.1.7.4 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-TR-101]
2. Passive Authentication according to [ICAO-9303-2006]
3. Secure messaging in MAC-ENC mode according to [ICAO-TR-101]
4. Symmetric Authentication Mechanism based on **TDES and AES** [93]
5. Terminal Authentication Protocol v.1 according to [BSI-TR-03110-1-V210]
6. **Active Authentication according to** [ICAO-9303-2006] [94]

to support user authentication.

FIA_UAU.5.2/PACE

The TSF shall authenticate any user's claimed identity according to the following rules:

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalization Agent by **the Authentication Mechanism with Personalization Agent Key(s)** [95].
3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.

92 [assignment: list of TSF-mediated actions]
93 [selection: Triple- DES, AES or other approved algorithms]
94 REFINEMENT
95 [selection: Triple-DES, AES or other approved algorithms]

4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1.
5. **none**. [96]

Note:

1. The SFR FIA_UAU.5.1/PACE in the current ST covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in the current ST covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

8.1.7.5 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:

1. The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO-9303-2006] 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.

8.1.7.6 FIA_UAU.6/PACE 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:

1. The PACE protocol specified in [ICAO-TR-101] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

8.1.7.7 FIA_API.1/CA Authentication Proof of Identity by Chip Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CA

The TSF shall provide a Chip Authentication Protocol Version 1 according to [BSI-TR-03110-1-

96 [selection: the Authentication Mechanism with Personalization Agent Key(s)]

V210] to prove the identity of the TOE.

Note:

1. Due to the fact that there is a SFR added to this ST using AA for Authentication Proof of Identity the SFR "FIA_API.1" of [BSI-PP-0056-V2-2012-132] is renamed to "FIA_API.1/CA" for mnemonic reason.
2. This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [BSI-TR-03110-1-V210]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (ECDH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO-9303-2006].
   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).

8.1.7.8 FIA_API.1/AA Authentication Proof of Identity by Active Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA

The TSF shall provide a Active Authentication Protocol according to [ICAO-9303-2006] part 1 vol. 2 NORMATIVE APPENDIX 4 to prove the identity of the TOE.

Note:

1. SFR FIA_API.1/AA is iterated from PP SFR FIA_API.1/CA ("FIA_API.1").
2. This SFR requires the TOE to implement the Active Authentication Mechanism specified in [ICAO-9303-2006]. The TOE computes a signature over a nonce received from the terminal, sends the signature to the terminal and the terminal verifies the signature.

8.1.7.9 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** [97] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.

FIA_AFL.1.2/PACE

When the defined number of unsuccessful authentication attempts has been met, the TSF shall **delay the next authentication attempt at least 6 seconds**. [98]

Notes:

1. With a delay at least 6 seconds a brute force attack lasts in the average more than 30 days even if the password consist only of 6 digits (e.g. the CAN might be so long and consists of digits only).
   The delay applies also when a new session is restarted.
   The MRZ is longer than 6 signs and consists of alpha numerical characters.

8.1.8 Class FDP User Data Protection

97 [assignment: rules describing how the multiple authentication mechanisms provide authentication]
98 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

8.1.8.1 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:

1. The SFR FDP_ACC.1.1/TRM in the current ST covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] 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.

8.1.8.2 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 Status** [99]
   c. **Terminal Authorization**. [100]

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.1.1/TRM according to [ICAO-TR-101] 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.

99 [assignment: list of actions]
100 **REFINEMENT** Terminal Authentication v.1

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

Notes:

1. The SFR FDP_ACF.1.1/TRM in the current ST covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in the current ST cover the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011]. The SFR FDP_ACF.1.4/TRM in the current ST covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] and extends it by 3) to 6). These extensions do not conflict with the strict conformance to PACE PP.
2. The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [BSI-TR-03110-1-V210]. 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.
3. Please note that the Document Security Object (SO.D) stored in EF.SOD (see [ICAO-9303-2006]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [ICAO-TR-101].
4. 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).
5. Reading according to FDP_ACF.1.2/TRM includes for a TOE providing Active Authentication the AA public key in EF.DG15.

8.1.8.3 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** [101] 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),
3. **none**. [102]

Note:

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

101 **REFINEMENT** Authorization of the Terminal
102 [selection: allocation of the resource to, deallocation of the resource from]

8.1.8.4 FDP_UCT.1/TRM Basic data exchange confidentiality - MRTD

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_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.

8.1.8.5 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.

8.1.9 Class FTP Trusted Path/Channels

8.1.9.1 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 enforce communication via the trusted channel for any data exchange between the

TOE and the Terminal.

Notes:

1. The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word "initiate" is changed to "enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.
2. The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K.MAC, PACE-K.Enc):
   This secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.
3. Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM
4. If Chip Authentication is successfully performed, secure messaging is immediately started using the derived session keys (CA-K.MAC, CA-K.Enc):
   this secure messaging enforces preventing tracing while the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC.
5. If first PACE session keys are used for establishing the trusted channel and afterward a Chip Authentication is successfully performed, the sessions keys of the CA are used only for the trusted channel (the PACE session keys are not longer used).

8.1.10 Class FAU Security Audit

8.1.10.1 FAU_SAS.1 Audit storage

Hierarchical to: No other components. Dependencies: No dependencies.

FAU_SAS.1.1

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

Note:

1. 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.

8.1.11 Class FMT Security Management

Note:

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

8.1.11.1 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:

1. The SFR FMT_SMR.1.1/PACE in the current ST covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

Note:

1. 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.

8.1.11.2 FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1

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

Deploying Test Features after TOE Delivery does not allow,

1. User Data to be manipulated and disclosed,
2. TSF data to be 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.

8.1.11.3 FMT_LIM.2 Limited availability

Hierarchical to: No other components

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1

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

Deploying Test Features after TOE Delivery does not allow:

1. User Data to be manipulated and disclosed,
2. TSF data to be 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.

Notes:

1. The formulation of "Deploying Test Features ..." in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to

enforce the same policy.
2. Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Note:

1. 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.

8.1.11.4 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: PK.CVCA,
2. initial Country Verifying Certification Authority Certificate: C.CVCA,
3. initial Current Date,
4. **none** [103]

to **Personalization Agent** [104].

Note:

1. The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

8.1.11.5 FMT_MTD.1/CVCA_UPD Management of TSF data - Country Verifying 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: PK.CVCA,
2. Country Verifying Certification Authority Certificate: C.CVCA

to Country Verifying Certification Authority.

Note:

1. 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-V210]). 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-V210]).

8.1.11.6 FMT_MTD.1/DATE Management of TSF data - Current date

Hierarchical to: No other components.

103 [assignment: list of objects]
104 [assignment: list of TSF data]

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:

1. The authorized roles are identified in their certificate (cf. [BSI-TR-03110-1-V210]) 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-V210]).

8.1.11.7 FMT_MTD.1/CA_AA_PK Management of TSF data - CA and AA Private Key

Hierarchical to: No other components.

Dependencies:

- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles

FMT_MTD.1.1/CA_AA_PK

The TSF shall restrict the ability to **create or load** [105] the Chip Authentication Private Key **and Active Authentication Private Key** [106] to **Personalization Agent** [107].

Note:

1. Due to the fact that this SFR is refined with Active Authenticationthe SFR "FMT_MTD.1/CAPK" of [BSI-PP-0056-V2-2012-132] is renamed to "FMT_MTD.1/CA_AA_PK".
2. The verb "load" means here that the Chip Authentication Private Key and the Active Authenticateion Private Key are generated securely outside the TOE and written into the TOE memory. The verb "create" means here that the Chip Authentication Private Key and Active Authenticateion Private Key is generated by the TOE itself.
3. This TOE is able to generate the Chip Authentication Private Key, see FCS_CKM.1/CA_EC_KeyPair or FCS_CKM.1/CA_RSA_KeyPair.
4. This TOE is able to generate the Active Authentication Private Key, see FCS_CKM.1/AA_EC_KeyPair and FCS_CKM.1/AA_RSA_KeyPair.

8.1.11.8 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
4. **Active Authentication Private Key** [108]

to none.

105 [assignment: the authorized identified roles]
106 [selection: create, load]
107 REFINEMENT
108 [assignment: the authorized identified roles]

Note:

1. The SFR FMT_MTD.1/KEY_READ in the current ST covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.

8.1.11.9 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:

1. 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.

8.1.11.10 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

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

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

Notes:

1. For "configuration" see chapter 3.4.3 TOE Life-Cycle section "Phase 3 "Personalization of the travel document" step (v).

8.1.11.11 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.

8.1.11.12 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 the Personalization Agent.

Note:

1. The TOE restricts the ability to write the Initialization Data and the Pre-personalization Data by
   i. allowing writing these data only once and
   ii. blocking the role Manufacturer at the end of the manufacturing phase.
   The Manufacturer writes the Initialization Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'OPERATIONAL'. Therefore, read and use access to the Initialization Data and Pre-personalization Data is blocked by the Personalization Agent, before the card is handed out to the travel document holder.
2. With "(i) allowing writing these data only once" the TOE allows to write the Initialization Data and Pre-personalization Data in more than one session but each data only once.

