Security Target 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)', Rev. 2.01, BAC 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-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

[FIPS-46-3-1999]

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[FIPS-197-2001]

Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[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

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-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-0002-2001]

BSI, Smartcard IC Platform Protection Profile, Version 1.0, July 2001, developed by Atmel Smart Card ICs, Hitachi Europe Ltd., Infineon Technologies AG, Philips Semiconductors

[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

[BSI-CR-CC-PP-0055-110]

BSI, Certification Report for BSI-CC-PP-0055-2009 Machine Readable Travel Document with "ICAO Application" Basic Access Control, 07 May 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-FAL-2004]

INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March 1 April 2004)

[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

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

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)

TSS
: TOE Summary Specification

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].

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 (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.

Counterfeit
: An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO-9303-2006]

Document Basic Access Key
: 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.

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]

Eavesdropper
: A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD'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]

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.

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 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.

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 MRTD
: Data of the MRTD holder stored according to the Logical Data Structure [ICAO-9303-2006] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD 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.

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 visa (MRV)
: A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [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]

MRTD application
: Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [ICAO-9303-2006], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14, EF.DG 16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.

MRTD Basic Access Control
: Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.

MRTD holder
: The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

MRTD's chip
: A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [ICAO-FAL-2004], p. 14.

MRTD's chip Embedded Software
: Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.

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.

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 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 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 MRTD's chip
: MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.

Primary Inspection System (PIS)
: An inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.

Random identifier
: Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability.

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

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.

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").

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 (BAC)'

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-968

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 (BAC)'.

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

The Security Target defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the 'ICAO Doc 9303' [ICAO-9303-2006].

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

i. Basic Access Control (BAC) according [BSI-CC-PP-0055-110].

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 library 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) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303' [ICAO-9303-2006].

The TOE comprises at least

i. the circuitry of the MRTD's chip (the integrated circuit, IC)
ii. the antenna,
iii. the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
iv. the IC Embedded Software (operating system),
v. the MRTD 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 MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD 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 MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on

i. the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and
ii. optional biometrics using the reference data stored in the MRTD.

The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this ST the MRTD is viewed as unit of

a) the physical MRTD as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
   1. the biographical data on the biographical data page of the passport book,
   2. the printed data in the Machine-Readable Zone (MRZ) and
   3. the printed portrait.
b) the logical MRTD as data of the MRTD holder stored according to the Logical Data Structure [ICAO-9303-2006] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
   1. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   2. the digitized portraits (EF.DG2),
   3. the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both [1]
   4. the other data according to LDS (EF.DG5 to EF.DG16) and
   5. the Document security object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO-9303-2006]. These security measures include the binding of the MRTD's chip to the passport book.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO-9303-2006]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This ST addresses the protection of the logical MRTD

i. in integrity by write-only-once access control and by physical means, and
ii. in confidentiality by the Basic Access Control Mechanism.

This ST does not address the Active Authentication and the Extended Access Control as optional security mechanisms.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system

i. reads optically the MRTD,
ii. authenticates itself as inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO-9303-2006], normative appendix

1 These additional biometric reference data are optional.

5.

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 MRTD application and the guidance documentation associated with these TOE components.

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

Phase 2 "Manufacturing"

(Step3) In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD'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 MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

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

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

(Step5) The MRTD manufacturer

(i) creates the MRTD application and

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

Creation of the application implies:

- the creation of MF and ICAO.DF.

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

Phase 3 "Personalization of the MRTD"

(Step6) The personalization of the MRTD includes

(i) the survey of the MRTD holder's biographical data,

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

(iii) the printing of the visual readable data onto the physical MRTD,

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

(v) configuration of the TSF.

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 MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use) is handed over to the MRTD 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) and the Basic Authentication Control Key. (cf. Application note 2 of [BSI-CC-PP-0055-110])

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. The selection of the authentication keys considers the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment. (cf. Application note 3 of [BSI-CC-PP-0055-110])

Phase 4 "Operational Use"

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

The authorized Personalization Agents are **not** allowed to add (**and** not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 "Operational Use" after issuing the travel document to the MRTD holder. (cf. Application note 4 of [BSI-CC-PP-0055-110])

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 2.(cf. Application note 5 of [BSI-CC-PP-0055-110])

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) have to be 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 MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

Note:

1. To be able to work as tavel 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
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.

