Security Target 'CardOS V6.0 ID R1.0 (BAC)'

Rev. 1.35R, Edition 11/2021

Contents

Atos Information Technology 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.

1 About this Document

1.1 Revision History

Table 1.1: History of released Versions

Version	Release date	Remarks
1.35R	2021-11-19	Release Version

1.2 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

CC
Common Criteria

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 term:*MRTD*

IC
Integrated Circuit

ICAO
International Civil Aviation Organization

ICC
Integrated Circuit Card

ICCSN
ICC Serial Number

IFD
Interface Device

IT
Information Technology

LCS
Life Cycle Status

LTD
Logical Travel Document

MF
Master File

MRTD
Machine Readable Travel Documents

MRZ
Non-block static secret key from Machine-Readable Zone, see [BSI-TR-03110-1-V220], section 2.3.

n.a.
not applicable

OCR
Optical Character Recognition

OSP
Organizational Security Policy

PACE
Password Authenticated Connection Establishment, see [ICAO-9303-2015], Part 11.

PCD
Proximity Coupling Device

PICC
Proximity Integrated Circuit Chip

PP
Protection Profile

PTRNG
Physical True Random Generator (short: physical RNG)

PT
Personalization Terminal

RF
Radio Frequency

RSA
Public key algorithm invented by Rivest, Shamir and Adleman

SAR
Security Assurance Requirements

SCIC
Smart Card IC

SE
Security Environment

SFP
Security Function Policy

SFR
Security Functional Requirement

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

TDES
Triple DES

TOE
Target Of Evaluation

TSF
TOE Security Functions

TSP
TOE Security Policy (defined by the current document)

TSS
TOE Summary Specification

1.3 Terms and Definitions

1.3.1 Security Evaluation Terms

Common Criteria Set of rules and procedures for evaluating the security properties of a product Note 1 to entry: see bibliography for details on the specification of *Common Criteria*.

Evaluation Assurance Level Set of assurance requirements for a product, its manufacturing process and its security evaluation specified by *Common Criteria*.

Protection Profile Document specifying security requirements for a class of products that conforms in structure and content to rules specified by *Common Criteria*.

Security Target 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 Profile*.

Target of Evaluation Abstract reference in a document, such as a *Protection Profile*, for a particular product that meets specific security requirements.

TOE Security Functions Functions implemented by the TOE to meet the requirements specified for it in a *Protection Profile* or *Security Target*.

1.3.2 Technical Terms

Note:

1. The following terms are taken over from [BSI-CC-PP-0056-V2-2012-MA-02]. References are adapted, e.g. [6] used by [BSI-CC-PP-0056-V2-2012-MA-02] is now [ICAO-9303-2015].

Active Authentication Security mechanism defined in [ICAO-9303-2015] 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-9303-2015] 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-9303-2015]

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.

175 **Counterfeit** An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO-9303-2015]

Document Basic Access Key The [ICAO-9303-2015] 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.

180 **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-9303-2015]

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-9303-2015]

190 **Extended Access Control** Security mechanism identified in [ICAO-9303-2015] 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 195 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-9303-2015]

Global Interoperability The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data 200 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-9303-2015]

IC Dedicated Support Software That part of the IC Dedicated Software (refer to above) 205 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.

210 **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-9303-2015]

Improperly documented person A person who travels, or attempts to travel with: (a) 215 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-9303-2015]

Initialization Process of writing MRTD Initialization Data to the TOE, and preparing a ePassport Application for personalization.

220 **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-9303-2015]

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-9303-2015]

Issuing State The Country issuing the travel document. [ICAO-9303-2015]

Logical Data Structure (LDS) The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303-2015]. 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-9303-2015] 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-9303-2015] 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-9303-2015]

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-9303-2015]

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-9303-2015]. 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-9303-2015]

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-9303-2015], - 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 document.

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-V220], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303-2015] (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.

330 **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.

335 **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-9303-2015]

340 **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].

345 **Secondary image** A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO-9303-2015]

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
350 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
355 summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO-9303-2015] (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
360 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
365 application of the travel document as defined in [BSI-TR-03110-1-V220] 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
370 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-9303-2015]

375 **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.

1.4 List of Tables

385 ## 1.5 List of Figures

2 Security Target Introduction (ASE_INT)

This section provides document management and overview information that are required
390 by a potential user of the TOE to determine, whether the TOE fulfills her requirements.

2.1 ST Reference

Title Security Target 'CardOS V6.0 ID R1.0 (BAC)'

TOE 'CardOS V6.0 ID R1.0 (BAC)'

Sponsor Atos Information Technology GmbH

395 **Editor(s)** Atos Information Technology GmbH

CC Version 3.1 (Revision 5)

Assurance Level EAL4 augmented with ALC_DVS.2.

Status Release

Version 1.35R

400 **Date** 2021-11-19

Certification ID BSI-DSZ-CC-1172

Keywords ICAO, BAC, Basic Access Control, ID-Card, Machine Readable Travel Document, CardOS

2.2 TOE Reference

405 This ST refers to the TOE 'CardOS V6.0 ID R1.0 (BAC)'.

The developer of the TOE is Atos Information Technology GmbH.

2.3 TOE Overview

This ST defines the security objectives and requirements for the chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the Interna-
410 tional Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the 'ICAO Doc 9303' [ICAO-9303-2015].

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].

415 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.

420 The TOE utilizes the evaluation of the underlying platform, which includes the Infineon chip SLC52GDA448*, the Toolbox v2.08.007, Base v2.08.007, SHA-2 v1.12.001 and Symmetric Crypto Library (SCL) v2.04.002.

2.3.1 Usage and major security features of the TOE

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-9303-2015] 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-9303-2015]. 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-9303-2015].

[1] These additional biometric reference data are optional.

The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

470 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.

475 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
480 access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO-9303-2015], chapter 4.

2.3.2 TOE type

The TOE's type addressed by this ST is a smart card with several applications.

The evaluated application is a readable travel documents (MRTD's chip) programmed
485 according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303' [ICAO-9303-2015].

2.3.3 Non-TOE hardware/software/firmware

In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) with contacts according to [ISO-IEC-7816-part-4] or supporting the
490 contactless communication according to [ISO-IEC-14443-2018].

For using the Basic Access Control the terminal needs to be equipped with means to acquire the MRZ from the data page to derive the Basic Access keys. Furthermore, the terminal software needs to support the execution of the BAC protocol including the encryption of the communication channel with secure messaging.

495 For communication to the terminal the TOE supports contact-based and contactless communication but requires non-TOE hardware technology (bound-outs, module plates, inlays, antenna technology, etc.) for the physical communication layer.

Observe, that if the TOE is used within a travel document the contact-based communication interfaces are not connected because travel documents support contactless communication
500 only. Therefore, some descriptions in the ST put an emphasis on the contactless communication, in particular those refering to the use as a travel document. However, the TOE is technically capable to support BAC also via the contact-based interface which is just not connected in contactless-only travel documents. Furthermore, the TOE can also be used for general eID applications supporting dual interface communication. In these configurations,
505 the BAC protocol can also be executed over the contact-based interface.

There is no other explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features.

2.4 TOE Description

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-9303-2015].

The TOE comprises of

- the circuitry of the chip including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (Card Operating System, COS) including configuration and initialization data related to the security functionality of the chip,
- the MRTD application
- additinally selected applications implemented in the file-system to be installed, and
- the associated guidance documentation including description of the file system installation procedure.