8.1.11.13 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 the Document Security Object (SO.D) to the Personalization Agent.

Note:

1. By writing SO.D into the TOE, the Personalization Agent confirms (on behalf of DS) the correctness and genuineness of all the personalization data related. This consists of user -and TSF- data.

8.1.12 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for 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 TOE functions.

8.1.12.1 FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMS.1.1

The TOE shall not emit

shape and amplitude of signals

time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines

during internal operations or data transmissions [109]

in excess of **unintelligible limits** [110] enabling access to

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K.MAC, PACE-K.Enc),
3. the ephemeral private key ephem-SK.PICC.PACE,
4. **none** [111],
5. Personalization Agent Key(s),
6. Chip Authentication Private Key and
7. **Active Authentication Private Key** [112].

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. **none** [113],
5. Personalization Agent Key(s) and
6. Chip Authentication Private Key and
7. **Active Authentication Private Key** [114].

Notes:

1. The SFR FPT_EMS.1.1 in the current St covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in the current ST covers the definition in PACE PP [BSI-CR-CC-PP-0068-V2-2011] and extends it by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.
2. The TOE preventd attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates.
   The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact-based interface according to ISO/IEC 7816-2 [ISO-IEC-7816-part-2] as well (in case the package only provides a contactless

109 REFINEMENT
110 [assignment: types of emissions]
111 [assignment: specified limits]
112 [assignment: list of types of TSF data]
113 [assignment: list of types of user data]
114 [assignment: list of types of TSF data]

interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

8.1.12.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

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

1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1,
3. **Failures during cryptographic operations**
4. **Memory failures during TOE execution**
5. **Out of range failures of temperature, clock and voltage sensors**
6. **Failures during random number generation**. [115]

8.1.12.3 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1

The TSF shall run a suite of self tests **during initial start-up and at the conditions**

1. **start-up**
2. **Reading Initialization and Pre-personalization Data according to** FMT_MTD.1/INI_DIS
3. **Reading data of LDS groups and EF.SOD**
4. **Reading CA keys (secret key only internally)**
5. **Cryptographic key generation according to** FCS_CKM.1/DH_PACE_EC **and** FCS_CKM.1/DH_PACE_RSA FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA
6. **Reading certificates internally before Terminal Authentication Protocol v.1 according to** FCS_COP.1/SIG_VER_EC **or** FCS_COP.1/SIG_VER_RSA
7. **Generating random numbers according to** FCS_RND.1 [116]

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.

8.1.12.4 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components. Dependencies: No dependencies.

FPT_PHP.3.1

115 [assignment: list of types of user data]
116 [assignment: list of types of failures in the TSF].

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

Note:

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

8.2 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 4 (EAL4)

and augmented by taking the following components:

- ALC_DVS.2,
- ATE_DPT.2 and
- AVA_VAN.5.

Note:

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

8.3 Security Requirements Rationale

8.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage.

Notes:

1. OTs and SFRs from PACE PP [BSI-CC-PP-0068-V2-2011] are marked with (1).
2. SFRs from PACE PP [BSI-CC-PP-0068-V2-2011] which are extended in EAC PP [BSI-CC-PP-0056-V2-2012-MA-02] are marked with (2).

Table 9: Functional Requirement to TOE security objective mapping

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AA_Proof	OT.AC_Pers	OT.Data_Integrity (1)	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification (1)	OT.Prot_Abusse-Func	OT.Prot_Inf_Leak(1)	OT.Tracing (1)	OT.Prot_Phys-tamper	OT.Prot_Malfunction

						(1)	(1)		(1)			(1)	(1)
FAU_SAS.1 (1)				x				x					
FCS_CKM.1/DH_PACE_EC (1)					x	x	x						
FCS_CKM.1/DH_PACE_RSA					x	x	x						
FCS_CKM.1/CA_EC	x	x		x	x	x	x						
FCS_CKM.1/CA_RSA	x	x		x	x	x	x						
FCS_CKM.1/CA_EC_KeyPair	x	x			x								
FCS_CKM.1/CA_RSA_KeyPair	x	x			x								
FCS_CKM.1/AA_EC_KeyPair			x										
FCS_CKM.1/AA_RSA_KeyPair			x										
FCS_CKM.4 (1)	x			x	x	x	x						
FCS_COP.1/CA_ENC	x	x		x	x		x						
FCS_COP.1/CA_MAC	x	x		x	x	x							
FCS_COP.1/PACE_ENC							x						
FCS_COP.1/PACE_MAC					x	x							
FCS_COP.1/SIG_VER_EC	x			x									
FCS_COP.1/SIG_VER_RSA	x			x									
FCS_COP.1/AA_SGEN_RSA			x										
FCS_COP.1/AA_SGEN_EC			x										
FCS_RND.1 (1)	x			x	x	x	x						
FIA_AFL.1/PACE (1)											x		
FIA_UID.1/PACE (2)	x			x	x	x	x						
FIA_UAU.1/PACE (2)	x			x	x	x	x						
FIA_UAU.4/PACE (2)	x			x	x	x	x						

FIA_UAU.5/PACE (2)	x			x	x	x	x						
FIA_UAU.6/PACE (1)					x	x	x						
FIA_UAU.6/EAC	x			x	x	x	x						
FIA_API.1/CA		x											
FIA_API.1/AA			x										
FDP_ACC.1/TRM (2)	x			x	x		x						
FDP_ACF.1/TRM (2)	x			x	x		x						
FDP_RIP.1 (1)					x	x	x						
FDP_UCT.1/TRM (1)	x				x		x						
FDP_UIT.1/TRM (1)					x		x						
FMT_SMF.1 (1)		x		x	x	x	x	x					
FMT_SMR.1/PACE (2)		x		x	x	x	x	x					
FMT_LIM.1 (2)									x				
FMT_LIM.2 (2)									x				
FMT_MTD.1/INI_ENA (1)				x				x					
FMT_MTD.1/INI_DIS (1)				x				x					
FMT_MTD.1/CVCA_INI	x												
FMT_MTD.1/CVCA_UPD	x												
FMT_MTD.1/DATE	x												
FMT_MTD.1/CA_AA_PK	x	x			x								
FMT_MTD.1/PA (1)				x	x	x	x						
FMT_MTD.1/KEY_READ (2)	x	x		x	x	x	x						
FMT_MTD.3	x												
FPT_EMS.1 (2)				x						x			
FPT_TST.1 (1)										x			x
FPT_FLS.1 (1)										x			x

FPT_PHP.3 (1)					x					x		x	
FTP_ITC.1/PACE (1)					x	x	x				x		

8.3.1.1 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 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.

8.3.1.2 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 S.OD 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 want 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_EC **or** FCS_CKM.1/CA_RSA [117] (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_EC **or** FCS_COP.1/SIG_VER_RSA [118] (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.

8.3.1.3 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,

117 [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]]

118 REFINEMENT FCS_CKM.1/CA_RSA is added to this ST

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_EC **and** FCS_CKM.1/DH_PACE_RSA [119] 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_EC **or** FCS_CKM.1/CA_RSA [120] (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/CA_AA_PK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterward. The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The SFR FMT_MTD.1/CA_AA_PK **requires that the Chip Authentication Key cannot be created unauthorized using** FCS_CKM.1/CA_EC_KeyPair **or** FCS_CKM.1/CA_RSA_KeyPair. **The SFR** FCS_RND.1 **represents a general support for cryptographic operations needed.** [121]

8.3.1.4 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_EC **and** FCS_CKM.1/DH_PACE_RSA [122] resp. FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA [123] 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 KMAC).

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

FMT_MTD.1/PA requires that S.OD 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.

8.3.1.5 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.

119 REFINEMENT FCS_COP.1/SIG_VER_RSA is added to this ST
120 REFINEMENT
121 REFINEMENT FCS_CKM.1/CA_RSA is added to this ST
122 REFINEMENT
123 REFINEMENT

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_EC **and** FCS_CKM.1/DH_PACE_RSA [124] resp. FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA [125] 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.

8.3.1.6 The security objective OT.Sense_Data_Conf "Confidentiality of sensitive biometric reference data"

is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER_EC **or** FCS_COP.1/SIG_VER_RSA [126].

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA [127] (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/CA_AA_PK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterward.