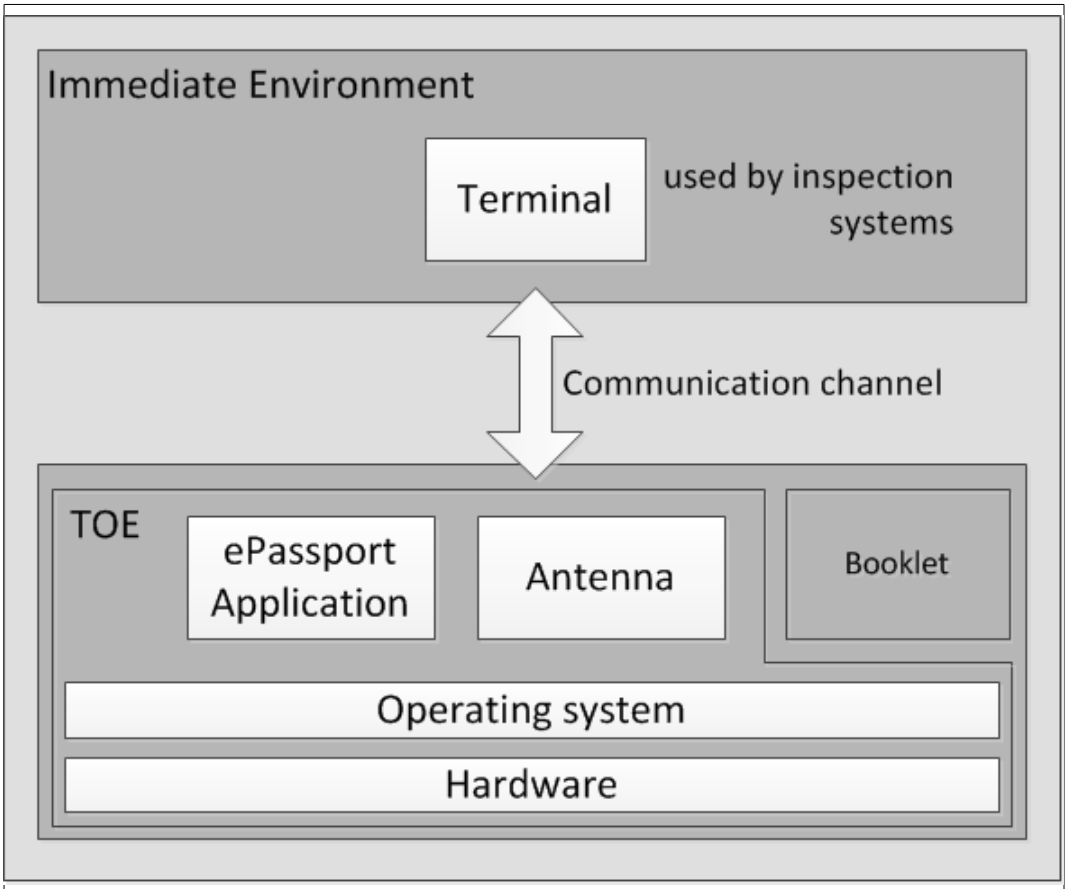

Figure 1: Scope of the MRTD, structural view

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 9.2.6 Usage of platform TSF by TOE TSF a detailed mapping shows how the platform TSF are separated into

1. relevant platform TSF being used by the composite ST, see Table 10: Relevant platform SFRs used by Composite ST, and
2. irrelevant platform TSF not being used by the composite ST, see Table 11: Irrelevant platform SFRs not being used by Composite ST.

4.1 CC Conformance Claim

This ST claims conformance to the Common Criteria version 3.1 Release 4,

- [CC-3.1-P1]
- [CC-3.1-P2]
- [CC-3.1-P3].

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2007-09-004, Version 3.1, Revision 4, September 2007, [CEM-3.1]

is taken into account.

4.2 PP Claim, Package Claim

This Security Target claims strict conformance to the Protection Profile

- Machine Readable Travel Document with "ICAO Application", Basic Access Control [BSI-CC-PP-0055-110].

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

- ALC_DVS.2 as defined in CC part 3 [CC-3.1-P3].

Note:

1. The Protection Profile [BSI-CC-PP-0055-110] has been certified by the Bundesamt fï¿½r Sicherheit in der Informationstechnik (BSI), cf. [BSI-CR-CC-PP-0055-110].

4.3 Conformance Rationale

No rational is necessary because

- 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 PP without changes
- the chapter 6 Security Objectives (ASE_OBJ) is taken over from the claimed PP without changes
- the chapter 7 Extended Component Definition (ASE_ECD) is taken over from the claimed PP without changes
- the chapter 8 Security Requirements (ASE_REQ) is taken over from the claimed PP without changes.

5 Security Problem Definition (ASE_SPD)

5.1 Introduction

Assets

The assets to be protected by the TOE include the User Data on the MRTD's chip.

Logical MRTD Data

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [ICAO-9303-2006]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons as the 'ICAO Doc 9303' [ICAO-9303-2006] the TOE described in this ST specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG4) [2].

A sensitive asset is the following more general one.

Authenticity of the MRTD's chip

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

5.1.1 Subjects

This ST considers the following subjects:

Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities

1. establishing the identity the holder for the biographic data in the MRTD,
2. enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s)
3. writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability,

2 Cf. [CC-3.1-P1] for details how to access these User data under EAC protection.

4. writing the initial TSF data and (iv) signing the Document Security Object defined in [ICAO-9303-2006].

Terminal

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

Inspection system (IS)

A technical system used by the border control officer of the receiving State

1. examining an MRTD presented by the traveler and verifying its authenticity and
2. verifying the traveler as MRTD holder.

The Basic Inspection System (BIS)

1. contains a terminal for the contactless communication with the MRTD's chip,
2. implements the terminals part of the Basic Access Control Mechanism and
3. gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism.

The Extended Inspection System (EIS) in addition to the General Inspection System

1. implements the Terminal Authentication Protocol and
2. is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

The security attributes of the EIS are defined of the Inspection System Certificates.

Note:

1. This ST does not distinguish between the BIS, GIS and EIS because the Active Authentication and the Extended Access Control is outside the scope (cf. application note 6 of [BSI-CC-PP-0055-110]).

MRTD Holder

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

Traveler

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

Attacker

A threat agent trying

1. to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data),
2. to read or to manipulate the logical MRTD without authorization, or
3. to forge a genuine MRTD.

Note:

1. An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE (cf. application note 7 of [BSI-CC-PP-0055-110]).

5.2 Assumptions

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

5.2.1 A.MRTD_Manufact MRTD manufacturing on steps 4 to 6

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its

manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

5.2.2 A.MRTD_Delivery MRTD delivery during steps 4 to 6

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

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

5.2.3 A.Pers_Agent Personalization of the MRTD's chip

The Personalization Agent ensures the correctness of

i. the logical MRTD with respect to the MRTD holder,
ii. the Document Basic Access Keys,
iii. the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and
iv. the Document Signer Public Key Certificate (if stored on the MRTD's chip).

The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

5.2.4 A.Insp_Sys Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State

i. examining an MRTD presented by the traveler and verifying its authenticity and
ii. verifying the traveler as MRTD holder.

