T · · Systems

Specification of the Security Target TCOS Passport Version 2.0 Release 1.1/P5CD080V0B

Extended Access Control

Version: 2.0.1.1

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	TCOS Passport Version 2.0 Release 1.1_EAC P5CD080V0B.doc
Stand:	18.03.2008
Version:	2.0.1.1
Autor:	Ernst-G. Giessmann
Geltungsbereich:	TeleSec Entwicklungsgruppe
Vertraulichkeitsstufe:	**Öffentlich**

History

Version	Date	Remark
2.0.1	2007-10-15	Final Version 2.0 Release 1
2.0.1.1	2008-03-18	Final Version 2.0 Release 1.1 for re-certification

Contents

Abbreviations

ATS	Answer To Select
BIS	Basic Inspection System
CC	Common Criteria
CVCA	Contry Verifying Certification Authority
DV	Document Verifier
EIS	Extended Inspection System
IS	Inspection System
MRTD	Machine readable travel document
n.a.	not applicable
OSP	Organizational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
SOF	Strength of function
SOM	Strength of mechanism
TOE	Target of evaluation
TSF	TOE security functions

The Terminology follows the Protection Profile [EACPP].

1 ST Introduction

1.1 ST Identification

ST Identification: Security Target refers to the Product “TCOS Passport Version 2.0 Release 1.1” (TOE) of T-Systems for CC evaluation.

Whereas the TCOS Passport Version 1 series refers to contactless integrated circuit chip of machine readable travel documents implementing the ICAO application “Basic Access Control” the Version 2 series chips provide additionally the Extended Access Control according to ICAO document [ICAOPKI].

Title: Specification of the Security Target TCOS Passport Version 2.0 Release 1.1

Date: 18.03.2008

Author: T-Systems TeleSec, Ernst-G. Giessmann

Certification ID: BSI-DSZ-CC-00518

TOE: TCOS Passport Version 2.0 Release 1.1

1.2 ST Overview

The security target is the description of a TOE as a contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) [ICAOLDS] and providing the Basic Access Control and the Extended Access Control according to ICAO document [ICAOPKI] and an authentication mechanism according to the technical report [BSI]. The hardware bases on a NXP chip P5CD080V0B with the TCOS operating system. The TOE is supplied with a file system, which contains all the data that is used in the context of the ICAO application as described in [EACPP].

The hardware base may be in some context relevant. In this case the TOE will referenced in more detail as "TCOS Passport Version 2.0 Release1.1/P5CD080V0B", otherwise the notion "TCOS Passport Version 2.0 Release1.1" applies to any realization regardless which hardware base is used.

The TOE follows the composite evaluation aspects (see also [AIS36]).

1.3 CC Conformance

The ST claims the conformance of the TOE to Common Criteria for IT Security Evaluation Version 2.3, August 2005

- Part 1,
- Part 2 (extended) and
- Part 3 (conformant).

The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations.

This ST claims conformance to the Protection Profile for Machine Readable Travel Document with ICAO Application “Extended Access Control” [EACPP].

The evaluation assurance level of the TOE is EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 as stated in [EACPP].

The minimum strength for the TSF is “high”.

The evaluation of the TOE uses the results of the CC evaluation of the hardware [CR].

2 TOE Description

2.1 TOE Definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [ICAOLDS], providing the Basic Access Control and the Extended Access Control according to the Technical Report [BSI], including the Chip Authentication mechanism, which replaces the Active Authentication [ICAOPKI] .

The TOE comprises of

- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- the IC Embedded Software (operating system)
- the MRTD application and
- the associated guidance documentation.

The TOE is a Smart Device with an operating system (TCOS) and a dedicated file system, that contains all data relevant for the ICAO applications.

The physical MRTD is the 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.

The logical MRTD consists of the MRTD holder's data stored according to the Logical Data Structure [ICAOLDS] 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 biometric reference data of finger(s) (EF.DG3) and/or iris image(s) (EF.DG4),

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

(5) the Document Security Object.

The components of the TOE are therefore the hardware (IC), the operating system TCOS (OS) and the dedicated file for the ICAO application in a file system. A detailed description of the parts of TOE will be given in other documents.

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) and organizational security measures (e.g. control of materials, personalization procedures). These security measures include the binding of the MRTD's chip the passport book. This document adresses the protection of the logical MRTD in integrity and in confidentiality by the Basic Access Control Mechanism and the Extended Access Control Mechanism.

The TOE implements the Basic Access Control as follows. The inspection system

(i) reads optically the MRTD (i.a. the printed data in the MRZ),

(ii) authenticates themselves as inspection system by means of Document Basic Access Keys derived from MRZ data.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAOPKI] and [ICAOLDS].

The TOE implements the Extended Access Control defined in the Technical Report [BSI] consisting of

(i) a Terminal Authentication Protocol to authenticate the inspection system as entity authorized by the Issuing State or Organization through the receiving State, and

(ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.

The Extended Access Control requires the Chip Authentication of the MRTD's chip to the inspection system first and uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive

biometric reference data during their transmission from the TOE to the inspection system.