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 SFR FMT_MTD.1/CA_AA_PK **requires that the Chip Authentication Key cannot be created unauthorized using** FCS_CKM.1/CA_EC_KeyPair **or** FCS_CKM.1/CA_RSA_KeyPair. [128]

8.3.1.7 The security objective OT.Chip_Auth_Proof "Proof of travel document's chip authenticity"

is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1/CA proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA [129] is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CA_AA_PK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [BSI-TR-03110-1-V210] requires additional TSF according to FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA [130] (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 SFR FMT_MTD.1/CA_AA_PK **requires that the Chip Authentication Key used for Chip Authentication Protocol v.1 cannot be created unauthorized using** FCS_CKM.1/CA_EC_KeyPair **or** FCS_CKM.1/CA_RSA_KeyPair. **The SFR** FCS_RND.1 **represents a general support for cryptographic operations needed.** [131]

124 REFINEMENT
125 REFINEMENT
126 REFINEMENT
127 REFINEMENT FCS_COP.1/SIG_VER_RSA is added to this ST
128 REFINEMENT
129 REFINEMENT
130 REFINEMENT
131 REFINEMENT

8.3.2 The security objective OT.AA_Proof Proof of the 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 is performed using a TOE internally stored confidential private key as required by** FMT_MTD.1/CA_AA_PK **and** FMT_MTD.1/KEY_READ. **The key pair is generated using** FCS_CKM.1/AA_EC_KeyPair **and** FCS_CKM.1/AA_RSA_KeyPair. **The Active Authentication Protocol** [ICAO-9303-2006] **requires additional TSF according to** FCS_COP.1/AA_SGEN_EC **and** FCS_COP.1/AA_SGEN_RSA **(for the generation ot the digital signatures)**.

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

The SFR FMT_MTD.1/CA_AA_PK **requires that the Active Authentication Key used for Active Authentication Protocol cannot be created unauthorized using** FCS_CKM.1/CA_EC_KeyPair **or** FCS_CKM.1/CA_RSA_KeyPair. **The SFR** FCS_RND.1 **represents a general support for cryptographic operations needed.** [132]

8.3.2.1 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.

8.3.2.2 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.

8.3.2.3 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 interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ). This objective is achieved as follows:

1. while establishing PACE communication with CAN or MRZ (non-blocking authorization data) - by FIA_AFL.1/PACE;
2. for listening to PACE communication (is of importance for the current ST, since S.OD is card-individual) - FTP_ITC.1/PACE.

8.3.2.4 The security objective OT.Prot_Phys-Tamper "Protection against Physical Tampering"

is covered by the SFR FPT_PHP.3.

8.3.2.5 The security objective OT.Prot_Malfunction "Protection against Malfunctions"

is covered by

1. 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
2. the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

132 REFINEMENT

8.3.3 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.

Please note that

- the dependency analysis for SFRs taken over from [BSI-CC-PP-0068-V2-2011] has directly been made within the description of each SFR in chapter 8.1 Security Functional Requirements for the TOE and
- these SFRs are not listed in the following table.

The Table 10: Dependencies between the SFR for the TOE shows the dependencies between the SFR of the TOE.

Table 10: Dependencies between the SFR for the TOE

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/CA_EC	[FCS_CKM.2 Cryptographic key distribution or	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC
	FCS_COP.1 Cryptographic operation],	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_CKM.1/CA_RSA	[FCS_CKM.2 Cryptographic key distribution or	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC
	FCS_COP.1 Cryptographic operation],	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]	[FDP_ITC.1 Import of user data without security attributes, or	Fulfilled by FCS_CKM.1/DH_PACE_EC from [BSI-CC-PP-0068-V2-2011] and FCS_CKM.1/CA_EC and FCS_CKM.1/AA_EC_KeyPair and FCS_CKM.1/AA_RSA_KeyPair and FCS_CKM.1/DH_PACE_RSA and FCS_CKM.1/CA_RSA
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
FCS_CKM.1/CA_EC_KeyPair	[FCS_CKM.2 Cryptographic key distribution or	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC
	FCS_COP.1 Cryptographic operation],	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_CKM.1/CA_RSA_KeyPair	[FCS_CKM.2 Cryptographic key distribution or	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC
	FCS_COP.1 Cryptographic operation],	

SFR	Dependencies	Support of the Dependencies
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_CKM.1/AA_EC_KeyPair	[FCS_CKM.2 Cryptographic key distribution or	Fulfilled by FCS_COP.1/AA_SGEN_EC
	FCS_COP.1 Cryptographic operation],	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_CKM.1/AA_RSA_KeyPair	[FCS_CKM.2 Cryptographic key distribution or	Fulfilled by FCS_COP.1/AA_SGEN_RSA
	FCS_COP.1 Cryptographic operation],	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1/CA_EC FCS_CKM.1/CA_RSA
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_COP.1/CA_MAC	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1/CA_EC FCS_CKM.1/CA_RSA
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_COP.1/SIG_VER_EC	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1/CA_EC FCS_CKM.1/CA_RSA
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_COP.1/SIG_VER_RSA	[FDP_ITC.1 Import of user data without security	See juctification No. 2 below

SFR	Dependencies	Support of the Dependencies
	attributes,	
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_COP.1/AA_SGEN_RSA	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1/AA_RSA_KeyPair
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
FCS_COP.1/AA_SGEN_EC	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1/AA_EC_KeyPair
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011]
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/EAC	No dependencies	n.a.
FIA_API.1/CA	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,	Fulfilled by FDP_ACC.1/TRM

SFR	Dependencies	Support of the Dependencies
	FMT_MSA.3 Static attribute initialization	justification 1 for non-satisfied dependencies
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/CVCA_INI	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1 from [BSI-CC-PP-0068-V2-2011]
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1 from [BSI-CC-PP-0068-V2-2011]
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1 from [BSI-CC-PP-0068-V2-2011]
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CA_AA_PK	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1 from [BSI-CC-PP-0068-V2-2011]
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1 from [BSI-CC-PP-0068-V2-2011]
	FMT_SMR.1 Security roles	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
FPT_EMS.1	No dependencies	n.a.

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

No. 1: 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.

No. 2: (i) Dependency "FCS_CKM.1 Cryptographic key generation" is not useful since all keys for Terminal Authentication are generated outside of the TOE, see "A.Auth_PKI PKI for Inspection Systems". (ii) Dependencies "FDP_ITC.1 Import of user data without security attributes" and "FDP_ITC.1 Import of user data with security attributes" are not necessary because all keys are written using SFR FMT_MTD.1/CVCA_INI **regardless whether the keys are EC or RSA keys.** [133]

133 REFINEMENT

8.3.4 Security Assurance Requirements Rationale

The EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

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 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

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

The component ALC_DVS.2 has no dependencies.

The component ATE_DPT.2 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_TDS.3 Basic modular design
- ADV_FUN.1 Functional testing

All of these are met or exceeded in the EAL4 assurance package.

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 EAL4 assurance package.

8.3.5 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 8.3.3 Dependency Rationale 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-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in section 8.1 Security Functional Requirements for the TOE are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance

requirements. The dependency analysis for the sensitive assurance components in section 8.3.4 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 8.3.3 Dependency Rationale and 8.3.4 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 8.3.4 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.

9 TOE summary specification (ASE_TSS)

This chapter provides a description of the TOE's Security Services, which show how the TOE meets each SFR of 8.1 Security Functional Requirements for the TOE.

9.1 TOE Security Services

9.1.1 User Identification and Authentication

This Security Service is responsible for maintaining of the following 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

according to FMT_SMR.1/PACE.

The TOE allows

- identification of the user according to FIA_UID.1/PACE before the authentication takes place according to FIA_UAU.1/PACE
- the execution of following TSF-mediated actions before the user is identified and associated with one of maintained roles
  1. to establish the communication channel
  2. carrying out the PACE Protocol according to
  3. to read the Initialization Data if it is not disabled by TSF
  4. to carry out the Chip Authentication Protocol v.1
  5. to carry out the Terminal Authentication Protocol v.1
  6. to carry out the Active Authentication Protocol
  7. to run self tests
- the execution of following TSF-mediated actions before the user is authenticated
  1. to establish the communication channel
  2. carrying out the PACE Protocol
  3. to read the Initialization Data if it is not disabled by TSF
  4. to identify themselves by selection of the authentication key
  5. to carry out the Chip Authentication Protocol Version 1
  6. to carry out the Terminal Authentication Protocol Version 1
  7. to carry out the Active Authentication Protocol
  8. to run self tests.

Note:

1. If a user acts as (Travel Document) Manufacturer or Personalization Agent, the user acts as Administrator according to [AIS-V53-CardOS-Users-Manual].

9.1.1.1 Travel document manufacturer Identification and Authentication

After the card leaves the Infineon site the IC Identification Data (a unique IC identifier) written by the IC Manufacturer according to

- FMT_SMF.1 (1)

allows tracing of the travel document.

The travel document manufacturer needs a procedure provided by the developer of the TOE to start his tasks (the card

is secured) according to

- FMT_SMF.1 (1) + (2)

which includes import the Initialization Data and Pre-personalization Data in the audit records (FAU_SAS.1) which contains at least the Personalization Agent Key(s) used for the symmetric authentication mechanism.

The travel document manufacturer creates also

- file system including MF and ICAO.DF and
- the ePassport application.