The Basic Inspection System for global interoperability

i. includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and
ii. implements the terminal part of the Basic Access Control [ICAO-9303-2006].

The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

Note:

1. According to [ICAO-9303-2006] the support of the Passive Authentication mechanism is mandatory whereas the the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST (cf. application note 8 of [BSI-CC-PP-0055-110]).

5.2.5 A.BAC-Keys Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [ICAO-9303-2006], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

Note:

1. When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date (cf. application note 9 of [BSI-CC-PP-0055-110]).

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.

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

5.3.1.1 T.Chip_ID Identification of MRTD's chip

Adverse action:

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.

Threat agent:

having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset:

Anonymity of user.

5.3.1.2 T.Skimming Skimming the logical MRTD

Adverse action:

An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.

Threat agent:

having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset:

confidentiality of logical MRTD data.

5.3.1.3 T.Eavesdropping Eavesdropping to the communication between TOE and inspection system

Adverse action:

An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

Threat agent:

having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset:

confidentiality of logical MRTD data.

5.3.1.4 T.Forgery Forgery of data on MRTD's chip

Adverse action:

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

Threat agent:

having enhanced basic attack potential, being in possession of one or more legitimate MRTDs

Asset:

authenticity of logical MRTD data.

5.3.2 The TOE shall avert the threats as specified below

5.3.2.1 T.Abuse-Func Abuse of Functionality

Adverse action:

An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order

1. to manipulate User Data,
2. to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or
3. to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

Threat agent:

having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset:

confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

5.3.2.2 T.Information_Leakage Information Leakage from MRTD's chip

Adverse action:

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

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 the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

Threat agent:

having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset:

confidentiality of logical MRTD and TSF data.

5.3.2.3 T.Phys-Tamper Physical Tampering

Adverse action:

An attacker may perform physical probing of the MRTD's chip in order

1. to disclose TSF Data or
2. to disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD's chip in order to

1. modify security features or functions of the MRTD's chip,
2. modify security functions of the MRTD's chip Embedded Software,
3. modify User Data or
4. to modify TSF data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) 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 direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and 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.

Threat agent:

having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset:

confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

5.3.2.4 T.Malfunction Malfunction due to Environmental Stress

Adverse action:

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to

1. deactivate or modify security features or functions of the TOE or
2. circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent:

having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset:

confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

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).

5.4.1 P.Manufact Manufacturing of the MRTD's chip

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

5.4.2 P.Personalization Personalization of the MRTD 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 MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by the issuing State or Organization only.

5.4.3 P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) [3] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO-9303-2006].

Note:

1. The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO-9303-2006]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent (cf. application note 10 of [BSI-CC-PP-0055-110]).

3 Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by this ST.

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.

6.1.1 OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD 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 MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Note:

1. The OT.AC_Pers implies that
   1. the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,
   2. the Personalization Agents may
      i. add (fill) data into the LDS data groups not written yet, and
      ii. update and sign the Document Security Object accordingly.

      The support for adding data in the "Operational Use" phase is optional (cf. application note 11 of [BSI-CC-PP-0055-110]).

6.1.2 OT.Data_Int Integrity of personal data

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

6.1.3 OT.Data_Conf Confidentiality of personal data

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

Note:

1. The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the MRTD.
   The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [ICAO-9303-2006] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful

Enhanced Access Control not covered by this ST. Thus the read access must be prevented even in case of a successful BAC Authentication. (cf. application note 12 of [BSI-CC-PP-0055-110]).

6.1.4 OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre- Personalization data includes writing of the Personalization Agent Key(s). In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

Note:

1. The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the MRTD". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent (cf. application note 13 of [BSI-CC-PP-0055-110]).

6.1.5 OT.Prot_Abuse-Func Protection against Abuse of Functionality

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to

i. disclose critical User Data,
ii. manipulate critical User Data of the IC Embedded Software,
iii. manipulate Soft-coded ICEmbedded Software or
iv. bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

Note:

1. This security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

6.1.6 OT.Prot_Inf_Leak Protection against Information Leakage

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip

- 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 and
- 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. Details correspond to an analysis of attack scenarios which is not given here (cf. application note 14 of [BSI-CC-PP-0055-110]).
2. This security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

6.1.7 OT.Prot_Phys-Tamper Protection against Physical Tampering

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with enhanced-basic attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips 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 charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, 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 functions.

Note:

1. This security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

6.1.8 OT.Prot_Malfunction Protection against Malfunctions

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

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 objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE's internals (cf. application note 15 of [BSI-CC-PP-0055-110]).
2. This security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

6.2 Security Objectives for the Operational Environment

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.MRTD_Manufact Protection of the MRTD Manufacturing

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

OE.MRTD_Delivery Protection of the MRTD delivery

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

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

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

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

6.2.1.2 OE.Personalization Personalization of logical MRTD

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization

i. establish the correct identity of the holder and create biographical data for the MRTD,
ii. enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and
iii. personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

6.2.1.3 OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

The issuing State or Organization must

i. generate a cryptographic secure Country Signing CA Key Pair,
ii. ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and
iii. distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity.

The issuing State or Organization must

i. generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys,
ii. sign Document Security Objects of genuine MRTD in a secure operational environment only and
iii. distribute the Certificate of the Document Signer Public Key to receiving States and Organizations.

The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO-9303-2006].

6.2.1.4 OE.BAC-Keys Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [ICAO-9303-2006] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

6.2.2 Receiving State or Organization

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

6.2.2.1 OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability

(i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303-2006].