The Chip Authentication is provided by the following steps:

(i) the inspection system communicates by means of secure messaging established by Basic Access Control,

(ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object,

(iii) the inspection system generates a ephemeral key pair,

(iv) the TOE and the inspection system agree on two session keys for secure messaging in MAC_ENC mode according to the Diffie-Hellman Primitive and

(v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. it could apply the Chip Authentication Private Key corresponding to the Chip Authentication Public Key for derivation of the session keys).

Note that the Chip Authentication defined in [BSI], as well as the optional Active Authentication described in [ICAOPKI] provide evidence of the MRTD's chip authenticity. The Chip Authentication prevents a chip tracing described in [ICAOPKI], Annex G, section G.3.3, but certainly not the traveller tracing.

The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers which create Inspection System Certificates.

The TOE implements the Chip Authentication Protocol defined in [BSI] instead of the optional Active Authentication described in [ICAOPKI].

(i) The inspection system communicates by means of secure messaging established by Basic Access Control.

(ii) The inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object.

(iii) The inspection system generates a ephemeral key pair,

(iv) The TOE and the inspection system agree on two session keys for secure messaging in MAC_ENC mode according to the Diffie-Hellmann Primitive.

(v) The inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly.

Following the protection profile PP0002 [PP0002, Fig. 15 p. 84] the life cycle phases of a TCOS Passport device can be divided into the following seven phases:

- Phase 1: Development of operating system software by the operating system manufacturer
- Phase 2: Development of the smart card controller by the semiconductor manufacturer
- Phase 3: Fabrication of the smart card controller (integrated circuit) by the semiconductor manufacturer
- Phase 4: Installation of the chip in an inlay with an antenna
- Phase 5: Completion of the smart card operating system
- Phase 6: Initialization and personalization of the MRTD
- Phase 7: Operational phase of the MRTD

According to the PP [EACPP] the TOE life cycle is described in terms of the four life cycle phases.

Life cycle phase 1 “Development”

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

The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

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

This life cycle phase 1 covers Phase 1 and Phase 2 of [PP0002].

Life cycle phase 2 "Manufacturing"

In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile memories (ROM and EEPROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer (note that both of these roles may be assigned to different entities).

The MRTD manufacturer

(i) add the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary,

(ii) creates the MRTD application, and

(iii) equips MRTD's chip with Pre-personalization Data and

(iv) packs the IC with hardware for the contactless interface in the passport book.

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

This life cycle phase 2 corresponds to Phase 3 and Phase 4 of [PP0002] and may include for flexibility reasons Phase 5 and some production processes from Phase 6 as well. Depending on the requirements of the following Personalization life cycle phase 3 some restrictions for the file system may also be fixed already in this phase. Despite of that they all could be made also during Personalization, i.e. they are not changing the TOE itself, such an approach of delivering the TOE with different configurations is useful for issuing states or organizations. The mentioned restrictions never change the structure of the file system, but affect only the pre-allocation of maximal available memory and the a priori appearance of elementary files (EFs) for data groups to be allocated and filled up during Personalization. Note that any other file parameter can not be changed. If an issuing state or organization will use biometric data of fixed size for one of the data groups DG3 or DG4 and optional the other, it may be appropriate to use a pre-configured TOE with already allocated memory for the first data group and a not initialized yet EF for the other one. For this version of the TOE two pre-configurations of the file systems apply, with pre-initialized EF.DG3 and another one, where EF.DG3 can be initialized during Personalization. EF.DG2 is already initialized and visible in both configurations but have different sizes of pre-allocated memory.

A detailed description of the sub-phases and the file system pre-configuration can be found in the Administrator Guidance [TCOSADM].

Life cycle phase 3 "Personalization of the MRTD"

The personalization of the MRTD includes

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

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

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

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

(v) the writing the TSF Data into the logical MRTD and configuration of the TSF if necessary.

The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of

(i) the digital MRZ data (EF.DG1),

(ii) the digitized portrait (EF.DG2), and

(iii) the Document Security Object.

The Document Security Object is signed by the Document signer [ICAOPKI], which is not necessarily the same role as Personalization Agent. Nevertheless the Personalization Agent must check the correctness of the Document Security Object before the personalization of the genuine MRTD for the MRTD holder is finalized.

The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

This life cycle phase corresponds to the remaining initialization and personalization processes not covered yet from Phase 6 of the [PP0002].

Life cycle phase 4 "Operational Use"

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

This life cycle phase corresponds to the Phase 7 of the [PP0002].

The product is finished after initialization, after testing the OS and creation of the dedicated file system with security attributes and ready made for the import of LDS. This corresponds to the end of life cycle phase 2 of the Protection Profile [EACPP]. In

this version the TOE may also be pre-configured during manufacturing which leads to different configurations for delivering. A more detailed description of the production processes in Phases 5 and 6 of PP0002 [PP0002] is given in the Administrator Guidance document [TCOSADM].

2.2 TOE Boundaries

2.2.1 TOE Physical Boundaries

Smart card as used in this ST means an integrated circuit containing a microprocessor, (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 EEPROM.

The chip is embedded in a module which provides the capability for standardized connection to systems separate from the chip through contactless interface in accordance with ISO standards.

The physical constituents of the TOE are the operating system, the data in elementary files of the dedicated file of the ICAO application (EEPROM), and temporary data used during execution of procedures associated to that dedicated file.