The components of the TOE are therefore the hardware (IC) with the operating system CardOS(OS) ready for initialization with a selected dedicated object system. The TOE Design Specification gives a detailed description of the parts of TOE.

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 dedicated object systems (file systems) are specified in detail in the Admin Guidance. The file systems support all security functionality and mechanisms described within the ST. After initialization and during personalization, applications (data groups) required for the intended functionality and mechanisms and their access rights are created. Creation of the applications (i.e. the [ISO-IEC-7816-part-4] conforming file structure) including data groups and their access rights) is subject to a limited availability and limited capability policy defined in the family FMT_LIM. In particular, the TOE initialization mechanisms ensure that creation or alteration of the file system is not possible after Initialization (this excludes populating data groups with values, as is done in the personalization phase). This is necessary for the manufacturer to use a single IC for different configurations.

The Guidance documentation ([Atos-V60-ADM]) provides further requirements for the manufacturer and security measures required for protection of the TOE until reception by the end-user.

The hardware platform of the TOE is identified as SLC52GDA448* (CC certification identifier IFX_CCI_000005 Design Step H13), which means that this ST applies to all derivates of the IFC_CCI_000005. For the TOE the following derivates will be used which differ only in the input capacities on the contactless interface:

- SLC52GDA448A8, 27pF
- SLC52GDA448A9, 78pF

The chips can be delivered as wafer, or packaged in the modules M8.8, MCC8, MCS8 (27pF) or COM8.6, COM 10.6 (78pF) or other modules or packages. In case of a contactless module, the module may be integrated in an antenna inlay, which is then used to build a optically and machine readable smart card or ePassport booklet. A dual interface module may be integrated in a smart card. Note that the different contact technologies are not considered part of the TOE.

Since CardOS is implemented on an already certified IC (certification number BSI-DSZ-CC-1110-V3-2020) the evaluation considers the composite evaluation aspects ([BSI-AIS36-V5]). This composite ST is based on the ST of the underlying platform ([Infineon-ST-SLC52-H13]), which claims conformance to Security IC Platform Protection Profile ([BSI-CC-PP-0084-2014]). The compatibility between this ST and the platform ST is considered in detail in section *Compatibility between the Composite ST and the Platform-ST*.

2.4.1 Life Cycle Phases Mapping

The typical life cycle phases for the current TOE type are development, manufacturing, card issuing and operational use. The life cycle phase development includes development of the
560 IC itself and IC embedded software. Manufacturing includes IC manufacturing and smart card manufacturing, and installation of a card operating system. Card issuing includes completion of the operating system, installation of the smart card applications and their electronic personalization, i.e. tying the application data up to the card holder.

Operational use of the TOE is explicitly in the focus of the Protection Profiles. Nevertheless,
565 some TOE functionality is already available in the manufacturing and the card issuing life cycle phases. Therefore it is also considered by the Protection Profiles and this ST.

The life cycle of the concrete TOE is described in terms of the following five life cycle phases, divided in steps to better explain TOE specific life cycle aspects. Furthermore, additional explanations are given how these phases relate to the phase definitions in the standard
570 life-cycle used in the relevant PPs.

Life cycle phase A "Development"

Step 1: The TOE is developed in phase 1. The IC developer develops

- the integrated circuit,
- the IC dedicated software and
- 575 the guidance documentation associated with these TOE components.

Step 2: 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 card application(s) and the guidance documentation associated with these TOE components.

580 The software developer ships the IC embedded software in accordance with the certified delivery and loading procedures to the IC manufacturer. Furthermore, the software developer ships load scripts which in particular contain the certified object system layout(s) for the various configurations as well as the relevant guidance documentation securely to the Initializer.

585 **Life cycle phase B "IC Manufacturing"**

Step 3: In a first step, the TOE integrated circuit is produced. The IC manufacturer writes IC identification data onto the chip in order to track and control the IC as dedicated card material during IC manufacturing, and during delivery to the electronic document manufacturer. Additionally, the IC manufacturer adds the IC embedded software in the
590 non-volatile programmable memory using the certified loading mechanisms of the IC.

The IC is securely delivered from the IC manufacturer to the composite product manufacturer.

Step 4 (optional): The IC may be delivered as a wafer, module or a packaged component, combined with hardware for the contact-based or contactless interface (e.g. inlays).

595 **Life cycle phase C "Composite Product Integration and Initialization"**

Step 5: The composite product manufacturer

- (optional) produces modules, or packaged components, combined with hardware for the contact-based or contactless interfaces (e.g. inlays)
- equips the card's chip with pre-personalization data, and
- 600 creates the application(s).

The creation of the application(s) is conducted by the *Initialization* of the card using secured load scripts to create the object system(s) for the certified ePass application.

Observe that additional eID applications can be loaded in this step as well.

The *Initialization* can also be organizationally and or physically separated from the other card manufacturing steps.

After the *Initialization* the card is ready for import of user data (Personalization).

The pre-personalized TOE together with the IC identifier is securely delivered from the card manufacturer to the *Personalization*. The composite product manufacturer also provides the relevant parts of the guidance documentation. The Administrator Personalization Key is also delivered securely to the *Personalization*.

Life cycle phase D "Personalization"

Step 6: The *Personalization* of the card includes for the ePass application:

1) the survey of the card holder's biographical data,
2) the enrollment of the card holder's biometric reference data, such as a digitized portrait or other biometric reference data,
3) printing the visual readable data onto the physical part of the card, and
4) configuration of the TSF, if necessary.

Parts of the configuration of the TSF is performed during *Personalization* and includes, but is not limited to, the creation of the digitized version of the textual, printed data, the digitized version of e.g. a portrait, or a cryptographic signature of a cryptographic hash of the data that are stored on the chip. The personalized electronic document, if required together with appropriate guidance for TOE use, is handed over to the card holder for operational use.

The signing of the Document security object by the Document Signer [ICAO-9303-2015] 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.

From a hardware point of view, this cycle phase is already an operational use of the composite product and not a personalization of the hardware. The hardware's "Personalization" (cf. [Infineon-ST-SLC52-H13]) ends with the *Installation* of the TOE (installation of the object system).

Life cycle phase E "Operational Use"

Step 7: The chip of the TOE is used by the card and terminals that verify the chip's data during the phase operational use. The user data can be read and modified according to the security policy of the issuer.

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.

Correspondence to the Life-Cycle Description in the Security IC Protection Profile

Following the [BSI-CC-PP-0084-2014] Protection Profile, section 1.2.3 the life cycle phases of a smart card can be divided into the following seven phases:

Phase 1: IC Embedded Software Development

Phase 2: IC Development

Phase 3: IC Manufacturing

Phase 4: IC Packaging

Phase 5: Composite Product Integration

Phase 6: Personalization

Phase 7: Operational Use

Phase A "Development", step 1 and step 2 cover exactly phase 1 and phase 2 of [BSI-CC-PP-0084-2014].

Phase B "IC Manufacturing" covers phase 3 of [BSI-CC-PP-0084-2014] completely and is conducted based on the certified production procedures of the IC.

The TOE can be delivered in various form factors. Thus, IC packaging i.e. phase 4 of [BSI-CC-PP-0084-2014] conducted either in the IC Manufacturing already (phase B) or at a later stage during the composite product integration (phase C). In any case, the TOE is delivered in a state where it is ready for initialization. Phase C also covers phase 5 of [BSI-CC-PP-0084-2014] completely.