Writing the Initialization Data and Pre-personalization Data are managed by FMT_MTD.1/INI_ENA.

With FMT_SMR.1/PACE (1) the TOE maintains the role of the Manufacturer.

Reading of the PACE passwords is not allowed according to FMT_MTD.1/KEY_READ.

9.1.1.2 Personalization Agent Identification and Authentication

With FMT_SMR.1/PACE (2) the TOE maintains the role of the Personalization Agent.

The Personalization Agent is identified and authenticated according to

- FIA_UAU.1/PACE (4)
  and the authentication data is not reused according to
- FIA_UAU.4/PACE (2)

using the Symmetric Authentication Mechanism provided by

- FIA_UAU.5.1/PACE (4)

and the authentication attempt is accepted according to

- FIA_UAU.5.2/PACE rule (2).

The usage of the

- Personalization Agent Key(s)

emit no information about IC power consumption in excess of unintelligible limits and any user is unable to gain access by the card interfaces to this keys according to FPT_EMS.1 (5).

The Personalization Agent performs MRTD Configuration for files (e.g. LDS data groups and EF.SOD) and for objects (e.g. for keys).

The tasks of the Personalization Agent are specified by FMT_SMF.1 (3) + (4).

The Personalization Agent is allowed to read out

- the Initialization Data and the Pre-personalization Data according to FMT_MTD.1/INI_DIS

and he is allowed to read the Initialization Data before he is identificated and authenticated according to

- FIA_UID.1/PACE (3)
- FIA_UAU.1/PACE (3).

Personalization Agent is identified using FIA_UAU.1/PACE (4) by selecting his key.

If the Personalization Agent is identificated and authenticated successfully, he is allowed to perform following tasks:

1. Writing
   (i) initial Country Verifying Certification Authority Public Key: PK.CVCA,
   (ii) initial Country Verifying Certification Authority Certificate: C.CVCA,

(iii) initial Current Date,
according to FMT_MTD.1/CVCA_INI
(iv) the Document Security Object (SO.D)
according to FMT_MTD.1/PA.

2. Loading
(v) Chip Authentication Private Key and Active Authentication Private Key
according to FMT_MTD.1/CA_AA_PK.
No one is able to read the Chip Authentication Private Key or Active Authentication Private Key after loading or creating it according to FMT_MTD.1/KEY_READ.
3. Creating
(vi) Chip Authentication Private Key
according to FMT_MTD.1/CA_AA_PK and FCS_CKM.1/CA_EC_KeyPair or FCS_CKM.1/CA_RSA_KeyPair
(vii) Active Authentication Private Key
according to FMT_MTD.1/CA_AA_PK and FCS_CKM.1/AA_EC_KeyPair or FCS_CKM.1/AA_RSA_KeyPair.
No one is able to read the Chip Authentication Private Key or Active Authentication Private Key after loading or creating it according to FMT_MTD.1/KEY_READ.
With FPT_TST.1 the TOE checks previously the correct functioning of the cryptographic routines.
1. Destructing
(viii) the Chip Authentication Private Key or Active Authentication Private Key
according to FCS_CKM.4.

Before issuing the TOE to the travel document holder the Personalization Agent

- has to block the read and use access to the Initialization Data.

This is done to prevent misuse, see [BSI-CC-PP-0068-V2-2011] application note 49.

Additionally the Personalization Agent shall invalidate his key(s).

9.1.1.3 PACE Terminal Identification and Authentication

With FMT_SMR.1/PACE (3) + (4) the TOE maintains the role of a Terminal and PACE authenticated BIS-PACE.

A user in the role terminal is

- a PACE Terminal after the 9.1.3.1 PACE protocol is successfully performed

using secure messaging in MAC-ENC mode according

- FIA_UAU.5.1/PACE (3).

After the PACE protocol is successfully performed the TOE accepts only commands sent by means of secure messaging according to

- FIA_UAU.5.2/PACE (1).

With FIA_UAU.4/PACE (1) the TOE prevents reuse of authentication data and with FIA_UAU.6/PACE the TOE re-authenticate the PACE Terminal by verifying each commands sent.

A user in the role terminal is allowed to carry out the PACE protocol according to

- FIA_UID.1.1/PACE (2)
- FIA_UAU.1.1/PACE (2)

before the user is identification or authenticated.

After performing PACE protocol the terminal shall perform (depending on it's ability)

- the 9.1.2 Advanced Inspection Procedure with PACE
- the 9.1.3.3 Active Authentication Protocol.

9.1.1.4 EIS-AIP-PACE Identification and Authentication

An Extended Inspection System (EIS) using successfully the 9.1.2 Advanced Inspection Procedure with PACE is a EIS-AIP-PACE using a PACE Terminal.

9.1.2 Advanced Inspection Procedure with PACE

An Inspection System is an Extended Inspection System after performing the all parts of the Advanced Inspection Procedure (AIP) successfully in this order:

1. The Inspection System uses an identified and authenticated PACE Terminal, see 9.1.1.3 PACE Terminal Identification and Authentication,
2. the chip is authenticated successfully to the inspection system, see 9.1.3.2 Chip Authentication Protocol v.1
3. the genuineness of the TOE is verified, see 9.1.4 Passive Authentication
4. the terminal used by inspection system is authenticated successfully to the TOE, see 9.1.3.4 Terminal Authentication Protocol v.1

If Advanced Inspection Procedure is performed successfully, the TOE sets the security attributes below (see FDP_ACF.1.1/TRM (3)):

- PACE Authentication
- the security attribute Terminal Authentication Status accordingly to the roles defined in the certificate used for authentication.
- the security attribute Terminal Authorization to the intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.

9.1.3 Protocols

The TOE support the following protocols.

9.1.3.1 PACE protocol

The TOE accepts authentication using the PACE protocol according to

- FIA_UAU.5.1/PACE (1)

using

- FCS_CKM.1/DH_PACE_EC or FCS_CKM.1/DH_PACE_RSA for PACE session keys

which are also used for establishing the trusted channel, see 9.1.7 Establishing the trusted channel.

If the terminal uses a wrong password (not derived from MRZ or CAN), the TOE delays the next attempt to establish the PACE protocol at least 5 seconds according to

- FIA_AFL.1/PACE.

This prevents skimming of the passwords because the passwords are non-blocking authorization data.

If the PACE protocol is performed successfully, the TOE sets the security attribute PACE Authentication (FDP_ACF.1.1/TRM (3.a)).

9.1.3.2 Chip Authentication Protocol v.1

The terminal proves the identify of the TOE using Chip Authentication Protocol v.1 according to [BSI-TR-03110-1-V210] section "3.4 Chip Authentication Version 1" using

- FIA_API.1/CA and
- FCS_CKM.1/CA_EC and FCS_CKM.1/CA_RSA for Chip Authentication session keys

which are also used for establishing the trusted channel, see 9.1.7 Establishing the trusted channel.

After the Chip Authentication Protocol v.1 is successfully performed the TOE accepts only commands sent by means of secure messaging according to

- FIA_UAU.5.2/PACE (3).

With FMT_MTD.1/KEY_READ no user is able to read the Chip Authentication Private Key.

After Chip Authentication Protocol v.1 the terminal has to validate the Chip Authentication Public Key by

- performing 9.1.4 Passive Authentication to verify the genuineness of the TOE.

The usage of the

- Chip Authentication Private Key

emit no information about IC power consumption in excess of unintelligible limits and any user is unable to gain access by the card interfaces to this keys according to FPT_EMS.1 (6).

See 9.1.1.2 Personalization Agent Identification and Authentication for the tasks loading or creating the CA key pair.

9.1.3.3 Active Authentication Protocol

The terminal proves the identify of the TOE using Active Authentication Protocol according to [ICAO-9303-2006] part 1 vol. 2 NORMATIVE APPENDIX 4 using

- FIA_API.1/AA

for providing the protocol and

- FCS_CKM.1/AA_EC_KeyPair or FCS_CKM.1/AA_RSA_KeyPair.

for generating the key pair and

- FCS_COP.1/AA_SGEN_RSA
- FCS_COP.1/AA_SGEN_EC

for signing the terminal's nonce.

With FMT_MTD.1/KEY_READ no user is able to read the Active Authentication Private Key.

The TOE accepts Active Authentication according to

- FIA_UAU.5.1/PACE (6).

After Active Authentication Protocol the terminal has to validate the Active Authentication Public Key by

- performing 9.1.4 Passive Authentication to verify the genuineness of the TOE.

The usage of the

- Active Authentication Private Key

emit no information about IC power consumption in excess of unintelligible limits and any user is unable to gain access by the card interfaces to this keys according to FPT_EMS.1 (7).

See 9.1.1.2 Personalization Agent Identification and Authentication for the tasks loading or creating the AA key pair.