2.2.2 TOE Logical Boundaries

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 TCOS 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 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 TCOS commands that can be used in the operating systems are described in more detail in an other document.

3 TOE Security Environment

3.1 Introduction

3.1.1 Assets

Assets are the elements of the TOE to be protected. Assets have to be protected in terms of confidentiality and/or integrity.

Logical MRTD Data

The logical MRTD data consists of the elementary files EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [ICAOLDS]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG14) 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.

User Data	TSF Data
Personal Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 – EF.DG13, EF.DG15, EF.DG16	Personalization Agent Reference Authentication Data
Sensitive biometric reference data (EF.DG3, EF.DG4)	Basic Access Control (BAC) Key
Chip Authentication Public Key in EF.DG14	Public Key CVCA
Document Security Object (SOD) in EF.SOD	CVCA Certificate
Common data in EF.COM	Current date
	Chip Authentication Private Key

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's holder is used by the traveller to prove his possession of a genuine MRTD.

3.1.2 Subjects

The Protection Profile [EACPP] considers the following subjects:

Manufacturer

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

Personalization Agent

The agent is acting on the behalf of the issuing State or Organization to personalize 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,

(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 and

(iv) signing the Document Security Object defined in [ICAOLDS].

Whether or not the Personalization Agent is the same role as the Document Signer is not relevant for the TOE. For simplicity reasons we will assume as in [EACPP] that these two role coincide.

Country Verifying Certification Authority

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

Document Verifier

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

Terminal

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

Inspection System

An Inspection System is a technical system used by the border control officer of the receiving State for

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

(ii) verifying the traveller 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 additional the Chip Authentication Mechanism.

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

(i) implements 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 by the Inspection System Certificates. Whereas the support of Basic Acess Control is optional according to [ICAOPKI], it can not be disabled in the TOE by the Personalization Agent.

MRTD Holder

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

Traveller

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 the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD),
(ii) to read or to manipulate the logical MRTD without authorization, or
(iii) to forge a genuine MRTD.

3.2 Assumptions

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

A.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 Info (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 ensures the correctness of the signature over the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

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 traveller and verifying its authenticity and
(ii) verifying the traveller as MRTD holder.

The Basic Inspection System for global interoperability

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

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

The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the au-

thenticity of the MRTD's chip during inspection and establishes secure messaging with keys agreed by the Chip Authentication Mechanism.

The Extended Inspection System in addition to the General Inspection System

(i) supports 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.

A.Signature_PKI PKI for Passive Authentication

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which

(i) securely generates, stores and uses the Country Signing CA Key pair, and

(ii) manages the MRTD's Chip Authentication Key Pairs.

The CA keeps the Country Signing CA Private Key secret and distributes the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity.

The Document Signer

(i) generates the Document Signer Key Pair,

(ii) hands over the Document Signer Public Key to the CA for certification,

(iii) keeps the Document Signer Private Key secret and

(iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs.

For simplicity reasons we follow the description in [EACPP]. In fact from the point of view of the TOE it must not be assumed that the Document Signer has generated the Document Signer Key by its own.

The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and organizations.

A.Auth_PKI PKI for Inspection Systems

The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the extended access control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the

receiving States or Organizations. The issuing States or Organizations distributes the public key of their Country Verifying Certification Authority to their MRTD's chip.

3.3 Threats

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

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

T.Chip_ID **Identification of MRTD's chip**

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker can not read optically and does not know in advance data from the physical MRTD.

T.Skimming **Skimming the logical MRTD**

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker cannot read and does not know in advance data from the physical MRTD.

T.Read_Sensitive_Data **Read the sensitive biometric reference data**

An attacker with high attack potential knowing the Document Basic Access Keys is trying to gain the sensitive biometric reference data through the communication interface of the MRTD's chip.

The attack T.Read_Sensitive_Data is similar to the threat T.Skimming in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from this in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visual readable on the physical MRTD as well.

T.Forgery Forgery of data on MRTD's chip

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose 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 an other identity of the traveller. 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 MRTD's to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveller into an other 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 in an other contactless chip.

T.Counterfeit MRTD's chip

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

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

The TOE shall avert the threat as specified below.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in TOE operational phase 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.

T.Information_Leakage Information Leakage from MRTD's chip

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

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

T.Phys-Tamper Physical Tampering

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

(i) to disclose TSF Data
(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,
(iii) to modify User Data or
(iv) to modify TSF data.

The physical tampering may be focused directly on the discloser or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

T.Malfunction Malfunction due to Environmental Stress

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 or 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.

3.4 Organizational Security Policies

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

P.Manufact **Manufacturing of the MRTD's chip**

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing. 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.

P.Personalization **Personalization of the MRTD by issuing State or Organization only**

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

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) 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 i.e. if the MRTD is presented to an inspection system. Additional to the Basic Access Control Authentication defined by ICAO in [ICAOPKI] the MRTD's chip shall shall protect the confidentiality and integrity of the personal data during transmission to the General Inspection System after Chip authentication.

P.Sensitive_Data **Privacy of sensitive biometric reference data**

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

4 Security Objectives for the TOE

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

OT.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 [ICAOLDS] 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 personalization and cannot be changed after finishing it. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

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 the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

OT.Data_Conf Confidentiality of personal data

The TOE must ensure the confidentiality of the data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 and the Document Security Object of the logical MRTD by granting read access to terminals successfully authenticated by as

(i) Personalization Agent, or

(ii) Basic Inspection System or

(iii) Extended Inspection System.