Phase D "Personalization" directly corresponds to phase 6 of [BSI-CC-PP-0084-2014].

Observe, that the TOE has reached its secure state already at the delivery point which is between phase B to phase C. Up to this point, the secure handling is controlled by the guidelines and security mechanisms provided by the IC manufacturer. After this point, the secure handling during *Initialization* and *Personalization* is controlled by the guidelines and security mechanisms provided by the TOE developer.

The security environment for the TOE and the ST of the underlying platform match, the IC life cycle phases up to 6 are covered by a controlled environment as required in [Infineon-ST-SLC52-H13], section 7.3.1.2. In IC life cycle phase 7 no restrictions apply.

The last life cycle phase E corresponds to the first step of Phase 7 of [BSI-CC-PP-0084-2014].

Specific Life-Cycle Aspects from the BAC Protection Profile

Several application notes in the BAC Protection Profile [BSI-CC-PP-0055-110] clarify life-cycle aspects which are specific for the BAC use in Machine Readable Travel Documents. The following explanations address these from the perspective of concrete implementation of the TOE:

Application note 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Basic Authentication Control Key.

The handling of TSF data is part of Life-Cycle Phase D "Personalisation" step 6.

Application note 3: This protection profile 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. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

This ST also considers the Personalization Agent and the Document Signer being two different roles defined by the ownership of the corrsponding key material which may or may not be separated. As far as the personalization key distribution is concerned the TOE uses symmetric keys for efficiency purposes.

Application note 4: The authorized Personalization Agents might be allowed to add (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". This will imply an update of the Document Security Object including the re-signing by the Document Signer.

This application note of the PP just clarifies organizational implications of the fact that the TOE internally stores a signature of the Document Signer over the Document Security Object.

Application note 5: The intention of the PP is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase 2 or later. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these

700 are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps. Note, that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, 705 generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

The description of the TOE life-cycle in this section clearly defines the TOE delivery point 710 and the distribution of the various production steps and the question if they are included in the evaluation scope or not.

2.4.2 TOE Boundaries

2.4.2.1 TOE Physical Boundaries

Smart card as used in this ST means an integrated circuit containing a microprocessor, 715 (CPU), a coprocessor for special (cryptographic) operations, a random number generator, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier. The integrated circuit is a single chip incorporating CPU and memory, which include RAM, ROM, and non-volatile memory.

The chip is embedded in a module, which provides the capability for standardized connec- 720 tion to systems separate from the chip through TOE's interfaces in accordance with ISO standards.

The physical constituent of the TOE is IC with the operating system loaded using the certified loading processes of the IC manufacturer and a set of load scripts which allow for installing the object system in a dedicated configuration.

725 The IC can be physically delivered on wafers, or as modules, or inlays but the physical boundary of the TOE is the IC itself excluding the connection technology.

After the *Installation* of the object system, the TOE can be personalized for the end-usage phase for the document holder as a card.

2.4.2.2 TOE Logical Boundaries

730 All card accepting devices (Host Applications) will communicate through the I/O interface of the operating system by sending and receiving octet strings. The logical boundaries of the TOE are given by the complete set of commands of the CardOS operating system for access, reading, writing, updating or erasing data.

The input to the TOE is transmitted over the physical interface as an octet string that has 735 the structure of Command Application Protocol Data Unit (CAPDU). The output octet string from the TOE has the structure of a Response Application Protocol Data Unit (RAPDU).

The Application Protocol Data Units or CardOS commands that can be used in the operating systems are described in more detail in the guidance [Atos-V60-ADM], [Atos-V60-USR].

2.4.2.3 TOE Delivery Format

740 In summary the delivery of the TOE consists of:

- the integrated circuit (IC) with the operation system pre-loaded
- the administrator and user guidance documentation [Atos-V60-ADM], [Atos-V60-USR]
- personalization information package, required for the secure personalization of the TOE. Further details about the secure personalization are provided in the guidance
745 documentation.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

Part 1: Introduction and general model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, [CC-Part1-V3.1]

Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, [CC-Part2-V3.1]

Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, [CC-Part3-V3.1]

as follows:

Part 2 extended, Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [CEM-V3.1] has to be taken into account.

3.1.1 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-Part3-V3.1].

Note:

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

3.1.2 Conformance Rationale

- the TOE type is a contactless / contact-based smart card and this type is consistent with the TOE type of the claimed PPs
- the chapter *Security Problem Definition (ASE_SPD)* is taken over from the claimed PP without changes
- the chapter *Security Objectives (ASE_OBJ)* is taken over from the claimed PP without changes
- the chapter *Extended Component Definition (ASE_ECD)* is taken over from the claimed PP without changes
- the chapter *Security Requirements (ASE_REQ)* is taken over from the claimed PP without changes.

4 Security Problem Definition (ASE_SPD)

4.1 Introduction

Assets

785 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-9303-2015]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) 790 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-9303-2015] the TOE described 795 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,
800 • Active Authentication Public Key in EF.DG15,
- Document Security Object (SO_D) 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)[1].

805 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.

810 4.1.1 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 815 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 820 the MRTD for the holder by some or all of the following activities

(i) establishing the identity the holder for the biographic data in the MRTD,

[1] Cf. [CC-Part1-V3.1] for details how to access these User data under EAC protection.

(ii) 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)

(iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability,

(iv) writing the initial TSF data and (iv) signing the Document Security Object defined in [ICAO-9303-2015].

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

(i) examining an MRTD presented by the traveler and verifying its authenticity and

(ii) verifying the traveler as MRTD holder.

The Basic Inspection System (BIS)

(i) contains a terminal for the contactless communication with the MRTD's chip,

(ii) implements the terminals part of the Basic Access Control Mechanism and

(iii) 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

(i) implements the Terminal Authentication Protocol and

(ii) 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

(i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data),

(ii) to read or to manipulate the logical MRTD without authorization, or

(iii) 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]).

4.2 Assumptions

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

4.2.1 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).

Notes

The title of the assumption is taken over from the protection profile and refers to the life-cycle step numbers of the standard Smartcard life-cycle defined in PP0084 [BSI-CC-PP-0084-2014]. For details how the life-cycle of the TOE fits into this model refer to section *TOE life-cycle*.

4.2.2 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.

Notes

The title of the assumption is taken over from the protection profile and refers to the life-cycle step numbers of the standard Smartcard life-cycle defined in PP0084 [BSI-CC-PP-0084-2014]. For details how the life-cycle of the TOE fits into this model refer to section *Life Cycle Phases Mapping*.

4.2.3 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.

4.2.4 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-9303-2015].

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-9303-2015] 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]).

4.2.5 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-9303-2015], 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]).

4.3 Threats

This section describes the threats to be averted by the TOE independently or in collaboration
940 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.

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

4.3.1.1 T.Chip_ID Identification of MRTD's chip

945 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:

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

Asset:

Anonymity of user.

4.3.1.2 T.Skimming Skimming the logical MRTD

955 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

Threat agent:

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

Asset:

confidentiality of logical MRTD data.

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

965 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.

970 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.

4.3.1.4 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.

4.3.2 The TOE shall avert the threats as specified below

4.3.2.1 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

(i) to manipulate User Data,

(ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or

(iii) 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.