9.1.3.4 Terminal Authentication Protocol v.1

A terminal authenticates itself to the TOE using the Terminal Authentication Protocol v.1 according to [BSI-TR-03110-1-V210] section "3.5 Terminal Authentication Version 1" using

- FIA_UAU.5.1/PACE (5)

and

- FCS_COP.1/SIG_VER_EC or FCS_COP.1/SIG_VER_RSA

for verifying the certificate chain which is managed by

- FMT_MTD.3 (the certificate chain to the trust anchor must be valid).

With FIA_UAU.5.2/PACE (4) the TOE accepts only authentication attempts using the Chip Authentication Public Key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1, see 9.1.3.2 Chip Authentication Protocol v.1 and 9.1.7 Establishing the trusted channel.

With FIA_UAU.4/PACE (3) the TOE prevents reuse of authentication data.

The random nonce is generated using FCS_RND.1.

With FPT_TST.1 reading of a certificate and the generation of a random nonce is checked previously.

If Terminal Authentication Protocol v.1 is performed successfully, the TOE

1. sets the security attribute Terminal Authentication Status (see FDP_ACF.1.1/TRM) accordingly to the roles defined in the certificate used for authentication. It is possible that the security attribute contains more than one value, e.g. CVCA and IS.
2. sets the security attribute Terminal Authorization to the intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
3. updates the Current Date and trust anchor if necessary, see :9.1.6 Write access at phase Operational Use

Note:

1. Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed.

9.1.4 Passive Authentication

The terminal verifies the genuineness of the TOE (MRTD) according to [BSI-TR-03110-1-V210] section "1.1 Passive Authentication" by

- verifying the signature of the SO.D
- reading the hash value of the Chip Authentication public key or the hash value of the Active Authentication public key stored on the chip (LDS data fields)
- comparing the hash values with the hash values computed by the terminal / inspection system over the public keys received from the chip during the respective protocol.

If the hash values are equal and signature is verified, the Passive Authentication is performed successfully.

The TOE accepts Passive Authentication according to

- FIA_UAU.5.1/PACE (2).

For accessing the SO.D and the LDS data fields see 9.1.5 Read access to the LTD and SO.D at phase Operational Use.

Note:

1. Performing Passive Authentication by verifying the signature of SO.D and comparing the stored values with hash value computed by the terminal / inspection system cannot be enforced by the TOE.

9.1.5 Read access to the LTD and SO.D at phase Operational Use

Access to the Logical Travel Document (LTD) and SO.D (EF.SOD) is allowed according to

- FDP_ACC.1/TRM
- FDP_ACF.1/TRM

after 9.1.7 Establishing the trusted channel according to FDP_ACF.1.4/TRM (2):

1. If security attribute PACE Authentication (FDP_ACF.1.1/TRM (3.a)) is set (i.e. the 9.1.3.1 PACE protocol is performed successfully)

then

- the inspection system is allowed to read data objects ((FDP_ACF.1.2/TRM):
  DG1, DG2, DG14, DG15, DG16 and the Security Object SO.D.

2. If security attribute Terminal Authentication Status (FDP_ACF.1.1/TRM (3.b)) has the value "IS" (i.e. the 9.1.2 Advanced Inspection Procedure with PACE is performed successfully), the inspection system is a Extended Inspection System and allowed to read data objects:

- DG1, DG2, DG14, DG15, DG16 and the Security Object SO.D
- DG3 if security attribute Terminal Authorization equals DG3
- DG4 if security attribute Terminal Authorization equals DG4
- DG3 and DG4 if security attribute Terminal Authorization equals DG3 / DG4.

Notes:

1. If the security attribute Terminal Authorization is set to one of the values "DG3" or "DG4" of "DG3 / DG4" and the terminal is not successfully authenticated as Extended Inspection System, the TOE denies access to data objects 2b) of FDP_ACF.1.1/TRM or data objects 2c) of FDP_ACF.1.1/TRM.
2. If security attribute Terminal Authentication Status is set to one of the values "CVCA" or "DV (domestic)" or "DV (foreign)", the TOE denies any inspection system the access to EF.DG3 or EF.DG4 (FDP_ACF.1.4/TRM (6)).

9.1.6 Write access at phase Operational Use

With FMT_SMR.1/PACE (5), (6) + (7) the TOE maintains the roles of Country Verifying Certification Authority, Document Verifier and Domestic Extended Inspection System.

The write access to the TOE phase Operational Use depends on role encoded in certificates.

1. A terminal in the role Country Verifying Certification Authority (security attribute terminal authentication status has the value CVCA) is allowed to update (the trust anchor)

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

according to FMT_MTD.1/CVCA_UPD if the Country Verifying CA Link-Certificates are valid (FMT_MTD.3) after

- 9.1.3.4 Terminal Authentication Protocol v.1 is successfully performed.

2. A terminal in the role

- Country Verifying Certification Authority (security attribute terminal authentication status has the value CVCA)

or

- Document Verifier (security attribute terminal authentication status has the value DV (domestic) or DV (foreign))

or

- Domestic Extended Inspection System [134] (security attribute terminal authentication status has the value IS)

is allowed to modify

- the Current Date

according to FMT_MTD.1/DATE if the Country Verifying CA Link-Certificates are valid (FMT_MTD.3) after

- 9.1.3.4 Terminal Authentication Protocol v.1 is successfully performed

and

134 From travel document's point of view an Extended Inspection System is a domestic one if the Extended Inspection System is authorized by the issuing State or Organization.

- if the Current Date is before the effective date of the respective certificate.

The Current Date is set to the maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates used during performing 9.1.3.4 Terminal Authentication Protocol v.1.

If operations (1) and (2) have to be performed both after 9.1.3.4 Terminal Authentication Protocol v.1, they are implemented as an atomic operation, see [BSI-TR-03110-3-V211] section "2.5.1 General Procedure".

Please note that a prerequisite for performing successfully TA is a successfully performed 9.1.3.2 Chip Authentication Protocol v.1.

9.1.7 Establishing the trusted channel

With FTP_ITC.1/PACE the TOE

- provides a communication channel between itself and another trusted IT product
- permits another trusted IT product to initiate communication via the trusted channel
- enforces communication via the trusted channel for any data exchange between the TOE and the Terminal

which is supported **in case of a PACE protocol** by

- FCS_CKM.1/DH_PACE_EC or FCS_CKM.1/DH_PACE_RSA for PACE session key derivation (with MRZ or CAN as password)
  and
  FIA_UAU.5.1/PACE (3) for secure messaging using
  1. FCS_COP.1/PACE_ENC for confidentiality (by encrypting the data)
  2. FCS_COP.1/PACE_MAC for integrity (by MACing the commands).

or **in case of a Chip Authentication protocol v.1** by

- FCS_CKM.1/CA_EC and FCS_CKM.1/CA_RSA for Chip Authentication session key derivation (with Chip Authentication Public Key)
  and
  FIA_UAU.5.1/PACE (3) for secure messaging using
  1. FCS_COP.1/CA_ENC for confidentiality (by encrypting the data)
  2. FCS_COP.1/CA_MAC for integrity (by MACing the commands).

and (when transmitting and receiving user data)

- FDP_UCT.1/TRM by protecting from unauthorized disclosure
- FDP_UIT.1/TRM by protecting from modification, deletion, insertion and replay errors and by determining on receipt of user data, whether modification, deletion, insertion and replay has occurred.

After the trusted channel is established the TOE does not execute any command with incorrect message authentication code according to

- FIA_UAU.6/EAC in case of a Chip Authentication protocol v.1
- FIA_UAU.6/PACE in case of a PACE protocol.

The usage of session keys

- {CA-K.MAC, CA-K.Enc} (generated during Chip Authentication)
- {PACE-K.MAC, PACE-K.Enc} (generated during PACE)

and

- ephemeral domain parameters {ephem-SK.PICC.PACE, ephem-PK.PICC.PACE} (used for starting of ECDH for PACE)

emit no information about IC power consumption in excess of unintelligible limits and any user is unable to gain access by the card interfaces to these keys according to FPT_EMS.1 (1) + (2) + (3).

After the trusted channel is terminated the session keys and the ephemeral private key ephem-SK.PICC.PACE are invalidated according to

- FCS_CKM.4
- FDP_RIP.1.

and

- the security attribute PACE Authentication (see FDP_ACF.1.1/TRM) is unset
- the security attribute Terminal Authentication Status is set to "none".

9.1.8 Test features

According to FMT_LIM.1 and FMT_LIM.2 the TOE is designed in a manner that limits the

- capabilities of TSF
- availability of TSF

to enforce the following policy

Deploying Test Features after TOE Delivery does 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 Test Features are disabled before the card leaves IC Manufacturer's site.