6.2.2.2 OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the receiving State uses the inspection system to verify the traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data

elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

6.2.2.3 OE.Prot_Logical_MRTD Protection of data from the logical MRTD

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

6.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

Table 1: Security Objective Rationale

	OT.AC_Pers	OT.Data_Int	OT.Data_conf	OT.identification	OT.Prot_Abuse_Func	OT.Prot_Inf_leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Perzonalization	OE.Pass_Auth_Sign	OE.BAC_Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				x									x			
T.Skimming			x										x			
T.Eavesdropping			x													
T.Forgery	x	x					x					x		x	x	
T.Abuse-Func					x						x					
T.Information_Leakage						x										
T.Phys-Tamper							x									
T.Malfunction								x								
P.Personalization	x			x							x					
P.Personal_Data		x	x													
A.MRTD_Manufact									x							

A.MRTD_Delivery										x						
A.Pers_Agent											x					
A.Insp_Sys														x		x
A.BAC-Keys													x			

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

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

i. the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD", 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 MRTD". 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 management of TSF to the Personalization Agent.

The **OSP P.Personal_Data** "Personal data protection policy" requires the TOE

i. to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and
ii. enforce the access control for reading as decided by the issuing State or Organization.

This policy is implemented by the security objectives **OT.Data_Int** "Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT.Data_Conf** "Confidentiality of personal data" describes the protection of the confidentiality.

The threat **T.Chip_ID** "Identification of MRTD's chip" addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered as described by the security objective **OT.Identification** by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Skimming** "Skimming digital MRZ data or the digital portrait" and **T.Eavesdropping** "Eavesdropping to the communication between TOE and inspection system" address the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective **OT.Data_Conf** "Confidentiality of personal data" through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Forgery** "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRTD passport book according to **OE.Exam_MRTD** "Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** "Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif** "Verification by Passive Authentication".

The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks using the MRTD's chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality". Additionally this objective is supported by the security objective for the TOE environment: **OE.Personalization** "Personalization of logical MRTD" ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are

enabled according to the intended use of the TOE.

The threats **T.Information_Leakage** "Information Leakage from MRTD's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high [4] attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak** "Protection against Information Leakage", **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot_Malfunction** "Protection against Malfunctions".

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

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

The assumption **A.Pers_Agent** "Personalization of the MRTD's chip" is covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD" including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the MRTD passport book". The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data from the logical MRTD" will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

The assumption **A.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" is directly covered by the security objective for the TOE environment **OE.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization

4 "high" should be read "moderate".

7 Extended Component Definition (ASE_ECD)

This ST uses components defined as extensions to CC part 2. Some of these components are defined in [BSI-CR-CC-PP-0055-110], other components are defined in this ST.

7.1 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.

7.2 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].

7.3 Definition of the Family FMT_LIM

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

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

The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1

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

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

FMT_LIM.2 Limited availability

Hierarchical to:

No other components

Dependencies:

FMT_LIM.1 Limited capabilities

FMT_LIM.2.1

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

Note:

1. The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the 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 test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

   The combination of both requirements shall enforce the policy.

7.4 Definition of the Family FPT_EMSEC

The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of [CC-3.1-P2].

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

FPT_EMSEC TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC TOE Emanation	1

FPT_EMSEC.1 TOE Emanation has two constituents:

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.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_EMSEC.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", "Basic Inspection System" and "Terminal" used in the following chapter is given in section 5.1 Introduction. Note, that all these subjects are acting for homonymous external entities. All used objects are defined in section 2.4 Terms and Definitions. The operations "write", "read", "modify", and "disable read access" are used in accordance with the general linguistic usage. The operations "transmit", "receive" and "authenticate" are originally taken from [CC-3.1-P2].

Definition of security attributes:

Table 2: Definition of security attributes

security attribute	values	meaning
Terminal Authentication Status	none (any Terminal)	default role (i.e. without authorization after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2
	Personalization Agent	Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2

Notes:

1. Security attribute Terminal Authentication Status is spelled differently in PP [BSI-CC-PP-0055-110], e.g. FDP_ACF.1 spells it authentication status of terminals.
2. These different spellings are corrected by refinements to read always Terminal Authentication Status.

8.1 Security Functional Requirements for the TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

8.1.1 Class FAU Security Audit

8.1.1.1 FAU_SAS.1 Audit storage

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

FAU_SAS.1.1

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

Note:

1. The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS)

8.1.2 Class Cryptographic support (FCS)

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

8.1.2.1 FCS_CKM.1 Cryptographic key generation - Generation of Document Basic Access Keys by the TOE

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

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bits that meet the following: [ICAO-9303-2006], normative appendix 5.

Note:

1. The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [ICAO-9303-2006], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO-9303-2006], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1

8.1.2.2 FCS_CKM.4 Cryptographic key destruction - MRTD

Hierarchical to: No other components.

Dependencies:

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

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with zeros** [5] that meets the following: **none** [6].

Note:

1. The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging

8.1.3 Cryptographic operation (FCS_COP.1)

8.1.3.1 FCS_COP.1/SHA Cryptographic operation - Hash for Key Derivation

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/SHA

The TSF shall perform hashing in accordance with a specified cryptographic algorithm **SHA-1** [7] and cryptographic key sizes none that meet the following: **FIPS 180-4** [8].

Notes:

1. This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [ICAO-9303-2006]
2. SHA-1 is provided by CardOS DI V5.3.

8.1.3.2 FCS_COP.1/ENC Cryptographic operation - Encryption / Decryption Triple DES

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/ENC

The TSF shall perform secure messaging (BAC) - encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bits that meet the following: [FIPS-46-3-1999] and [ICAO-9303-2006] normative appendix 5, A5.3.

Notes:

1. This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.
2. This TOE uses the Triple-DES provided by the underlying chip SLE78CLFX*P (M7892 B11).
3. For the "secure messaging - encryption and decryption" using TDES see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.2 Triple-DES Operation.