4.3.2.2 T.Information_Leakage Information Leakage from MRTD's chip

Adverse action:

1015 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. 1020 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 1025 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 pT.Phys-Tamper Physical Tampering

1030 Asset:

confidentiality of logical MRTD and TSF data.

4.3.2.3 T.Phys-Tamper Physical Tampering

Adverse action:

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

1035 (i) to disclose TSF Data or

(ii) to disclose/reconstruct the MRTD's chip Embedded Software.

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

(i) modify security features or functions of the MRTD's chip,

(ii) modify security functions of the MRTD's chip Embedded Software,

1040 (iii) modify User Data or

(iv) 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 1045 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 1050 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:

1055 confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

4.3.2.4 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

(i) deactivate or modify security features or functions of the TOE or

(ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

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.

4.4 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-Part1-V3.1], sec. 3.2).

4.4.1 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.

4.4.2 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 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.

4.4.3 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)[2] 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

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

data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO-9303-2015].

1095 Note:

1. The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO-9303-2015]. 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]).

5 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.

5.1 Security Objectives for the TOE

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

5.1.1 OT.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-9303-2015] 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

5.1.2 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.

5.1.3 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-9303-2015] 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 protection profile. Thus the read access must be prevented even in case of a successful BAC Authentication.

5.1.4 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.

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

5.1.5 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 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.

5.1.6 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.

5.1.7 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.

5.1.8 OT.Prot_Malfunction Protection against Malfunctions

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation 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.

5.2 Security Objectives for the Operational Environment

5.2.1 Issuing State or Organization

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

5.2.1.1 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.

5.2.1.2 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.

5.2.1.3 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 togOE.Pass_Auth_Sign Authentication of logical MRTD by Signature protect the confidentiality and integrity of these data.

5.2.1.4 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 on the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO-9303-2015]

(iii) distribute the Certificate of the Document Signer Public Key to receiving StatOE.BAC-Keys Cryptographic quality of Basic Access Control Keys.

5.2.1.5 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-9303-2015] 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.

5.2.2 Receiving State or Organization

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

5.2.2.1 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-9303-2015].

5.2.2.2 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.

5.2.2.3 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)

5.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

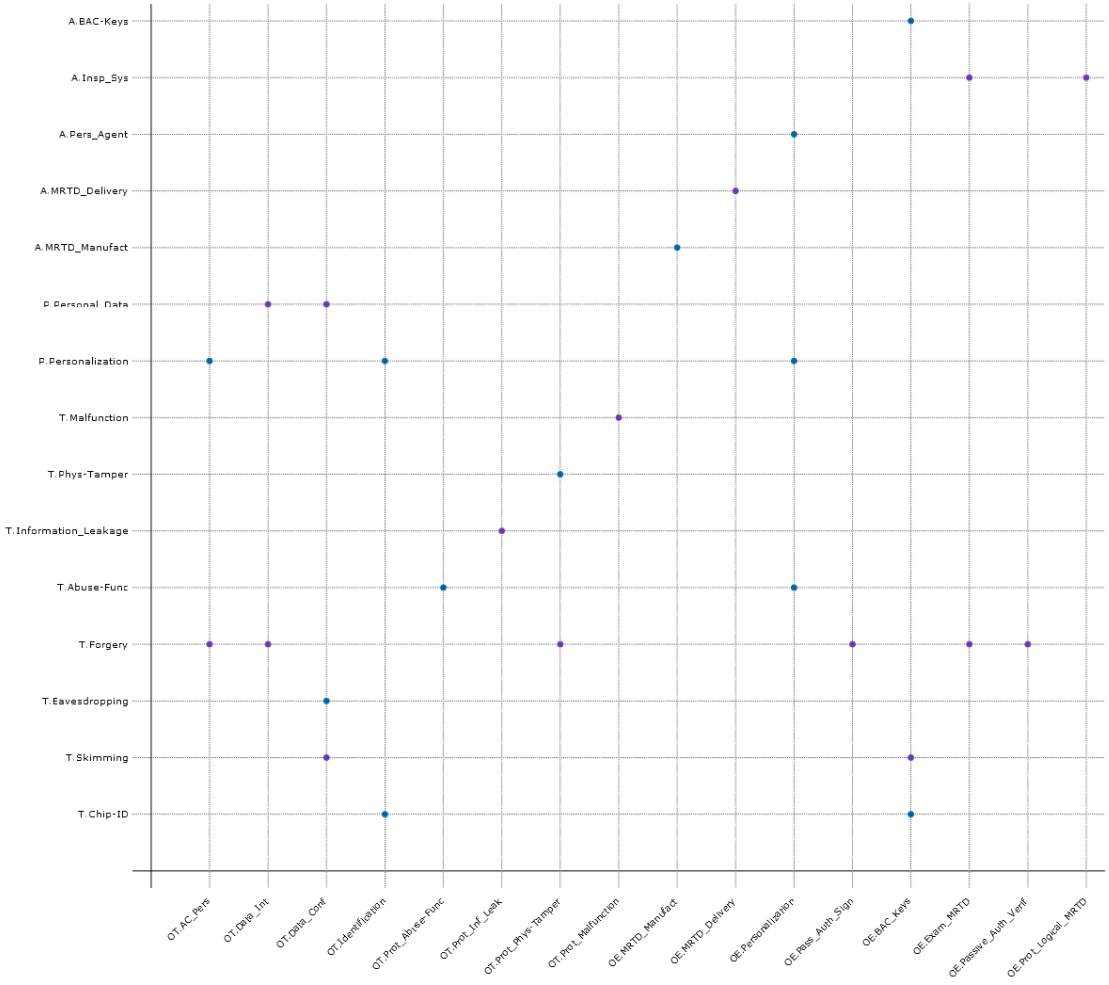

Fig. 5.1: Security Objective Rationale

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

1365 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-**
1370 **Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high[1] 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_**
1375 **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.

1380 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
1385 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
1390 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
1395 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

[1] "high" should be read "moderate".

6 Extended Component Definition (ASE_ECD)

This ST uses components defined as extensions to CC part 2 in Chapter 5 of [BSI-CR-CC-PP-0055-110].

In addition this ST uses the extended component FCS_RNG.1 defined in Chapter 5 of [BSI-CC-PP-0084-2014] as a replacement of the extended component FCS_RND.1 because it allows for a more accurate definition of the random number properties as required by the current random number generator evaluation methodology.

No other extended components are used.

7 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-Part1-V3.1] 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 *Introduction*. Note, that all these subjects are acting for homonymous external entities. All used objects are defined in section *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-Part2-V3.1].

Definition of security attributes:

Table 7.1: 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.

7.1 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.

7.1.1 Class FAU Security Audit

7.1.1.1 FAU_SAS.1 Audit storage

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

FAU_SAS.1.1

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

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)

7.1.2 Class FCS Cryptographic support

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

7.1.2.1 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-9303-2015], section 4.3.

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-9303-2015], section 4.3, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO-9303-2015], section 9.7.4. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RNG.1

2. The static Document Basic Access keys are generated and downloaded by the Personalization Agent and used for [ICAO-9303-2015], section 4.3.1 steps 3 a), b), f) and g).

   The TOE generates the Triple-DES and Retail-MAC session keys used for trusted channel secure messaging as specified by [ICAO-9303-2015], section 4.3.1 step 5) using FCS_COP.1/SHA.

7.1.2.2 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**[1] that meets the following: **none**[2].

Note:

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

7.1.2.3 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**[3] and cryptographic key sizes none that meet the following: **FIPS 180-4**[4].