9.1.9 Protection

This Security Service is responsible for the protection of the TSF, TSF data and user data. The TOE runs a suite of tests to demonstrate the correct operation of the security assumptions provided by the IC platform that underlies the TSF. The following tests are performed during initial start-up (FPT_TST.1):

- The SLE78CLFX*P (M7892 B11) provides a high security initialization software concept. The self test software (STS) is activated by the chip after a cold or warm reset (ISO-reset with I/O=1). It contains diagnostic routines for the chip, see [Infineon-Chip-HW-Ref], chapter 8.
- After erasure of RAM the state of the User EEPROM is tested and, if not yet initialized, this will be done.
- The User EEPROM heap is checked for consistency. If it is not valid, the TOE will preserve a secure state (life cycle DEATH).
- The backup buffer is checked and its data is restored to User EEPROM, if they were saved because of a command interruption.
- The integrity of stored TSF executable code is verified. If this check fails, the TOE will preserve a secure state (life cycle DEATH).
- The integrity of stored data (objects and files) is verified before their use.
- The hardware sensors, the symmetric coprocessor and the random number generator are tested. If one of the tests fails, the chip platform will perform a security reset.

The TOE will furthermore run tests during

1. start-up
2. Reading Initialization and Pre-personalization Data according to "FMT_MTD.1/INI_DIS"
3. Reading data of LDS groups and EF.SOD
4. Reading CA keys (secret key is used only internally by the TOE)
5. Cryptographic key generation according to "FCS_CKM.1/DH_PACE_EC", "FCS_CKM.1/DH_PACE_RSA", "FCS_CKM.1/CA_EC" and "FCS_CKM.1/CA_RSA"
6. Reading certificates internally before Terminal Authentication Protocol v.1 according to "FCS_COP.1/SIG_VER_EC" or "FCS_COP.1/SIG_VER_RSA"
7. Generating random numbers according to "FCS_RND.1"

according to FPT_TST.1.

The correct operation of generation of the key pairs is demonstrated by performing the following checks:

- The TOE's life cycle phase is checked. Only the Personalization Agent can perform key pair generation according to FMT_MTD.1/CA_AA_PK using FCS_CKM.1/CA_EC_KeyPair, FCS_CKM.1/CA_RSA_KeyPair, FCS_CKM.1/AA_EC_KeyPair or FCS_CKM.1/AA_RSA_KeyPair
- Before a random number from the PTRNG is used for the generation of the SCD/SVD key pair the correct functioning of the random number generator is checked by reading out the status register of PTRNG.

Furthermore the TOE checks

- all command parameters for consistency
- access rights.

If a critical failure occurs during these tests, the TOE will preserve a secure state according to FPT_FLS.1. This comprises the following types of failures:

- Failure of sensors
- Failure of Active Shield
- Failure of cryptographic operation, e.g. during key creation
- Memory failures during TOE execution

The TOE is furthermore able to detect physical manipulation and physical probing (FPT_PHP.3). This comprises tampering attempts before start-up and during operation. If the underlying IC hardware is attacked by physical or mechanical means, the TOE will respond automatically in form of a continuously generated reset and the TOE functionality will be blocked.

The TOE protects itself against interference and logical tampering by the following measures:

Each application removes its own data from the used memory area at the latest after execution of a command.

- Clearance of sensitive data, as soon as possible (when they are dispensable) according to FCS_CKM.4 and FDP_RIP.1
- No parallel but only serial execution of commands
- Encapsulation of context data (security relevant status variables, etc.)
- Use of the chips MMU (Memory Management Unit)
- Separation of User ROM and Test ROM, where the chip's self test software is located, and to which entries are not possible (apart from cold or warm reset)
- Removal of channel data, when the channel is closed

The TOE protects itself against bypass by not allowing any function in the TSF to proceed if a prior security enforcement function was not executed successfully. The TOE always checks that the appropriate user is successfully authenticated (cf. 9.1.1 User Identification and Authentication) for a certain action.

With FPT_EMS.1 the TOE ensures any users are unable to use the following interface smart card circuit contacts to gain access to

- Chip Authentication Session Keys
- PACE Session Keys (PACE-K.MAC, PACE-K.Enc),
- the ephemeral private key ephem-SK.PICC.PACE,
- Personalization Agent Key(s) and
- Chip Authentication Private Key and
- Active Authentication Private Key.

The TOE provides contact-based and contactless interfaces and is able to connect itself

i. with terminals which provide a contactless interface
ii. with terminals which provide a contact-based interface.

In the case that the TOE is connected using it's contactless interface the TOE accepts attempts to establish a connection using it's contact-based interface by

i. resetting first it's contactless interface
ii. restarting using it's contact-based interface only.

If the TOE is connected using it's contact-based interface, the TOE does not accept any attempt to establish a connection using it's contactless interface.

9.2 Compatibility between the Composite ST and the Platform-ST

The sections

- 9.2.1 Assurance requirements of the composite evaluation
- 9.2.2 Assumptions of platform for its Operational Environment
- 9.2.3 Security objectives of Platform
- 9.2.4 Organizational security policies of platform
- 9.2.5 Threats of the platform
- 9.2.6 Usage of platform TSF by TOE TSF

show the compatibility of this Composite ST and the Platform-ST as required by [BSI-AIS36-V4].

The Platform-ST is the security target of all controllers SLE78CLFX*P (M7892 B11) used by this TOE as platform.

9.2.1 Assurance requirements of the composite evaluation

The Platform-ST requires

- Common Criteria version v3.1 part 1, part 2 and part 3 and
- EAL6 augmented with the component ALC_FLR.1.

The Composite-ST requires:

- Common Criteria version 3.1, cf. [CC-3.1-P1], [CC-3.1-P2], and [CC-3.1-P3] and
- EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

Therefore the Composite-SAR is a subset of the Platform-SAR.

9.2.2 Assumptions of platform for its Operational Environment

The following table list all assumptions of the hardware platform related to its operational environment not relevant for this Composite-ST automatically (IrPA).

Table 11: Irrelevant assumptions of platform for its Operational Environment

Assumptions of the HW platform related to its operational environment	Meaning	OT of this composite TOE
inherited from [BSI-PP-0035]		
A.Plat-Appl	Usage of Hardware Platform	n.a. (see note (1) below)

Note:

1. CardOS DI V5.3 considers the reqirements of A.Plat-Appl by its technical design and implementation.

The following table list all relevant assumptions of the hardware platform related to its operational environment which are

fulfilled by the Composite-ST automatically (CfPA).

Table 12: Relevant assumptions of platform for its Operational Environment

Assumptions of the HW platform related to its operational environment	Meaning	OT of this composite TOE
inherited from [BSI-PP-0035]		
A.Resp-Appl	Treatment of User Data	OT.Data_Integrity OT.Data_Authenticity OT.Prot_Abuse-Func OT.Prot_Phys-Tamper
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	OT.Identification
dedicatedly defined in [Infineon-ST-Chip-B11-2015-10-13]		
A.Key-Function	Usage of Key-dependent Functions	OT.Prot_Inf_Leak

With table Table 11: Irrelevant assumptions of platform for its Operational Environment and Table 12: Relevant assumptions of platform for its Operational Environment all assumptions provided by the Platform-ST related to its operational environment are listed and therefore the set of assumptions of the Platform-ST related to its operational environment belonging neither to the group IrPA nor CfPA is empty (SgPA).

9.2.3 Security objectives of Platform

The following table list all security objectives of the hardware platform which relevant to OTs of this Composite-ST.

Table 13: Mapping of security objectives of platform

Security objectives of the Platform-ST	OTs of the Composite-ST									
	OT.Prot_Phys-Tamper	OT.Malfunction	OT.Prot_Inf_Leak	OT.Prot_Abuse-Func	OT.Identification	OT.Chip_Auth_Proof	OT.AA_Proof	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality
O.Phys-Manipulation	x									
O.Phys-Probing	x									

Security objectives of the Platform-ST	OTs of the Composite-ST									
	OT.Prot_Phys-Tamper	OT.Malfunction	OT.Prot_Inf_Leak	OT.Prot_Abuse-Func	OT.Identification	OT.Chip_Auth_Proof	OT.AA_Proof	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality
O.Malfunction	x	x								
O.Leak-Inherent			x							
O.Leak-Forced			x			x		x	x	x
O.Abuse-Func				x						
O.Identification					x					
O.RND						x		x	x	x
O.Add-Functions						x	x	x	x	x

The security objectives of the Platform-ST and the OTs of this Composite-ST are not contradictory since they can be mapped.

The following security objective of platform can not be mapped to OTs of this Composite-ST (list 1)

- O.Mem-Access

since no OT of the Composite-ST needs the respective security functionality.

For the following OTs of the Composite-ST no security objectives of platform exists (list 2)

- OT.Sens_Data_Conf
- OT.Tracing
- OT.AC_Pers

since no security objectives of the Platform-ST provides a functionality needed by this TOE.

With table Table 13: Mapping of security objectives of platform, list 1 and list 2 all security objectives of the Platform-ST and all OTs of the Composite-ST are listed and therefore the security objectives of the Platform-ST are not contradictory to those of the Composite-ST.

9.2.4 Organizational security policies of platform

The Platform-ST lists two organizational security policies:

- P.Process-TOE
- (augmented) P.Add-Functions.