The TOE implements the Basic Access Control as defined by ICAO [ICAOPKI] and enforce Basic Inspection System to 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 General Inspection System after Chip Authentication.

Application Note: This objective concerns the confidentiality of the access to personal data based on knowledge of the Document Basic Access Keys and is not releated to the question how these keys are generated, stored or distributed (cf. A.Pers_Agent). Any attack based on decision of the ICAO Technical Report [ICAOPKI] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective. The TOE provides ahead the Chip Authenti-

cation Protocol that ensures the confidentiality of the transmission by a higher entropy of the generated session keys.

OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

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

OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. In Phase 4 “Operational Use” the TOE shall identify itself only to a successful authenticated Basic Inspection System or a Personalization Agent.

Application Note: In Phase 4 “Operational Use” the TOE may be certainly identified by the unique Document number as part of the printed and digital MRZ, but there will be no identification data transmitted over the contactless interface.

OT.Chip_Auth_Proof Proof of MRTD'S chip authenticity

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MTRD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [BSI]. The authenticity proof provided by MRTD'S chip shall be protected against attacks with high attack potential.

Application note: The OT.Chip_Auth_Proof implies the MRTD's chip to have

(i) an unique identity as given by the MRTD's Document number,

(ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data.

The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD's chip i.e. a certificate for the Chip Authentication Public Key that fits to the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by

(i) the Chip Authentication Public Key (EF.DG14) in the LDS [ICAOLDS] and

(ii) the unambigously defined Key Identifier (e.g. a hash value) of the Authentication Public Key in the Document Security Object signed by the Document Signer.

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

OT.Prot_Abuse-Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order

(i) to disclose critical User Data,

(ii) to manipulate critical User Data of the Smartcard Embedded Software,

(iii) to manipulate soft-coded Smart Card Embedded Software or

(iv) bypass, deactivate, change or explore security features or functions of the TOE.

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

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

(i) 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

(ii) by forcing a malfunction of the TOE and/or

(iii) by a physical manipulation of the TOE.

OT.Prot_Phys-Tamper Protection against Physical Tampering

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

(i) 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

(ii) 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)

(iii) manipulation of the hardware and its security features, as well as

(iv) controlled manipulation of memory contents (User Data, TSF Data)

with a prior reverse-engineering to understand the design and its properties and functions.

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.

4.1 Security Objectives for the Development and Manufacturing Environment

Security Objectives are separated for the Development and Manufacturing Environment and the Operational Environment (see next section)

OD.Assurance Assurance Security Measures in Development and Manufacturing Environment

The developer and manufacturer ensure that the TOE is designed and fabricated so that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. This includes the use of the Initialization Data for unique identification of the TOE and the pre-personalization of the TOE including the writing of the Personalization Agent Authentication key(s). The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against obvious penetration attacks with high attack potential.

OD.Material Control over MRTD Material

The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, to initialize, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.

4.2 Security Objectives for the Operational Environment

4.2.1 Issuing State or Organization

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

OE.Personalization Personalization of logical MRTD

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

(i) establish the correct identity of the holder and create biographic data for the MRTD,

(ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and

(iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

The Issuing State or Organization must

(i) generate a cryptographic secure Country Signing Key Pair,

(ii) ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment, and

(iii) distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity.

The Issuing State or organization must

(i) generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys,

(ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and

(iii) distribute the Certificate of the Document Signing Public Key to receiving States and organizations.

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

OE.Auth_Key_MRTD MRTD Authentication Key

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

(i) generate the MRTD's Chip Authentication Key Pair,

(ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key in DG14 and

(iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

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

4.2.2 Receiving State or Organization

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

OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the Receiving State must examine the MRTD presented by the traveller 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 [ICAOPKI].

Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the Receiving State or Organization uses the inspection system to verify the traveller as the 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 organi-

zations must manage the Country Signing Public Key and the Document Signing Public Key maintaining their authenticity and availability in all inspection systems.

OE.Prot_Logical_MRTD Protection of data of 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 inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

Application note: The figure 2.1 in [BSI] supposes that the GIS and the EIS after running the Basic Access Control Protocol read only those parts of the logical MRTD after which are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key) and start afterwards the Chip Authentication protocol. The supposed sequence has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. Nevertheless reading less-sensitive data directly after Basic Access Control Mechanism is allowed and can not be prevented. Therefore it is not assumed as a threat. The TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

OE.Ext_Insp_Systems Authorization of Extended Inspection Systems

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

5 IT Security Requirements

In the following all assignments and selections are marked straight underlined if they are already made in the PP [EACPP]. All other assignments in the present ST are *slanted and underlined.* Refinements are printed in **bold**.

5.1 Security Functional Requirements for the TOE

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

5.1.1 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below For the extended components definition refer to [EACPP] chapter 4.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1	The TSF shall provide the Manufacturer[1] with the capability to store the IC Identification Data[2] in the audit records.

Dependencies: No dependencies.

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). The security measures in the manufacturing environment assessed under ADO_IGS and ADO_GEL ensure that the audit records will be used to fulfill the security objective OD.Assurance.