5 [assignment: cryptographic key destruction method]
6 [assignment: list of standards]
7 [selection: SHA-1 or other approved algorithms]
8 [selection: FIPS 180-2 or other approved standards]

8.1.3.3 FCS_COP.1/AUTH Cryptographic operation - Authentication

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/AUTH

> The TSF shall perform symmetric authentication - encryption and decryption in accordance with a specified cryptographic algorithm **AES in CBC mode** [9] and cryptographic key sizes **128 and 256** [10] bits that meet the following: **[FIPS-197-2001]** [11].

Note:

1. This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).
2. This TOE uses the AES provided by the underlying chip SLE78CLFX*P (M7892 B11).
3. For the "Advanced Encryption Standard (AES)" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.3 AES Operation.
4. The key used for authentication is provided with a usecounter. The usecounter is decremented by one in case of that the correct key is used and in case of that a wrong key is used. The usecounter is less than 10.
5. The key stored on the card for authentication is individual to the chip.

8.1.3.4 FCS_COP.1/MAC Cryptographic operation - Retail 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/MAC

> The TSF shall perform secure messaging - message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).

Note:

1. 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 the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.
2. This TOE uses the Triple-DES provided by the underlying chip SLE78CLFX*P (M7892 B11).
3. For the "Triple-DES encrypting and decrypting" see [Infineon-ST-Chip-B11-2015-10-13], 7.1.4.2 Triple-DES Operation.

8.1.4 Random Number Generation (FCS_RND.1)

The TOE shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below (Common Criteria Part 2 extended).

9 [selection: Triple-DES, AES]
10 [selection:112, 128, 168, 192, 256]
11 [selection: FIPS 46-3 [9], FIPS 197 [12]]

8.1.4.1 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 **random numbers generation Class PTG.2 according to [BSI-AIS31-V3]** [12].

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 used for the authentication protocols as required by FIA_UAU.4.

8.1.5 Class FIA Identification and Authentication

The Table 3: Overview on authentication SFR provides an overview on the authentication mechanisms used.

Table 3: Overview on authentication SFR

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO-9303-2006], normative appendix 5, and [BSI-TR-03110-1-V210]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	AES with 128 or 256 bit keys (cf. FCS_COP.1/AUTH)

8.1.5.1 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1

The TSF shall allow

1. to read the Initialization Data in Phase 2 "Manufacturing",
2. to read the random identifier in Phase 3 "Personalization of the MRTD",
3. to read the random identifier in Phase 4 "Operational Use"
4. **to run self tests according to** FPT_TST.1 [13].

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

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

12 [assignment: a defined quality metric]
13 REFINEMENT

Notes:

1. The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 "Manufacturing". The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System
2. In the "Operational Use" phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD's chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID

8.1.5.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1

The TSF shall allow

1. to read the Initialization Data in Phase 2 "Manufacturing",
2. to read the random identifier in Phase 3 "Personalization of the MRTD",
3. to read the random identifier in Phase 4 "Operational Use"
4. **to run self tests according to** FPT_TST.1 [14].

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

FIA_UAU.1.2

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

Note:

1. The Basic Inspection System and the Personalization Agent authenticate themselves

8.1.5.3 FIA_UAU.4 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

The TSF shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on **AES** [15]

Notes:

1. The TOE uses a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.
2. The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO-9303-2006]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to

14 REFINEMENT
15 [selection: Triple-DES, AES or other approved algorithms]

the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE stops further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

8.1.5.4 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1

The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on **AES** [16]

to support user authentication.

FIA_UAU.5.2

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

1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) **the Symmetric Authentication Mechanism with the Personalization Agent Key** [17]
2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

Notes:

1. In case the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control' [BSI-PP-0056-V2-2012-132] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES. The Personalization Agent could be authenticated by using the symmetric AES-based authentication mechanism or other (e.g. the Terminal Authentication Protocol using the Personalization Key, cf. [BSI-PP-0056-V2-2012-132] FIA_UAU.5.2).
2. The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

8.1.5.5 FIA_UAU.6 Re-authenticating - Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1

The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

Notes:

1. The Basic Access Control Mechanism specified in [ICAO-9303-2006] includes the 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 Retail-MAC whether it was sent by the successfully

16 [selection: Triple-DES, AES]

17 [selection: the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]]

authenticated terminal (see FCS_COP.1/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 BAC user.

2. Note that in case the TOE should also fulfill [BSI-PP-0056-V2-2012-132] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

8.1.5.6 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when **2** [18] unsuccessful authentication attempt occurs related to **authentication attempts using BAC during one card session** [19].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been **met** [20], the TSF shall **delay the next authentication attempt at least 6 seconds**. [21]

Note:

1. With a delay at least 6 seconds a brute force attack lasts in the average about 28 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.

8.1.6 Class FDP User Data Protection

8.1.6.1 Subset access control (FDP_ACC.1)

8.1.6.1.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

The TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.

8.1.6.2 Security attribute based access control (FDP_ACF.1)

8.1.6.2.1 FDP_ACF.1 Basic Security attribute based access control - Basic Access Control

Hierarchical to: No other components.

18 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
19 [assignment: list of actions]
20 [assignment: met or surpassed]
21 [assignment: list of actions]

Dependencies:

- FDP_ACC.1 Subset access control
- FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

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

1. Subjects:
   a. Personalization Agent,
   b. Basic Inspection System,
   c. Terminal,
2. Objects:
   a. data EF.DG1 to EF.DG16 of the logical MRTD,
   b. data in EF.COM,
   c. data in EF.SOD,
3. Security attributes
   a. **Terminal Authentication Status** [22].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.

FDP_ACF.1.3

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

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the rule:

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.

Note:

1. The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this ST (cf. [BSI-PP-0056-V2-2012-132] for details).

8.1.6.3 Inter-TSF-Transfer

Note:

1. FDP_UCT.1 and FDP_UIT.1 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 authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

8.1.6.4 FDP_UCT.1 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

22 REFINEMENT authentication status of terminals

- [FDP_ACC.1 Subset access control, or
- FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1

The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure.