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-9303-2015]
2. This TOE uses the SHA library [Infineon-Chip-HCL52] of the underlying chip SLC52GDA448*.

[1] [assignment: cryptographic key destruction method]
[2] [assignment: list of standards]
[3] [selection: SHA-1 or other approved algorithms]
[4] [selection: FIPS 180-2 or other approved standards]

7.1.2.4 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: [NIST-FIPS-46-3-1999] and [ICAO-9303-2015] section 4.3 and chapter 9.8.

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 SLC52GDA448*.
3. For the "secure messaging - encryption and decryption" using TDES see [Infineon-ST-SLC52-H13], 7.1.4.2 Triple-DES Operation.

7.1.2.5 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 CMAC mode**[5] and cryptographic key sizes **192**[6] bits that meet the following: [NIST-FIPS-197] **and** [ISO-IEC-9797-1-2011][7].

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 SLC52GDA448*.
3. For the "Advanced Encryption Standard (AES)" see [Infineon-ST-SLC52-H13], 7.1.4.3 AES Operation.

[5] [selection: AES]
[6] [selection: 192]
[7] [selection: FIPS 46-3 [9], FIPS 197 [12]]

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.

7.1.2.6 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 SLC52GDA448*.
3. For the "Triple-DES encrypting and decrypting" see [Infineon-ST-SLC52-H13], 7.1.4.2 Triple-DES Operation.

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

7.1.2.7 FCS_RNG.1 (Random number generation)

Hierarchical to No other components.

Dependencies No dependencies.

FCS_RNG.1.1 The TSF shall provide a **hybrid deterministic**[8] random number generator that implements:

(DRG.4.1) The internal state of the RNG shall use PTRNG of class PTG.2 as random source.

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy for every call.

(DRG.4.5) The internal state of the RNG is seeded by a PTRNG of class PTG.2 according to [BSI-AIS31-V3].[9]

[8] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]
[9] [assignment: list of security capabilities]

FCS_RNG.1.2 The TSF shall provide **random numbers** that meet:

(DRG.4.6) The RNG generates output for which 2^{12} strings of bit length 128 are mutually different with probability $1-2^{-105}$ (acc. to [NIST-SP800-90A] **C.3).**

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A as defined in [BSI-AIS2031-RNG-CLASSES-V2].[10]

Notes

1. This SFR has been adapted from [BSI-CC-PP-0084-2014] (FCS_RNG.1) to meet [BSI-AIS2031-RNG-CLASSES-V2]. It correlates with the SFR 'FCS_RNG.1' from [BSI-CC-PP-0055-110].
2. For the "random numbers generation Class PTG.2 according to [BSI-AIS31-V3]" see [Infineon-ST-SLC52-H13] "7.1.1.1.1 True Random Number Generation".
3. Entropy source uses PTG.2 of the hardware as noise source and Block_Cipher_df as specified in [NIST-SP800-90A] using the AES block cipher as a conditioning component to implement CTR_DRBG as specified in [NIST-SP800-90A].
4. This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

7.1.3 Class FIA Identification and Authentication

The following provides an overview on the authentication mechanisms used.

Table 7.2: Overview on authentication SFR

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO-9303-2015], and [BSI-TR-03110-1-V220]
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 192 bit keys (cf. FCS_COP.1/AUTH)

7.1.3.1 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"

[10] [assignment: a defined quality metric]

4. **to run self tests according to** FPT_TST.1[11].

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.

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

7.1.3.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1

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[12].

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

[11] REFINEMENT
[12] REFINEMENT

7.1.3.3 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**[13]

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-9303-2015]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to 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.

7.1.3.4 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**[14]

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**[15]
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-CC-PP-0056-V2-2012-MA-02] should also be fulfilled the Personalization Agent should not be authenticated by using

[13] [selection: Triple-DES, AES or other approved algorithms]
[14] [selection: Triple-DES, AES]
[15] [selection: the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]]

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-CC-PP-0056-V2-2012-MA-02] 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.

7.1.3.5 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-9303-2015] 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 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-CC-PP-0056-V2-2012-MA-02] 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.

7.1.3.6 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when **2**[16] **consecutive**[17] unsuccessful authentication attempt occurs related to **authentication attempts using BAC**[18].

FIA_AFL.1.2

[16] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

[17] REFINEMENT

[18] [assignment: list of actions]

When the defined number of unsuccessful authentication attempts has been **met**[19], the TSF shall **delay the next authentication attempt at least 6 seconds**.[20]

Note:

1. The delay applies also when a new session is restarted and requires a successful authentication attempt to be turned off.

   Resistance against a Brute Force attack depends on the entropy of the MRZ-derived access keys (see [ICAO-9303-2015], Annex A to Part 11).

7.1.4 Class FDP User Data Protection

7.1.4.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

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.

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

Hierarchical to: No other components.

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**[21].

FDP_ACF.1.2

[19] [assignment: met or surpassed]
[20] [assignment: list of actions]
[21] REFINEMENT authentication status of terminals

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-CC-PP-0056-V2-2012-MA-02] for details).

7.1.4.3 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]
- [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.

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.

7.1.4.4 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]
- [FDP_ACC.1 Subset access control, or
- FDP_IFC.1 Subset information flow control]

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.

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.

7.1.5 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.

7.1.5.1 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.

1855 #### 7.1.5.2 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

1860 1. Manufacturer,
2. Personalization Agent,
3. Basic Inspection System.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

1865 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.

7.1.5.3 FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

1870 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:

1875 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
1880 enable other attacks.

7.1.5.4 FMT_LIM.2 Limited availability

Hierarchical to: No other components

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1

1885 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,
1890 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.

7.1.5.5 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

7.1.5.6 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.

7.1.5.7 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.

7.1.5.8 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.

7.1.6 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.

7.1.6.1 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[22]

in excess of **unintelligible limits**[23] enabling access to

1. Personalization Agent Key(s)
2. **Document Basic Access Keys**[24]
3. **Secure Messaging Keys**[25].

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) **Document Basic Access Keys**[26] and **Secure Messaging Keys**[27].

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.

7.1.6.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

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

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

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

7.1.6.3 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1

The TSF shall run a suite of self tests **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_RNG.1[28]

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.

7.1.6.4 FPT_PHP.3 Resistance to physical attack

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

FPT_PHP.3.1

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

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 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.

[28] [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]]

2. The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [CC-Part2-V3.1]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

7.2 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.