[1] [assignment: *authorized users*]

[2] [assignment: *list of audit information*]

5.1.2 Class Cryptographic Support (FCS)

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

FCS_CKM.1/KDF_MRTD Cryptographic key generation – Key Derivation Function by the MRTD

Hierarchical to: No other components.

FCS_CKM.1.1/ KDF_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Control Key Derivation Algorithm[3] and specified cryptographic key sizes 112 bit[4] that meet the following: [ICAOPKI], Annex E[5].

Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

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 [ICAOPKI], Annex E.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC BAC session keys for secure messaging by the algorithm in [ICAOPKI], Annex E.1. The TOE uses this key derivation function as well to derive other session keys from shared secrets established by the Chip Authentication Protocol for the secure messaging required by FCS_COP.1/TDES_MRTD and FCS_COP.1/ MAC_MRTD. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1/MRTD.

FCS_CKM.1/DH_MRTD Cryptographic key generation – Diffie-Hellman Keys by the TOE

Hierarchical to: No other components.

FCS_CKM.1.1/	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH Session*

[3] [*assignment: cryptographic key generation algorithm*]

[4] [*assignment: cryptographic key sizes*]

[5] [*assignment*: *list of standards*]

DH_MRTD	*Key Derivation Algorithm*[6] and specified cryptographic key sizes *112 bit*[7] that meet the following: [BSI], Annex A.1[8].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

The TOE generates a shared with the terminal secret value during the Chip Authentication Protocol (see [BSI] sec. 3.1 and Annex A.1, [ECCTR]) based on the ECDH protocol compliant to [BSI], Annex A.1. The shared secret value is used to derive the 112 bit Triple-DES key for encryption and the 112 bit Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [ICAOPKI], annex E.1, for the TSF as required by FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD.

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (Common Criteria Part 2).

FCS_CKM.4 Cryptographic key destruction - MRTD

Hierarchical to: No other components.

FCS_CKM.4.1/ MRTD	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with zeros or the new key*[9] that meets the following: *none*[10].

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]
FMT_MSA.2 Secure security attributes

The TOE destroys the BAC Session Keys

(i) after detection of an error in a received command by verification of the MAC and

(ii) after successful run of the Chip Authentication Protocol.

---

[6] [*assignment: cryptographic key generation algorithm*]

[7] [*assignment: cryptographic key sizes*]

[8] [*assignment*: *list of standards*]

[9] [*assignment: cryptographic key destruction method*]

[10] [*assignment: list of standards*].

The TOE destroys the Chip Authentication Session Keys after detection of an error in a received command by verification of the MAC.

The TOE clears the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

5.1.2.1 Cryptographic operation (FCS_COP.1)

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

FCS_COP.1/SHA_MRTD Cryptographic operation – Hash for Key Derivation by MRTD

Hierarchical to: No other components.

FCS_COP.1.1/ SHA_MRTD	The TSF shall perform hashing[11] in accordance with a specified cryptographic algorithm *SHA-1*[12] and cryptographic key sizes none[13] that meet the following: FIPS 180-2[14].

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
FMT_MSA.2 Secure security attributes

The TOE does not use other hash functions for key derivation.

FCS_COP.1/TDES_MRTD Cryptographic operation – Encryption / Decryption Triple DES

Hierarchical to: No other components.

FCS_COP.1.1/ TDES_MRTD	The TSF shall perform secure messaging – encryption and decryption[15] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[16] and cryptographic key sizes 112 bit[17] that meet the following: FIPS 46-3 [FIPS46] and [ICAOPKI]; Annex E[18].

[11] [*assignment: list of cryptographic operations*]

[12] [assignment: *cryptographic algorithm*]

[13] [assignment*: cryptographic key sizes*]

[14] [assignment: *list of standards*]

[15] [assignment: *list of cryptographic operations*]

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
FMT_MSA.2 Secure security attributes

The session keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/KDF_MRTD and FIA_UAU.4/BAC_BT or the Chip Authentication Protocol according to the requirement FCS_CKM.1/DH_MRTD.

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_MRTD: The TSF shall perform secure messaging – message authentication code[19] in accordance with a specified cryptographic algorithm Retail MAC[20] and cryptographic key sizes 112 bit[21] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[22].

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
FMT_MSA.2 Secure security attributes

The MAC keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/KDF_MRTD and FIA_UAU.4/BAC_BT or the Chip Authentication Protocol according to the requirement FCS_CKM.1/DH_MRTD.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD

Hierarchical to: No other components.

[16] [assignment: *cryptographic algorithm*]

[17] [assignment: *cryptographic key sizes*]

[18] [assignment: *list of standards*]

[19] [assignment: *list of cryptographic operations*]

[20] [assignment: *cryptographic algorithm*]

[21] [assignment: *cryptographic key sizes*]

[22] [assignment: *list of standards*]

FCS_COP.1.1/ SIG_VER	The TSF shall perform digital signature verification[23] in accordance with a specified cryptographic algorithm *ECDSA*[24] and cryptographic key sizes *192, 224, 256, 288 and 320 bit*[25] that meet the following: *ISO 15946* [ISO15946][26].

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
FMT_MSA.2 Secure security attributes

The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge. The key sizes are selected according to the SFR for the environment.