8.1.6.5 FDP_UIT.1 Data exchange integrity - 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_UIT.1.1

The TSF shall enforce the Basic 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

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

8.1.7 Class FMT Security Management

Note:

1. The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

8.1.7.1 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.

8.1.7.2 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1

The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Basic Inspection System.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

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.

8.1.7.3 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 disclosed or manipulated
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.

8.1.7.4 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 disclosed or manipulated,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.

Note:

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

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.

8.1.7.5 FMT_MTD.1/INI_ENA Management of TSF data - Writing of Initialization Data and Prepersonalization Data

Hierarchical to: No other components.

Dependencies:

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

FMT_MTD.1.1/INI_ENA

The TSF shall restrict the ability to write the Initialization Data and Prepersonalization Data to the Manufacturer.

Note:

1. The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key

8.1.7.6 FMT_MTD.1/INI_DIS Management of TSF data - Disabling of Read Access to Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

Dependencies:

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

FMT_MTD.1.1/INI_DIS

The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.

Note:

1. According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Prepersonalization Data by
   i. allowing to write these data only once and
   ii. blocking the role Manufacturer at the end of the Phase 2.
   The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access will be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

8.1.7.7 FMT_MTD.1/KEY_WRITE Management of TSF data - Key Write

Hierarchical to: No other components. Dependencies:

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

FMT_MTD.1.1/KEY_WRITE

The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

8.1.7.8 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 Document Basic Access Keys and Personalization

Agent Keys to none.

Note:

1. The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

8.1.8 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_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSF testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFRs "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and 2Resistance to physical attack (FPT_PHP.3)" together with the SAR "Security architecture description" (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

8.1.8.1 FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMSEC.1.1

The TOE shall not emit

the shape and amplitude of signals

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

during internal operations or data transmissions [23]

in excess of **unintelligible limits** [24] enabling access to

1. Personalization Agent Key(s)
2. **Document Basic Access Keys** [25]
3. **none** [26].

FPT_EMSEC.1.2

The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) **and Document Basic Access Keys** [27] and **none** [28].

Note:

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

23 [assignment: types of emissions]
24 [assignment: specified limits]
25 REFINEMENT
26 [assignment: list of types of user data]
27 REFINEMENT
28 [assignment: list of types of user data]

8.1.8.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

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

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

8.1.8.3 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 Data according to** FMT_MTD.1/INI_DIS
3. **Reading data of LDS groups and EF.SOD**
4. **Reading Document Basic Access Keys**
5. **Generating random numbers according to** FCS_RND.1 [29]

to demonstrate the correct operation of the TSF.

FPT_TST.1.2

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

FPT_TST.1.3

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

Note:

1. The MRTD's chip uses state of the art smart card technology it will run self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorized user" Manufacturer in the Phase 2 Manufacturing. Other self tests run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 "Operational Use", e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks.

8.1.8.4 FPT_PHP.3 Resistance to physical attack

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

FPT_PHP.3.1

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

Notes:

1. The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP

29 [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]]

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.

2. The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [CC-3.1-P2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

8.2 Security Assurance Requirements for the TOE

The Security 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 component:

ALC_DVS.2.

8.3 Security Requirements Rationale

8.3.1 Security Functional Requirements Rationale

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

Table 4: Functional Requirement to TOE security objective mapping

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuuncntion	OT.Prot_Abusse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					
FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_RND.1	x	x	x					

FIA_UID.1			x	x				
FIA_AFL.1			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4	x	x	x					
FIA_UAU.5	x	x	x					
FIA_UAU.6	x	x	x					
FDP_ACC.1	x	x	x					
FDP_ACF.1	x	x	x					
FDP_UCT.1	x	x	x					
FDP_UIT.1	x	x	x					
FMT_SMF.1	x	x	x					
FMT_SMR.1	x	x	x					
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA				x				
FMT_MTD.1/INI_DIS				x				
FMT_MTD.1/KEY_WRITE	x	x	x					
FMT_MTD.1/KEY_READ	x	x	x					
FPT_EMSEC.1	x				x			
FPT_TST.1					x		x	
FPT_FLS.1	x				x		x	
FPT_PHP.3	x				x	x		

8.3.1.1 The security objective OT.AC_Pers "Access Control for Personalization of logical MRTD"

addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and

FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [BSI-PP-0056-V2-2012-132] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

8.3.1.2 The security objective OT.Data_Int "Integrity of personal data"

requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

The security objective OT.Data_Int "Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

8.3.1.3 The security objective OT.Data_Conf "Confidentiality of personal data"

requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

8.3.1.4 The security objective OT.Identification "Identification and Authentication of the TOE"

address the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1. Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. FIA_UAU.4 note 1). In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

8.3.1.5 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.

8.3.1.6 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 MRTD'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_EMSEC.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.

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

is covered by the SFR FPT_PHP.3.

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

is covered by

i. the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and
ii. the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

8.3.2 Dependency Rationale

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

The Table 5: Dependencies between the SFR for the TOE shows the dependencies between the SFR of the TOE.

Table 5: Dependencies between the SFR for the TOE

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or	Fulfilled by FCS_COP.1/ENC, and

SFR	Dependencies	Support of the Dependencies
	FCS_COP.1 Cryptographic operation],	FCS_COP.1/MAC
	FCS_CKM.4 Cryptographic key destruction	Fulfilled FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or	Fulfilled by FCS_CKM.1
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes,	justification 1 for non-satisfied dependencies
	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
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1
	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
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes,	justification 2 for non-satisfied dependencies
	FDP_ITC.2 Import of user data with security attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	justification 2 for non-satisfied dependencies
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1
	FDP_ITC.2 Import of user data with security	

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

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

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

No. 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

No. 2: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

No. 3: The access control TSF according to FDP_ACF.1 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. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

8.3.3 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 MRTD's development

and manufacturing especially for the secure handling of the MRTD's material.