7.3 Security Requirements Rationale

7.3.1 Security Functional Requirements Rationale

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

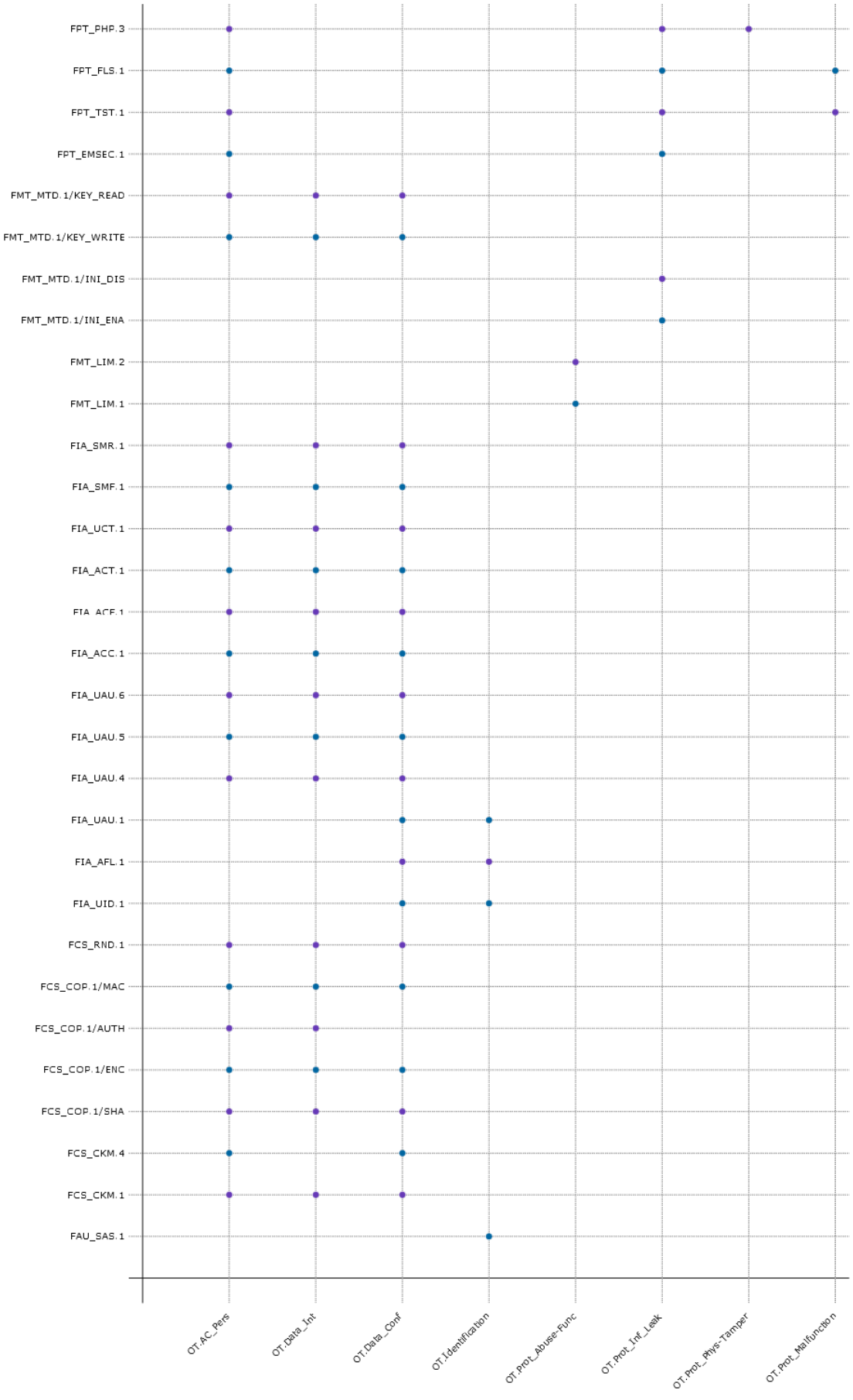

Fig. 7.1: Functional Requirement to TOE security objective mapping

7.3.1.1 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
2060 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_RNG.1 (for key
2065 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-CC-PP-0056-V2-2012-MA-02] 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 se-
2070 cure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RNG.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
2075 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.

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

2080 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
2085 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.

2090 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_RNG.1 (for
2095 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.

7.3.1.3 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_RNG.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.

7.3.1.4 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.

7.3.1.5 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.

7.3.1.6 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.

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

is covered by the SFR FPT_PHP.3.

7.3.1.8 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.

7.3.2 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 following table shows the dependencies between the SFR of the TOE.

Table 7.3: SFR Dependencies

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 FCS_COP.1/MAC
	FCS_COP.1 Cryptographic operation],	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled FCS_CKM.4

continues on next page

Table 7.3 – continued from previous page

SFR	Dependencies	Support of the Dependencies
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 attributes, or	
	FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_RNG.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1

continues on next page

Table 7.3 – continued from previous page

SFR	Dependencies	Support of the Dependencies
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
	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
2175 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.

7.3.3 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.

7.3.4 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 *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 *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.

8 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 *Security Functional Requirements for the TOE*.

8.1 TOE Security Services

8.1.1 User Identification and Authentication (BAC)

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 B "Manufacturing",
  2. to read the random identifier in Phase D "Personalization (of the MRTD)",
  3. to read the random identifier in Phase E "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 B "Manufacturing",
  2. to read the random identifier in Phase D "Personalization (of the MRTD)",
  3. to read the random identifier in Phase E "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 [Atos-V60-CardOS-Users-Manual].
2. For further explanations of the life-cycle phases refer to section *Life Cycle Phases Mapping*

8.1.1.1 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.

8.1.1.2 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 *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 *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])

8.1.1.3 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 *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.

8.1.2 Protocols

The TOE support the following protocols.

8.1.2.1 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 *Secure messaging*.

If the terminal (or the Personalization Agent see *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 upon closure of the secure messaging.

With FIA_UAU.5 (1) the TOE provides the means to authenticat the terminal during the BAC authentication.

8.1.3 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 *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 *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,

8.1.4 Secure messaging

With FCS_CKM.1 (cf. [ICAO-9303-2015], section 4.3) and FCS_COP.1/SHA and FCS_RNG.1 (cf. [ICAO-9303-2015], section 4.3) 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-9303-2015], section 9.8).

The secure messaging keys are also protected agains side-channel attacks as mandated by

- FPT_EMSEC.1

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.

8.1.5 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.

8.1.6 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 SLC52GDA448* 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-16bit-V01], 6.2.4 Power-up and references to *High-security boot-up software (BOS)*.
- After erasure of RAM the state of the User EEPROM is tested and, if not yet initialized, this will be done.
- The User EEPROM heap is checked for consistency. If it is not valid, the TOE will preserve a secure state (life cycle DEATH).
- The backup buffer is checked and its data is restored to User EEPROM, if they were saved because of a command interruption.
- The integrity of stored TSF executable code is verified. If this check fails, the TOE will preserve a secure state (life cycle DEATH).
- The integrity of stored data (objects and files) is verified before their use.
- The hardware sensors, the symmetric coprocessor and the random number generator are tested. If one of the tests fails, the chip platform will perform a security reset.

The TOE will furthermore run tests during

1. start-up
2. Reading Initialization and Pre-personalization Data according to "FMT_MTD.1/INI_DIS"
3. Reading data of LDS groups and EF.SOD
4. Reading Basic Access Keys
5. Generating random numbers according to "FCS_RNG.1"

according to FPT_TST.1.

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
- Memory failures during TOE execution
- Out of range failures of temperature, clock and voltage sensors
- Failures during random number generation

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)
- 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. *User Identification and Authentication (BAC)* for a certain action.

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

- Basci Access Keys

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 Compatibility between the Composite ST and the Platform-ST

IP_SFR Irrelevant Platform SFR

RP_SFR-SERV Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.

RP_SFR-MECH Relevant Platform SFRs being used by the Composite-ST because of its security properties providing protection against attack to the TOE as a whole

IrOE Objectives for the environment not being relevant for the Composite-ST

CfPOE Objectives for the environment being fulfilled by the Composite-ST automatically, i.e. they can be assigned to TOE security objectives.