5.1.2.2 Random Number Generation (FCS_RND.1)

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

FCS_RND.1/MRTD Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1/ MRTD	The TSF shall provide a mechanism to generate random numbers that meet *the requirements for SOF-high according to [AIS31]*[27].

Dependencies: No dependencies.

5.1.3 Class FIA Identification and Authentication

The following table provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [ICAOPKI], Annex E, and [BSI]

[23] [assignment: *list of cryptographic operations*]

[24] [assignment: *cryptographic algorithm*]

[25] [assignment: *cryptographic key sizes*]

[26] [assignment: *list of standards*]

[27] [assignment: *a defined quality metric*]

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [ICAOPKI], Annex E, and [BSI]
Symmetric Authentication Mechanism for Personaliza-tion Agents	FIA_UAU.4/MRTD	FIA_API.1/SYM_PT	Triple-DES with 112 bit keys
Basic Access Control Authentication Mechanism	FIA_AFL.1, FIA_UAU.4/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/BT FIA_UAU.6/BT	Triple-DES, 112 bit keys Retail-MAC, 112 bit keys
Chip Authentication Protocol	FIA_API.1/MRTD, FIA_UAU.5/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/GIS FIA_UAU.5/GIS FIA_UAU.6/GIS	ECDH, Retail-MAC, 112 bit keys
Terminal Authentication Protocol	FIA_UAU.5/MRTD	FIA_API.1/EIS	ECDSA with SHA-1

Table 5.1.3.T1: Overview on authentication SFR

5.1.3.1 Timing of identification (FIA_UID.1)

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

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow
(1) to establish the communication channel,
(2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[28]
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.

Dependencies: No dependencies.

[28] [assignment: *list of TSF-mediated actions*]

The MRTD's chip and the terminal establish the communication channel through the contactless interface. The Protocol Type A defines an "Answer to Select" (ATS) and the protocol Type B is managed through the commands "Answer to Request" and "Answer to Attrib". The terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal for communication with more than one RFID. The so called historical bytes do not contain country/issuer specific information of the manufacturer or the issuer nor any other pre-issuing data (i.e. the tags '1Y', '2Y', '5Y' and '6Y' defined for these purposes in Section 8 of ISO 7816-4 are not used). Therefore it will not lead to vulnerability by the means of identifying the chip. In the operational phase the MRTD chip uses a randomly selected identifier for the communication channel with any Inspection System. The identifier consists of 4 Byte, where the first is always fixed (0x08) and the other three are randomly selected, therefore OT.Identification is not violated here.

In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer creates 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 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. After successful authentication as Basic Inspection System the terminal may identify themselves as Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or as Personalization Agent by selection of the Personalization Agent Authentication Key.

5.1.3.2 Timing of authentication (FIA_UAU.1)

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1	The TSF shall allow (1) to establish the communication channel, (2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS (3) to identify themselves by selection of the authentication key[29] 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.

Dependencies: FIA_UID.1 Timing of identification.

5.1.3.3 Single-use authentication mechanisms (FIA_UAU.4)

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

FIA_UAU.4/MRTD Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components.

FIA_UAU.4.1/MRTD	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism, 2. Terminal Authentication Protocol, 3. Authentication Mechanism based on Triple-DES[30].

Dependencies: No dependencies.

All listed authentication mechanisms use a challenge of 8 Bytes freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt: the Basic Access Control Authentication Mechanism uses RND.ICC [ICAOPKI], and the Authentication Mechanism based on Triple-DES may use a Challenge as well.

The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAOPKI]. 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 the first

[29] [assignment: *list of TSF-mediated actions*]

[30] [assignment: *identified authentication mechanism(*s)]

step the TOE sends a randomly chosen challenge which shall contain sufficient entropy to prevent T.Chip_ID. In the second step the MRTD's chip provides a challenge-response-pair which allows the terminal a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. The TOE does not continue the protocol execution with a terminal not successfully authenticated in the first step to fulfil the security objective OT.Identification and to prevent T.Chip_ID.

5.1.3.4 Multiple authentication mechanisms (FIA_UAU.5)

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

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism,
2. Terminal Authentication Protocol,
3. Secure Messaging in MAC_ENC-mode,
4. Symmetric Authentication Mechanism based on Triple-DES[31]

to support user authentication.

[31] [assignment: *list of multiple authentication mechanisms*]

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 mechanisms
   (a) The Basic Access Control Authentication Mechanism with the Personalization Agent Keys,
   (b) The Symmetric Authentication Mechanism with the Personalization Agent Key,
   (c) The Terminal Authentication Protocol with Personalization Agent Keys
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.
3. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging with key agreed with the authenticated terminal by means of the Basic Access Control Authentication Mechanism.
4. After run of the Chip Authentication Mechanism the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism[32].

Dependencies: No dependencies.

Depending on the authentication methods used the Personalization Agent holds

(i) a pair of a Triple-DES encryption key and a retail-MAC key for the Basic Access Control Mechanism specified in [ICAOPKI], or

(ii) a Triple-DES key for the Symmetric Authentication Mechanism or

(iii) an asymmetric key pair for the Terminal Authentication Protocol (e.g. provided in a valid in the PKI for Inspection System's Authentication card verifiable certificate with appropriate encoded access rights).