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements Dependencies

ALC_DVS.2: no dependencies.

8.3.4 Security Requirements - Mutual Support and Internal Consistency

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

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

The dependency analysis in section 8.3.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

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 8.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

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. Basic Inspection System.

according to FMT_SMR.1.

The TOE allows

- identification of the user according to FIA_UID.1 before the authentication takes place according to FIA_UAU.1
- the execution of following TSF-mediated actions before the user is identified and associated with one of maintained roles
  1. to read the Initialization Data in Phase 2 "Manufacturing",
  2. to read the random identifier in Phase 3 "Personalization of the MRTD",
  3. to read the random identifier in Phase 4 "Operational Use"
  4. to run self tests according to FPT_TST.1.
- the execution of following TSF-mediated actions before the user is authenticated
  1. to read the Initialization Data in Phase 2 "Manufacturing",
  2. to read the random identifier in Phase 3 "Personalization of the MRTD",
  3. to read the random identifier in Phase 4 "Operational Use"
  4. to run self tests according to FPT_TST.1.

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 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 (1) the TOE maintains the role of the Manufacturer.

Reading of the Document Basic Access Keys is not allowed according to FMT_MTD.1/KEY_READ.

9.1.1.2 Personalization Agent Identification and Authentication

The Personalization Agent can be identified and authenticated according to

- FMT_SMR.1 (2)
- FIA_UAU.5 (2)

using

- the 9.1.2.1 BAC protocol
- the symmetric authentication using FCS_COP.1/AUTH.

Note:

1. The symmetric key stored for authentication is individual to the chip.

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

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_EMSEC.1 (1).

Only the Personalization Agent is able

- to write the Document Basic Access Keys (FMT_MTD.1/KEY_WRITE)

Reading of the Document Basic Access Keys is not allowed (FMT_MTD.1/KEY_READ).

With FIA_UAU.4 (2) the TOE prevents reuse of Document Basic Access Keys.

With FMT_MTD.1/INI_DIS the Personalization Agent disables the read access of IC Identification Data before issuing the MRTD to the card holder, see also 9.1.1.1 Travel document manufacturer Identification and Authentication point 2.c.

For this TOE the Personalization Agents invalidate always their keys before issuing to the card Holder. The authorized Personalization Agents are **not** allowed to add (**and** not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 "Operational Use" after issuing the travel document to the MRTD holder. (cf. Application note 4 of [BSI-CC-PP-0055-110])

9.1.1.3 Terminal Identification and Authentication

A terminal used by a Basic Inspection System can be identified and authenticated according to

- FMT_SMR.1 (3)

using

- the 9.1.2.1 BAC protocol.

The usage of the

- Document Basic Access Keys

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_EMSEC.1 (2).

With FIA_UAU.4 (1) the TOE prevents reuse of Document Basic Access Keys.

9.1.2 Protocols

The TOE support the following protocols.

9.1.2.1 BAC protocol

The TOE accepts authentications using the BAC protocol according to

- FMT_SMR.1 (2) and (3)
- FIA_UAU.5 (1)

using

- FCS_CKM.1

which is also used for establishing 9.1.4 Secure messaging.

If the terminal (or the Personalization Agent see 9.1.1.2 Personalization Agent Identification and Authentication) uses a wrong password, the TOE delays the next attempt to establish the PACE protocol at least 5 seconds according to

- FIA_AFL.1.

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

If the BAC protocol is performed successfully, the TOE sets the security attribute Terminal Authentication Status (FDP_ACF.1.1 (3.a)).

The BAC protocol requires to generate session key using FCS_CKM.1 which are destructed

With FIA_UAU.5 (1) the TOE provide

9.1.3 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
- FDP_ACF.1

after establishing 9.1.4 Secure messaging according to FDP_ACF.1.4 (2):

1. If security attribute Terminal Authentication Status (FDP_ACF.1.1 (3.a)) is set (i.e. the 9.1.2.1 BAC protocol is performed successfully, value Basic Inspection System)

then

- the inspection system is allowed to read data objects (FDP_ACF.1.2):
  EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD

2. If security attribute Terminal Authentication Status (FDP_ACF.1.1 (3.b)) has the value "Personalization Agent" (i.e. the Personalization Agent is successfully authenticated), the Personalization Agent is allowed to

- write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,

9.1.4 Secure messaging

With FCS_CKM.1 (cf. [ICAO-9303-2006], normative appendix 5, A5.2) and FCS_COP.1/SHA and FCS_RND.1 (cf. [ICAO-9303-2006], normative appendix 5, A5.1) the TOE

- is able to generate session keys

which support

- FDP_UCT.1 (to protected from unauthorised disclosure) and
- FDP_UIT.1 (to protected from modification, deletion, insertion and replay errors)

using

- FCS_COP.1/ENC for confidentiality (by encrypting the data)
- FCS_COP.1/MAC for integrity (by MACing the commands)

to establish secure messaging (cf. [ICAO-9303-2006], normative appendix 5, A5.3).

After successful authentication of the terminal with Basic Access Control Authentication Mechanism the secure messaging is established and the TOE re-authenticate the user under the conditions each command sent according to

- FIA_UAU.6.

After the secure messaging is terminated the session key are destructed using FCS_CKM.4.

9.1.5 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.

9.1.6 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 Data according to** FMT_MTD.1/INI_DIS
3. **Reading data of LDS groups and EF.SOD**

4. **Reading Document Basic Access Keys**
5. **Generating random numbers according to** FCS_RND.1

according to FPT_TST.1.

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

- 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
- 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.

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.