SgOE Remaining security objectives for the environment of the Platform-ST not belonging to the group IrOE nor CfPOE and thus need to be addressed in the Composite-ST

The sections

- *Assurance requirements of the composite evaluation*
- *Security objectives for the environment of the platform*
- *Usage of platform TSF by TOE TSF*

show the compatibility of this Composite ST and the Platform-ST as required by [BSI-AIS36-V5].

The Platform-ST is the security target of all controllers SLC52GDA448* used by this TOE as platform.

9.1 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-Part1-V3.1], [CC-Part2-V3.1], and [CC-Part3-V3.1] and
- EAL4 augmented with ALC_DVS.2.

Therefore the Composite-SAR is a subset of the Platform-SAR.

9.2 Security objectives for the environment of the platform

The Platform-ST defined the following objectives for the environment:

- OE.Process-Sec-IC is directly supported by the P.Manufact and the implementing objective OT.Identification which provides means to identify the TOE. Thus, the objective falls in both classes CfPOE and SgOE because it is partially fulfilled by the TOE but also remains partially significant of the composite ST objectives for the environment.

- OE.Lim_Block_Loader, OE.TOE_Auth, and OE.Loader_Usage are not relevant because they are concerned with the authentication of the TOE and the usage of the flash loader in early production phases at the IC manufacturer. Therefore, they are irrelevant objectives fir the environment (IrOE)
- OE.Resp-Appl concerns the treatment of the user data by the Composite-TOE and is enforced intrinsically by the security architecture of the Composite-TOE. Thus, this objective belongs to the automatically fulfilled objectives (CfPOE).

Overall, the objectives for the environment of the platform are fully captured by the Composite-ST.

Thus, the objectives of the Platform-TOE and the Composite-TOE are not contradictory.

9.3 Usage of platform TSF by TOE TSF

The relevant SFRs (*RP_SFR-SERV*, *RP_SFR-MECH*) of the platform being used by the Composite ST are listed in the following table.

Table 9.1: Relevant Platform SFRs used as services or *mechanisms*

RP_SFR-SERV ***RP_SFR-MECH***	**Meaning**	**Used by TOE SFR**
FRU_FLT.2	Limited Fault Tolerance	FPT_TST.1
FPT_FLS.1	Failure with Preservation of Secure State	FPT_FLS.1
FPT_PHP.3	Resistance to Physical Attack	FPT_PHP.3
FDP_ITT.1	Basic Internal Transfer Protection	FPT_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/TRNG	Quality Metric for Random Numbers	FCS_RNG.1
FPT_TST.2	Subset TOE Security Testing	FPT_TST.1, FPT_PHP.3 (active shield and sensors)
FCS_COP.1/TDES-SCL-1 FCS_CKM.4/DES-SCL-1	Cryptographic Support (3DES)	FCS_COP.1/ENC (TDES), FCS_COP.1/MAC (TDES)
FCS_COP.1/CMAC-SCL-1 FCS_CKM.4/CMAC-SCL-1	Cryptographic Support (AES)	FCS_COP.1/AUTH
FCS_COP.1/AES		FCS_RNG.1
(FCS_COP.1/HCL)	The SHA implementation is functionally dependent on the underlying crypto library but addressed in the scope of this evaluation as reflected by the addition of FCS_COP.1/SHA in this ST	FCS_COP.1/SHA

continues on next page

Table 9.1 – continued from previous page

RP_SFR-SERV *RP_SFR-MECH*	Meaning	Used by TOE SFR
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	used as supporting mechanism
FDP_ACF.1	Security Attribute Based Access Control	used as supporting mechanism
FDP_SDC.1	Stored date confidentiality	used as supporting mechanism
FDP_SDI.2	Stored data integrity monitoring and action	used as supporting mechanism
FDP_UCT.1	Basic data exchange confidentiality	used as supporting mechanism
FDP_UIT.1	Data exchange integrity	used as supporting mechanism
FDP_LIM.1/Loader	Limited Capabilities Loader	used as supporting mechanism
FDP_LIM.2/Loader	Limited Availability Loader	used as supporting mechanism

Any platform SFR not listed in Table 9.1 is not being used by the Composite ST and thus an
2495 irrelevant SFRs (*IP_SFR*).

9.4 Conclusion

Overall there is **no conflict** between **security requirements** of this Composite-ST and the Platform-ST.

A Overview of Cryptographic Algorithms

2500 This TOE is a composite product and uses for cryptographic mechanism listed only mechanism provided by the underlying chip SLC52GDA448*.

The "Standard of Implementation" is a citation of the ST of the underlying chip SLC52GDA448* only, cf. [Infineon-ST-SLC52-H13].

Table A.1: Cryptographic mechanisms used

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
1	Authentication	BAC, Symmetric Authentication, *TDES* (CBC, Retail MAC)	[NIST-SP800-67] (*TDES*), [NIST-800-38A-2001] (CBC), [ISO-IEC-9797-1-2011] algorithm 3 and padding method 2 (Retail MAC), [BSI-TR-03110-1-V220], [ICAO-9303-2015]	112 (CBC), 112 (Retail MAC), 64 (nonce)	[BSI-TR-03110-1-V220], [ICAO-9303-2015]	*Document Basic Access Key*
2	Authentication	Symmetric Authentication, AES in CMAC mode	[NIST-FIPS-197] (AES), [ISO-IEC-9797-1-2011] algorithm 5 and padding method 2 (CMAC), [BSI-TR-03110-1-V220]	192	[BSI-TR-03110-1-V220]	Personalization-key, FCS_COP.1/AUTH

continues on next page

Table A.1 – continued from previous page

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
3	Key Agreement	BAC Key Derivation Algorithm	[ICAO-9303-2015], Section 4.3	112	[BSI-TR-03110-1-V220]	FCS_CKM.1, FCS_COP.1/SHA, (see note 1)
4	Confidentiality	Secure Messaging, *TDES* in CBC mode	[NIST-SP800-67] (*TDES*) [NIST-800-38A-2001] (CBC)	112	[BSI-TR-03110-1-V220] [ICAO-9303-2015] Section 4.3	FCS_COP.1/ENC (see note 4)
5	Integrity	Secure Messaging, *TDES* in Retail MAC Mode	NIST Special Publication 800-67 V1.1 (*TDES*) [ISO-IEC-9797-1-2011] algorithm 3 and padding method 2 (Retail MAC)	112	[ICAO-9303-2015] chapter 9, [BSI-TR-03110-1-V220]	FCS_COP.1/MAC (see note 4)
6	Trusted Channel	ICAO BAC Secure Messaging established during BAC	[ICAO-9303-2015] section 4.3	112	[ICAO-9303-2015] section 4.3, [BSI-TR-03110-1-V220]	FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC

continues on next page

Table A.1 – continued from previous page

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
7	Cryptographic Primitive	DRG.4 random number generator	[NIST-SP800-90A] CTR_DRBG, using AES as block cipher, random source of class PTG.2 according to [BSI-AIS31-V3]	./.	N/A	FCS_RNG.1 (see note 3)
8	Cryptographic primitive	SHA-1	[NIST-FIPS-180-4]	-	[BSI-TR-03110-3-V221]	key derivation (see note 2)

Notes:

2505 1. This TOE computes session keys according to [ICAO-9303-2015], section 4.3 and chapter 9.