The Personalization Agent may use the Symmetric Authentication Mechanism without secure messaging mechanism if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal, otherwise secure messaging must be used.

[32] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

5.1.3.5 Re-authenticating (FIA_UAU.6)

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

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

Hierarchical to: No other components.

FIA_UAU.6.1/MRTD The TSF shall re-authenticate the user under the conditions

1. Each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS.
2. Each command sent to TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS[33].

Dependencies: No dependencies.

The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [BSI] include the secure messaging for all commands of theses protocols 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_MRTD for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticate the user for each received command and accept only those commands received from the initially authenticated user. This requirement is applicable to all commands associated with the Access Control SFP to the Logical MRTD data (FDP_ACF.1). A command outside the scope of MRTD application may not fulfill this requirement.

5.1.3.6 Authentication Failure Handling (FIA_AFL.1)

The TOE shall meet the requirement “Authentication Failure Handling (FIA_AFL.1)” as specified below.

FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components.

[33] [assignment: *list of conditions under which re-authentication is required*]

FIA_AFL.1.1	The TSF shall detect when *1*[34] unsuccessful authentication attempts occur related to *BAC authentication protocol within a single power-on-session*[35].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *wait before accepting any other command at least the time which is necessary for re-initialization after power-off*[36].

Dependencies: No dependencies.

These assignments ensure the high strength of authentication function as terminal part of the Basic Access Control Authentication Protocol and the Extended Access Control Authentication Protocol.

5.1.3.7 Authentication Proof of Identity (FIA_API.1)

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

FIA_API.1/CAP Authentication Proof of Identity - MRTD

Hierarchical to: No other components.

FIA_API/CAP	The TSF shall provide an Chip Authentication Protocol according to [BSI][37] to prove the identity of the TOE[38].

Dependencies: No dependencies.

The TOE and the terminal generate a shared secret using the Diffie-Hellmann Protocol (ECDH) and two session keys for secure messaging in MAC_ENC mode according to [ICAOPKI, Annex E.1]. The terminal verifies by means of secure messaging whether the MRTD’s chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

---

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

[35] [assignment: *list of authentication events*]

[36] [assignment: *list of actions*]

[37] [assignment: *authentication mechanism*]

[38] [assignment: *authorized user or rule*]

5.1.4 Class FDP User Data Protection

5.1.4.1 Subset access control (FDP_ACC.1)

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

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1	The TSF shall enforce the Access Control SFP[39] on terminals gaining write, read and modification access to the data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD[40].

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.4.2 Security attribute based access control (FDP_ACF.1)

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

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the Access Control SFP[41] to objects based on the following:

1. Subjects:
   a. Personalization Agent
   b. Basic Inspection System
   c. Extended Inspection System
   d. 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. authentication status of terminals
   b. terminal authorization[42].

[39] [assignment: *access control SFP*]

[40] [assignment: *list of subjects*, *objects, and operations among subjects and objects covered by the SFP*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. the successfully authenticated Personalization Agent is allowed to write data and to read data of 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 data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
3. the successfully authenticated Extended Inspection System is allowed to read data in EF.COM, EF:SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
4. the successfully authenticated Extended Inspection System is allowed to read data in EF.DG3 according to the Terminal Authorization,
5. the successfully authenticated Extended Inspection System is allowed to read data in EF.DG4 according to the Terminal Authorization[43].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following sensitive rules: none[44].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rule:

1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,
5. the Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD[45].

[41] [assignment: *access control SFP*]

[42] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes*, *or named groups of SFP-relevant security attributes*]

[43] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[44] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

[45] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

Application Note: The identified in FMT_SMR.1 roles CVCA and CA are in fact different instantiations of a Terminal with different access rights. This allows to sum up them in one Subject in FDP_ACF.1.

The TOE verifies the certificate chain established by the Country Verifier Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifier Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

5.1.4.3 Inter-TSF-Transfer

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

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

FDP_UCT.1.1/MRTD The TSF shall enforce the Access Control SFP[46] to be able to transmit and receive[47] objects in a manner protected from unauthorized disclosure **after Chip Authentication**.

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]

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

FDP_UIT.1/MRTD Data exchange integrity - MRTD

Hierarchical to: No other components.

46 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

47 [selection*: transmit, receive*]

FDP_UIT.1.1/MRTD	The TSF shall enforce the Access Control SFP[48] to be able to transmit and receive[49] user data in a manner protected from modification, deletion, insertion and replay[50] errors **after Chip Authentication**.
FDP_UIT.1.2/MRTD	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[51] has occurred **after Chip Authentication**.

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

The authentication mechanism as part of Basic Access Control Mechanism and the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

5.1.5 Class FMT Security Management

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Personalization 3. Configuration[52].

[48] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[49] [selection*: transmit, receive*]

[50] [selection: *modification, deletion, insertion, replay*]

[51] [selection: *modification*, *deletion, insertion, replay*]

[52] [assignment: *list of security management functions to be provided by the TSF*]

Dependencies: No Dependencies

Application Note: Because the Initialization Data is written already before the TOE is ready made, we don't consider it in the following. Moreover as the TOE can not be configured for usage with Basic Inspection Systems only, a separate Configuration management is not necessary. Because it is implicitly included in the Personalization we consider it as one management function only.