OSP P.Process-TOE of the platform is relevant since this organizational security policiy is covered by

- OSP P.Manufact

of the Composite-ST.

OSP P.Add-Functions of the platform is relevant since this policy provides security functionality needed by

- OT.Chip_Auth_Proof (ECDH)
- OT.AA_Proof (RSA and EC)
- OT.Data_Integrity (AES and TDES)
- OT.Data_Authenticity (AES and TDES)

The organizational security policies of the Platform-ST and the OTs of this Composite-ST are not contradictory since they are are not relevant or can be used directly by this TOE.

9.2.5 Threats of the platform

The following table provides a mapping of the threats of the Platform-ST to the threats of this Composite-ST using the OTs provided by table Table 13: Mapping of security objectives of platform and threats mapped to this OTs by Table 4: Security Objective Rationale and the threats of the Platform-ST ([BSI-PP-0035] section 4.4).

Table 14: Mapping of the threats of the Platform-ST

Threats of the Platform-ST	Threats of this Composite-ST								
	T.Phys-Tamper	T.Forgery	T.Malfunction	T.Information_Leakage	T.Abuse-Funczion	T.Counterfeit	T.Skimming	T.Forgery	T.Eavesdropping
T.Leak-Inherent				x					
T.Phys-Probing	x	x							
T.Malfunction	x	x	x						
T.Phys-Manipulation	x	x							
T.Leak-Forced				x		x	x	x	x
T.Abuse-Func					x				
T.RND						x	x	x	x
T.Mem-Access	x		x		x				

9.2.6 Usage of platform TSF by TOE TSF

The relevant SFRs (RP_SFR) of the platform being used by the Composite ST are listed in the following table:

Table 15: Relevant platform SFRs used by Composite ST

RP_SFR	Meaning	Used by TOE SFR
FRU_FLT.2	Limited Fault Tolerance	FPT_TST.1
FPT_FLS.1	Failure with Preservation of Secure State	FPT_FLS.1
FPT_PHP.3	Resistance to Physical Attack	FPT_PHP.3
FDP_ITT.1	Basic Internal Transfer Protection	FPT_EMS.1
FDP_IFC.1	Subset Information Flow Control	FPT_EMS.1
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	FPT_EMS.1
FCS_RNG.1	Quality Metric for Random Numbers	FCS_CKM.1/CA_EC_KeyPair, (EC Key Pair generation for CA) FCS_CKM.1/CA_RSA_KeyPair (RSA Key Pair generation for CA) FCS_CKM.1/AA_EC_KeyPair (EC Key Pair generation for AA) FCS_CKM.1/AA_RSA_KeyPair (RSA Key Pair generation for AA) FIA_UID.1/PACE for ► (2) PACE Protocol ► (5) Terminal Authentication Protocol v.1 FCS_CKM.1/CA_EC FCS_CKM.1/CA_RSA FPT_EMS.1 (blinding) FCS_RND.1
FPT_TST.2	Subset TOE Security Testing	FPT_TST.1 FPT_PHP.3 (active shield and sensors)
FCS_CKM.1/EC	Cryptographic key generation	FCS_CKM.1/CA_EC_KeyPair, FCS_CKM.1/AA_EC_KeyPair
FCS_CKM.1/RSA	Cryptographic Key Generation (RSA)	FCS_CKM.1/AA_RSA_KeyPair FCS_CKM.1/CA_RSA_KeyPair
FCS_COP.1/ECDH	Cryptographic Support (ECDH)	FCS_CKM.1/CA_EC,

RP_SFR	Meaning	Used by TOE SFR
		FCS_CKM.1/DH_PACE_EC
FCS_COP.1/ECDSA	Cryptographic Support (ECDSA)	FCS_COP.1/SIG_VER_EC FCS_COP.1/AA_SGEN_EC
FCS_COP.1/RSA	Cryptographic Support (RSA)	FCS_COP.1/SIG_VER_RSA FCS_CKM.1/DH_PACE_RSA FCS_CKM.1/CA_RSA FCS_COP.1/AA_SGEN_RSA
FCS_COP.1/DES	Cryptographic Support (3DES)	FCS_COP.1/CA_ENC (TDES), FCS_COP.1/CA_MAC (TDES) FCS_COP.1/PACE_ENC (TDES) FCS_COP.1/PACE_MAC (TDES)
FCS_COP.1/AES	Cryptographic Support (AES)	FCS_COP.1/CA_ENC (AES), FCS_COP.1/CA_MAC (AES) FCS_COP.1/PACE_ENC (AES) FCS_COP.1/PACE_MAC (AES)
FCS_COP.1/SHA	Cryptographic Support (SHA-2)	FCS_CKM.1/CA_EC, FCS_CKM.1/DH_PACE_EC FCS_CKM.1/DH_PACE_RSA FCS_CKM.1/CA_RSA
FAU_SAS.1	Audit Storage	FAU_SAS.1
FMT_LIM.1	Limited Capabilities	FMT_LIM.1
FMT_LIM.2	Limited Availability	FMT_LIM.2
FDP_ACC.1	Subset Access Control	no conflicts with TSF
FDP_ACF.1	Security Attribute Based Access Control	no conflicts with TSF

The irrelevant SFRs (IP_SFR) of the platform not being used by the Composite ST are listed in the following table:

Table 16: Irrelevant platform SFRs not being used by Composite ST

IP_SFR	Meaning	Comment
FDP_SDI.1	Stored Data Integrity Monitoring	Not used by TSF
FDP_SDI.2	Stored Data Integrity Monitoring and Action	Not used by TSF
FMT_MSA.1	Management of Security Attributes	Not used by TSF
FMT_MSA.3	Static Attribute Initialization	Not used by TSF
FMT_SMF.1	Specification of Management Functions	Not used by TSF

There is no conflict between the security problem definition, the security objectives and the security requirements of the

current Composite Security Target and the platform Security Target (security target of the controller SLE78CLFX*P (M7892 B11)). All related details (operations on SFRs, definition of security objectives, threats etc.) can be found in both the documents.

10 Appendix: Cryptographic mechanisms used

This TOE is a composite product and uses for cryptographic mechanism listed only mechanism provided by the underlying chip SLE78CLFX*P (M7892 B11) exept for SHA-1, SHA-224 and SHA-384, see notes 11 and 12 below. The "Standard of Implementation" is a citation of the ST of the underlying chip SLE78CLFX*P (M7892 B11) only, cf. [Infineon-ST-Chip-B11-2015-10-13].

Table 17: Cryptographic mechanisms used

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments ST Reference
1	Authenticity	Terminal Authentication, ECDSA-signature verification using SHA-224, SHA-256, SHA-384 or SHA-512	ANSI X9.62-2005 section 7.4.1 and ISO/IEC 15946-2:2002 section 6.4 see Cryptographic Primitive No. 23 for SHA-2	224 NIST, 256 NIST, 384 NIST, 224 r1 BP, 256 r1 BP, 384 r1 BP, 512 r1 BP	[ICAO-9303-2006], [BSI-TR-03110-3-V211]	FCS_COP.1/SIG_VER_EC (see notes 1 + 2 below)
2		Terminal Authentication, RSA-signature verification using SHA-224, SHA-256, SHA-384 or SHA-512	PKCS v2.1 RFC3447, section 5.2.2 RSAVP1, padding according to RSASSA-PSS or RSASSA-PKCS1-v1_5 see Cryptographic Primitive No. 23 for SHA-2	1024, 1280, 1536, 2048, 3072	[ICAO-9303-2006], [BSI-TR-03110-3-V211]	FCS_COP.1/SIG_VER_RSA (see notes 3 + 4)
3	Authentication	PACE using SHA-1 (for MRZ), generic and integrated mapping [135]	[BSI-TR-03110-1-V210]	160 (MRZ) 128 (nonce) 56 or 73 (CAN), see note 13	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_CKM.1/DH_PACE_EC
4		PACE using SHA-1 (for MRZ), DH	[BSI-TR-03110-1-V210]	160 (MRZ) 128	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_CKM.1/DH_PACE_RSA

135 Integrated Mapping is a licensed technology protected by MORPHO under the patents FR2946818 and FR2946819 and their foreign extensions.