2. This TOE uses the Infineon libraries RSA, ECC and Toolbox (ACL52 v2.08.007), SHA (HCL52 v1.12.001) and Symmetric Crypto Library (SCL52 v2.04.002) of the underlying chip SLC52GDA448*. For the standard of implementation of hash algorithms SHA-1
2510 see [Infineon-Chip-HCL52].

3. This TOE uses the random numbers generation provided by the underlying chip SLC52GDA448* as random source for the hybrid deterministic random number generator. For the standard of implementation of "random numbers generation Class DRG.4 according to [BSI-AIS2031-RNG-CLASSES-V2]" see [Infineon-ST-SLC52-H13].

2515 4. This TOE uses *TDES* provided by the underlying chip SLC52GDA448*. For *TDES* operation see [Infineon-ST-SLC52-H13], "7.1.4.3 Cryptography by the Symmetric Cryptographic Library SCL".

Bibliography

[CC-Part1-V3.1] CCMB-2017-04-001, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC-Part2-V3.1] CCMB-2017-04-002, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC-Part3-V3.1] CCMB-2017-04-003, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CEM-V3.1] CCMB-2017-04-004, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, 2017-04.

[CC-CompositeEval-Smart-Cards] Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1, CCDB-2007-09-001.

[BSI-AIS2031-RNG-CLASSES-V2] AIS 20 / AIS 31, A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, 2011-09-18.

[BSI-AIS36-V5] AIS 36, Anwendungshinweise und Interpretationen zum Schema, AIS36: Kompositionsevaluierung, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 5, 2017-03-15.

[BSI-AIS31-V3] AIS 31, Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3, 2013-05-15.

[BSI-CC-PP-0055-110] Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application" Basic Access Control, BSI-CC-PP-0055 Version 1.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-03-25.

[BSI-CR-CC-PP-0055-110] Certification Report for BSI-CC-PP-0055-2009 Machine Readable Travel Document with "ICAO Application" Basic Access Control, Bundesamt für Sicherheit in der Informationstechnik (BSI),2009-05-07.

[BSI-CC-PP-0059-2009-MA-02] Protection profiles for Secure signature creation device - Part 2: Device with key generation, Information Society Standardization System CEN/ISSS, EN 419211-2:2013, 2013-07-17.

[BSI-CC-PP-0071-2012-MA-01] Protection profiles for Secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application, Information Society Standardization System CEN/ISSS, EN 419211-4:2013, 2013-11-27

[BSI-CC-PP-0072-2012-MA-01] Protection profiles for Secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN 419211-5:2013, 2013-12-04.

[BSI-CC-PP-0056-V2-2012-MA-02] 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, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-12-05.

[BSI-CC-PP-0068-V2-2011-MA-01] Machine Readable Travel Document using Standard Inspection Procedure with PACE(PACE PP), BSI-CC-PP-0068-V2-2011-MA-01,

Version 1.0.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-07-22.

[BSI-CC-PP-0084-2014] Security IC Platform Protection Profile with Augmentation Packages, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.0, 2014-01-13.

[BSI-CC-PP-0086-2015] Common Criteria Protection Profile / Electronic document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP], Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.01, 2015-05-20.

[BSI-TR-03110-1-V220] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.20, 2015-02-26.

[BSI-TR-03110-2-V221] Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token ü Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.21, 2016-12-21.

[BSI-TR-03110-3-V221] BSI, Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.21, 2016-12-21.

[BSI-TR-03110-4-V221] BSI, Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 4: Applications and Document Profiles, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.21, 21. December 2016

[BSI-TR-03111-V210-ECC] TR-03111, Technical Guideline TR-03111: Elliptic Curve Cryptography, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.10, 2018-06-01.

[BSI-TR-03116-2] TR-03116-2, Technische Richtlinie BSI TR-03116 - Kryptographische Verfahren für Projekte der Bundesregierung - Teil 2: Hoheitliche Dokumente, Bundesamt für Sicherheit in der Informationstechnik (BSI), Stand 2021, 2021-02-23.

[EU-Reg-910-2014] eIDAS Regulation (Regulation (EU) No 910/2014), REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Communities, L257:73 - 114, 2014-08-28.

[DIR-1999-93-EC] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities, L13:12 - 20, 2000-01-19.

[ICAO-9303-2015] ICAO Doc 9303, Machine Readable Travel Documents - Machine Readable Passports, (this includes the latest supplemental for ICAO Doc 9303 which also should be considered), International Civil Aviation Organization (ICAO), Seventh Edition, 2015.

[ICAO-TR-110] ICAO SAC v1.1, Machine Readable Travel Documents, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, International Civil Aviation Organization (ICAO), Version 1.1, 2014-04-15.

[NIST-FIPS-180-4] FIPS PUB 180-4, Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology (NIST), August 2015.

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

[NIST-FIPS-197] FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), Information Technology Laboratory, National Institute of Standards and Technology (NIST), 2001-11-26

[NIST-FIPS-46-3-1999] FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), U.S. DEPARTMENT OF COMMERCE, National Institute of Standards and Technology (NIST), 1999-10-25.

[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, ISO/IEC, 2008.

[ISO-IEC-7816-part-4] ISO/IEC 7816-4:2013, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, ISO/IEC, 2013-04.

[ISO-IEC-14443-2018] ISO/IEC 14443 Identification cards – Contactless integrated circuit cards - Contactless proximity objects, ISO/IEC, 2018.

[ISO-IEC-9797-1-2011] ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO/IEC, 2011-03.

[ISO-IEC-14888-3] ISO/IEC 14888_3:2006 - Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms, ISO/IEC, 2006-11.

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

[RFC-5639-2010-03] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010-03.

[NIST-800-38A-2001] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology (NIST), 2001 Edition, 2001-12.

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

[NIST-SP800-67] NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, National Institute of Standards and Technology (NIST), Revision 2, 2012-01.

[NIST-SP800-90A] NIST Special Publication 800-90A, Recommendation Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology (NIST), Revision 1, 2015-06.

[RSA-PKCS1-v2.2] PKCS #1 v2.2: RSA Cryptography Standard, Version 2.2, 2012-10-27.

[RSA-PKCS-3-V1.4] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, 1993-11-01.

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

[ANSI-X9.63] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, ANSI, 2001-11-20.

[Infineon-ST-SLC52-H13] Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h with Options, Common Criteria EAL6 augmented / EAL6+, Infineon, Version 1.9, 2021-05-18.

[Infineon-Chip-HW-Ref-16bit-V01] 16-bit Security Controller Family - V01, Hardware Reference Manual (HRM), Revision 7.0, 2019-06-11

[Infineon-Chip-HCL52] HCL52-CPU-C65 Hash Crypto Library for CPU SHA, 16-bit Security Controller, User interface manual, v1.12.001, 2020-01-14.

[IEEE-1363] IEEE 1363A-2004, IEEE Standard Specifications for Public-Key Cryptography, IEEE Standards Board, 2004-07-22.

[SOG-IS-Crypto-Catalog-V1.2] SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms, Version 1.2, 2020-01.

[Atos-V60-CardOS-Users-Manual] CardOS V6.0 User's Manual, Atos Information Technology GmbH

[Atos-V60-ADM] Administrator Guidance 'CardOS V6.0 ID R1.0' and 'CardOS V6.0 ID R1.0 (BAC)', Atos Information Technology GmbH

[Atos-V60-USR] User Guidance 'CardOS V6.0 ID R1.0' and 'CardOS V6.0 ID R1.0 (BAC)', Atos Information Technology GmbH

Index

R

S

T

U

V