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 6: 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 7: 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]		

Assumptions of the HW platform related to its operational environment	Meaning	OT of this composite TOE
A.Resp-Appl	Treatment of User Data	OT.Data_Int OT.Data_Conf 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 6: Irrelevant assumptions of platform for its Operational Environment and Table 7: 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 8: 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.Data_Int	OT.Data_Conf
O.Phys-Manipulation	x						
O.Phys-Probing	x						
O.Malfunction	x	x					
O.Leak-Inherent			x				
O.Leak-Forced			x			x	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.Data_Int	OT.Data_Conf
O.Abuse-Func				x			
O.Identification					x		
O.RND						x	x
O.Add-Functions						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.AC_Pers

since no security objectives of the Platform-ST provides a functionality needed by this TOE.

With table Table 8: 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 and it is covered by organizational security policy

- P.Manufact

of the Composite-ST.

OSP P.Add-Functions of the platform is relevant and it is needed by security objectives of the TOE

- OT.Data_Int (AES and TDES)

The organizational security policies of the Platform-ST and the OTs of this Composite-ST are not contradictory.

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 8: Mapping of security objectives of platform and threats mapped to this OTs by Table 1: Security Objective Rationale and the threats of the Platform-ST ([Infineon-ST-Chip-B11-2015-10-13] section 4.1 "Threats" and section 4.1.1 "Additional Threat due to TOE specific Functionality").

Table 9: 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-Function	T.Skimming	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
T.Abuse-Func					x		
T.RND						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 10: 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

RP_SFR	Meaning	Used by TOE SFR
FDP_ITT.1	Basic Internal Transfer Protection	FPT_EMSEC.1
FDP_IFC.1	Subset Information Flow Control	FPT_EMSEC.1
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	FPT_EMSEC.1
FCS_RNG.1	Quality Metric for Random Numbers	FCS_CKM.1 FCS_RND.1 FIA_UID.1 for ► (2) read the RI in phase 3 ► (3) to read RI in phase 4 FPT_EMSEC.1 (blinding)
FPT_TST.2	Subset TOE Security Testing	FPT_TST.1 FPT_PHP.3 (active shield and sensors)
FCS_COP.1/DES	Cryptographic Support (3DES)	FCS_COP.1/ENC (TDES), FCS_COP.1/MAC (TDES)
FCS_COP.1/AES	Cryptographic Support (AES)	FCS_COP.1/AUTH (AES)
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 11: 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_SMF.1	Specification of Management Functions	Not used by TSF
FMT_MSA.3	Static Attribute Initialization	Not used by TSF
FCS_CKM.1/RSA	Cryptographic Key Generation (RSA)	Not used by TSF

IP_SFR	Meaning	Comment
FCS_COP.1/RSA	Cryptographic Support (RSA)	Not used by TSF
FCS_CKM.1/EC	Cryptographic key generation	Not used by TSF
FCS_COP.1/ECDH	Cryptographic key generation	Not used by TSF
FCS_COP.1/ECDSA	Cryptographic Support (ECDSA)	Not used by TSF
FCS_COP.1/SHA	Cryptographic Support (SHA-2)	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, see note 2 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 12: Cryptographic mechanisms used

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments ST Reference
1	Authentication	BAC, Symmetric Authentication, Triple-DES (CBC)	NIST Special Publication 800-67 V1.1 (TDES) [NIST-800-38A-2001] (CBC)	112	[BSI-TR-03110-1-V210]	BIS-key (see note 1)
2		Symmetric Authentication, AES in CBC mode	FIPS PUB 197 (AES) [NIST-800-38A-2001] (CBC)	128, 256	[BSI-TR-03110-1-V210]	Personalization-key, FCS_COP.1/AUTH
3	Key Agreement	BAC Key Derivation, SHA-1	see Cryptographic primitive No. 9 (SHA-1)	-	[BSI-TR-03110-1-V210]	FCS_COP.1/SHA
4		Document Basic Access Key Derivation Algorithm	[ICAO-9303-2006] normative appendix 5	-	[BSI-TR-03110-1-V210]	FCS_CKM.1
5	Confidentiality	Secure Messaging, TDES in CBC mode	NIST Special Publication 800-67 V1.1 (TDES) [NIST-800-38A-2001] (CBC) [ICAO-9303-2006] normative appendix 5	112	[BSI-TR-03110-1-V210]	FCS_COP.1/ENC (see note 4)
6	Integrity	Secure Messaging, TDES in Retail MAC mode Sequence Message Counter, padding mode 2	NIST Special Publication 800-67 V1.1 (TDES) [ISO-IEC-9797-1-2011] algorithm 3 and padding method 2 (Retail MAC)	112	[ICAO-9303-2006], [BSI-TR-03110-1-V210]	FCS_COP.1/MAC (see note 4)

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments ST Reference
7	Trusted Channel	ICAO BAC Secure Messaging established during BAC	[ICAO-9303-2006]	see No. 1, 5, 6	[ICAO-9303-2006], [BSI-TR-03110-1-V210]	FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC
8	Cryptographic primitive	PTG.2 random number generator	[BSI-AIS31-V3]	-	[BSI-TR-03116-2]	FCS_RND.1 (see note 3)
9		SHA-1	[NIST-FIPS-PUB-180-4]	-	[BSI-TR-03110-3-V211]	key derivation (see note 2)

Notes:

1. This TOE computes session keys according to [ICAO-9303-2006], normative appendix 5.
2. The hash algorithm SHA-1 is provided by CardOS DI V5.3.
3. For the challenge the random number generator of the underlying chip SLE78CLFX*P (M7892 B11) is used. The chip provides a Physical True Random Number Generator (PTRNG) which meets the requirements of the functionality class PTG.2 of the [BSI-AIS31-V3].
4. This TOE uses TDES provided by the underlying chip SLE78CLFX*P (M7892 B11). For TDES operation see [Infineon-ST-Chip-B11-2015-10-13], "7.1.4.2 Triple-DES Operation".

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], [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.