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments ST Reference
		Mapping		(nonce) 56 or 73 (CAN), see note 13		
5		Active Authentication, ECDSA signature generation using SHA-224, SHA-256, SHA-384 or SHA-512	(1) According to section 7.3 in ANSI X9.62 - 2005 (2) According to section 6.2 (6.2.2. + 6.2.3) in ISO/IEC 15946-2:2002 see Cryptographic Primitive No. 23 for SHA-2	224 NIST, 256 NIST, 384 NIST, 224 r1 BP, 256 r1 BP, 384 r1 BP, 512 r1 BP	[ICAO-9303-2006]	FCS_COP.1/AA_SGEN_EC (see notes 2 + 5)
6		Active Authentication, RSA signature generation using SHA-256	(1) According to section 5.2.1 RSASP1 in PKCS v2.1 RFC3447 for u = 2 (2) padding according to ISO/IEC 9796-2 see Cryptographic Primitive No. 23 for SHA-2	2048	[ICAO-9303-2006]	FCS_COP.1/AA_SGEN_RSA (see note 6)
7		Implicite authentication during SM TDES in CBC mode	see Confidentiality No. 13 (TDES)	112	see No. 12	FCS_COP.1/CA_ENC session keys after PACE or CA (cf Table 6: Keys and certificates)
8		Implicite authentication during SM AES in CBC mode	see Confidentiality No. 14 (AES)	128, 192, 256	see No. 13	FCS_COP.1/CA_ENC session key after PACE or CA (cf Table 6: Keys and certificates)
9		Symmetric Authentication, AES in CBC mode	FIPS PUB 197 (AES) [NIST-800-38A-2001] (CBC)	128, 256	[BSI-TR-03110-1-V210]	Personalization-key, secure messaging

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments ST Reference
10	Key agreement	PACE Key derivation ECDH using SHA-1 and SHA-256	[ICAO-TR-101] see Cryptographic Primitive No. 23 for SHA-1 and SHA-2	112 (TDES), 128 (AES), 192 (AES), 256 (AES)	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_CKM.1/DH_PACE_EC
11		PACE Key derivation DH using SHA-1 and SHA-256	[RSA-PKCS-3-1993] see Cryptographic Primitive No. 23 for SHA-1 and SHA-2	112 (TDES), 128 (AES), 192 (AES), 256 (AES)	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_CKM.1/DH_PACE_RSA
12		Chip Authentication EC key pair generation	ECDSA Key Generation appendix A4.3 in ANSI X9.62-2005 and section 6.1 (not 6.1.1) in ISO/IEC 15946-1:2002	224 NIST, 256 NIST, 384 NIST, 224 r1 BP, 256 r1 BP, 384 r1 BP, 512 r1 BP	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_CKM.1/CA_EC_KeyPair (see note 2 + 7)
13		Chip Authentication RSA key pair generation	RSA Key Generation section 3.2(2) in PKCS v2.1 RFC3447	2048	[ICAO-TR-110], [BSI-TR-03110-1-V210]	FCS_CKM.1/CA_RSA_KeyPair (see note 14)
14		Chip Authentication Key derivation ECDH using SHA-1 and SHA-256	[ICAO-TR-101] see Cryptographic Primitive No. 23 for SHA-1 and SHA-2	112 (TDES), 128 (AES), 192 (AES), 256 (AES)	[ICAO-TR-110], [BSI-TR-03110-1-V210], 	FCS_CKM.1/CA_EC

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments ST Reference
15		Chip Authentication Key derivation DH using SHA-1 and SHA-256	[RSA-PKCS-3-1993] see Cryptographic Primitive No. 23 for SHA-1 and SHA-2	112 (TDES), 128 (AES), 192 (AES), 256 (AES)	[BSI-TR-03110-1-V210]	FCS_CKM.1/CA_RSA (see note 15)
16	Confidentiality	Secure Messaging, TDES in CBC mode	NIST Special Publication 800-67 V1.1 (TDES) [NIST-800-38A-2001] (CBC)	112	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_COP.1/CA_ENC FCS_COP.1/PACE_ENC (see note 8)
17		Secure Messaging, AES in CBC mode	FIPS PUB 197 (AES) [NIST-800-38A-2001] (CBC)	128, 192, 256	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_COP.1/CA_ENC FCS_COP.1/PACE_ENC (see note 9)
18	Integrity	Secure Messaging, TDES in Retail MAC mode	NIST Special Publication 800-67 V1.1 (TDES) [ISO-IEC-9797-1-2011] algorithm 3 and padding method 2 (Retail MAC)	112	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_COP.1/CA_MAC FCS_COP.1/PACE_MAC (see note 8)
19		Secure Messaging, AES in CMAC mode	FIPS PUB 197 (AES) [ISO-IEC-9797-1-2011] algorithm 5 and padding method 2 (CMAC)	128, 192, 256	[ICAO-TR-101], [BSI-TR-03110-1-V210]	FCS_COP.1/CA_MAC FCS_COP.1/PACE_MAC (see note 9)
20	Trusted Channel	Secure Messaging in ENC MAC mode established during PACE	[BSI-TR-03110-1-V210] see also No 3, 4, 7, 8, 16 - 19	see No. 16 - 19	[ICAO-TR-101], [ICAO-9303-2006], [BSI-TR-03110-1-V210]	FTP_ITC.1/PACE
21		Secure Messaging in ENC MAC mode rstablished during CA after PACE	[BSI-TR-03110-1-V210] see also No 7, 8, 14 - 19	see No. 14 - 19	[ICAO-TR-101], [ICAO-9303-2006], [BSI-TR-03110-1-V210]	FTP_ITC.1/PACE FCS_CKM.1/CA_EC FCS_CKM.1/CA_RSA
22	Cryptographic	PTG.2 random	[BSI-AIS31-V3]	-	[BSI-TR-03116-2]	FCS_RND.1

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments ST Reference
	primitive	number generator				for PACE additionally processed according to [BSI-TR-03116-2] section 1.3.3.1 (see note 10)
23		SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[NIST-FIPS-PUB-180-4]	-	[BSI-TR-03110-3-V211]	Signature verification, signature generation, key derivation (see note 11 + 12)

Notes:

1. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CLFX*P (M7892 B11). For the standard of implementation of "digital signature verification" using EC see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.7 Elliptic Curve DSA (ECDSA) operation", section "Signature Verification:".
2. EC curves for TA are taken from [BSI-TR-03110-3-V211] Table 4: Standardized Domain Parameters.
3. This TOE uses the RSA crypto library v1.02.013 of the underlying chip SLE78CLFX*P (M7892 B11). For the standard of implementation of "digital signature verification" see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.4 Rivest-Shamir-Adleman (RSA) operation", section "Signature Verification:".
4. The RSA bit lengths for TA are taken over from [BSI-TR-03110-3-V211] section A.6.3.2. Public Key Format.
5. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CLFX*P (M7892 B11). For the standard of implementation of "digital signature generation" see [Infineon-ST-Chip-B11-2015-10-13], 8.5.4 Elliptic Curves EC, section "Signature Generation".
6. This TOE uses the RSA (Signature Generation) provided by the underlying chip SLE78CLFX*P (M7892 B11). For the standard of implementation of "digital signature generation" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation, section "Signature Generation (with or without CRT)::".
7. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CLFX*P (M7892 B11). For the "cryptographic key generation algorithm" see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.8 Elliptic Curve (EC) key generation"
8. This TOE uses the Triple-DES provided by the underlying chip SLE78CLFX*P (M7892 B11). For the the standard of implementation of "secure messaging - encryption and decryption" using TDES see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.2 Triple-DES Operation.
9. This TOE uses the AES provided by the underlying chip SLE78CLFX*P (M7892 B11). For the standard of implementation of "Advanced Encryption Standard (AES)" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.3 AES Operation.
10. This TOE uses the random numbers generation provided by the underlying chip SLE78CLFX*P (M7892 B11). For the standard of implementation of "random numbers generation Class PTG.2 according to [BSI-AIS31-V3]" see [Infineon-ST-Chip-B11-2015-10-13] "7.1.1.1 FCS_RNG".
11. The hash algorithm SHA-1 is provided by CardOS DI V5.3 according to [NIST-FIPS-PUB-180-4] section 6.1.
12. This TOE uses for SHA-{256, 512} the SHA crypto library v1.01 of the underlying chip SLE78CLFX*P (M7892 B11). For the standard of implementation of hash algorithms SHA-{256, 512} see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.10 SHA-2 Operation".
    The hash algorithm SHA-224 is provided by CardOS DI V5.3 using a SHA-256 value according to [NIST-FIPS-PUB-180-4] section 6.3.
    A SHA-384 value is computed by CardOS DI V5.3 from a SHA-512 value according to [NIST-FIPS-PUB-180-4] chapter 6.5.
13. Cf. [BSI-TR-03110-1-V210] section "A.1. Document Basic Access Keys".
14. This TOE uses the RSA crypto library v1.02.013 of the underlying chip SLE78CLFX*P (M7892 B11). For the "cryptographic key generation algorithm" see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.5 Rivest-Shamir-

Adleman (RSA) key generation"

15. For computing the shared secret the modular exponentation function (cryptorsasignexp) of the RSA crypto library of the Infineon chip SLE78CLFX*P (M7892 B11) is used. Function "cryptorsasignexp" of RSA crypto library is used also for signing.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to [ICAO-9303-2006], [ICAO-TR-101], [BSI-TR-03110-1-V210], and [BSI-TR-03110-3-V211] the algorithms are suitable for authenticity, authentication, key agreement, confidentiality and integrity. An explicit validity period is not given.