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

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1	The TSF shall maintain the roles 1. Manufacturer, 2. Personalization Agent, 3. Country Verifier Certification Authority, 4. Document Verifier, 5. Basic Inspection System, 6. domestic Extended Inspection System 7. foreign Extended Inspection System[53].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Hierarchical to: FIA_UID.1 Timing of identification.

Application Note: The Manufacturer has no access rights after the completion of the TOE. Nevertheless it is included because the role of the Manufacturer is identified and maintained in the Life Cycle Phase 2.

Application Note: The TSF maintain in fact only one effective role for an Extended Inspection System (cf. [BSI, A.3.4.3]) and grant access to the TOE security data according to the corresponding rights given in the Certificate Holder Authorization in the certificate presented by an EIS (cf. FMT_MTD.3). For this reason in the following the identified in [EACPP] roles of domestic and foreign Extended Inspection System are considered as one role with different given access rights.

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

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below. For the extended components definition refer to [EACPP] chapter 4.

53 [assignment: *the authorised identified roles*]

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed and 4. substantial information about construction of TSF to be gathered which may enable other attacks[54].

Dependencies: FMT_LIM.2 Limited availability.

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below. For the extended components definition refer to [EACPP] chapter 4.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed and 4. substantial information about construction of TSF to be gathered which may enable other attacks[55].

Dependencies: FMT_LIM.1 Limited capabilities.

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

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

[54] [assignment: *Limited capability and availability policy*]

[55] [assignment: *Limited capability and availability policy*]

Hierarchical to: No other components.

FMT_MTD.1/INI_ENA	The TSF shall restrict the ability to write[56] the Initialization Data and Pre-personalization Data[57] to the Manufacturer[58].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

The Pre-personalization Data includes the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Authentication Key.

Application Note: This SFR is not applicable, because the Initialization and Pre-Personalization Data is written before the TOE is completed. Nevertheless the Manufacturer uses already the security mechanisms supplied by the TSF.

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.

FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to disable read access for users to[59] the Initialization Data[60] to the Personalization Agent[61].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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“. 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 shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

[56] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[57] [assignment: *list of TSF data*]

[58] [assignment: *the authorized identified roles*]

[59] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[60] [assignment: *list of TSF data*]

[61] [assignment: *the authorized identified roles*]

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

Hierarchical to: No other components.

FMT_MTD.1.1/ CVCA_INI	The TSF shall restrict the ability to write the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifier Certification Authority Certificate, 3. initial Current Date[62] to the Personalization Agent[63].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

The initial Country Verifying Certification Authority Public Key will be written by the Personalization Agent (cf. [BSI], sec. 2.2.4). The data of the initial Country Verifier Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

Application Note: Because the complete CVCA data initialization of the MRTD is performed by the Personalization Agent only, the data of the initial Country Verifier Certification Authority Certificate can also be written directly.

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

Hierarchical to: No other components.

FMT_MTD.1.1/ CVCA_UPD	The TSF shall restrict the ability to update the 1. Country Verifier Certification Authority Public Key, 2. Country Verifier Certification Authority Certificate[64] to Country Verifier Certification Authority[65].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

The Country Verifier Certification Authority updates its asymmetric key pair and distributes the public key by means of the Country Verifier CA Link-Certificates (cf. [BSI], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifier CA Link-

[62] [assignment: *list of TSF data*]

[63] [assignment: *the authorized identified roles*]

[64] [assignment: *list of TSF data*]

[65] [assignment: *the authorized identified roles*]

Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [BSI], sec. 2.2.3 and 2.2.4).

FMT_MTD.1/Date Management of TSF data – Current Date

Hierarchical to: No other components.

FMT_MTD.1.1/ Date	The TSF shall restrict the ability to modify the Current Date[66] to 1. Country Verifier Certification Authority, 2. Document Verifier 3. domestic Extended Inspection System[67].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application Note: The used here function does not change the Current Date partially (modification) but the complete data of the Current Date (overwriting).

FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write

Hierarchical to: No other components.

FMT_MTD.1.1/KEY_WRITE	The TSF shall restrict the ability to write[68] the Document Basic Access Keys[69] to the Personalization Agent[70].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

Hierarchical to: No other components.

FMT_MTD.1.1/CAPK	The TSF shall restrict the ability to *load*[71] the Chip Authentication Private Key[72] to *the Chip Manufacturer and the Personalization Agent*[73].

[66] [assignment: *list of TSF data*]

[67] [assignment: *the authorized identified roles*]

[68] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[69] [assignment: *list of TSF data*]

[70] [assignment: *the authorized identified roles*]

[71] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[72] [assignment: *list of TSF data*]

[73] [assignment: *the authorized identified roles*]

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

The Chip Authentication Private Key is loaded either by the Manufacturer or by the Personalization Agent.

Application Note: The verb "load" means that the Chip Authentication Private Key security parameters are generated securely outside the TOE and written into the TOE memory. This covers also a private key selection, which is in fact a selection of a random multiplier only, done by the MRTD's chip during the loading procedure.

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

Hierarchical to: No other components.

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[74] the

1. Document Basic Access Keys,
2. Chip Authentication Private Key,
3. Personalization Agent Keys[75]

to none[76].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data **of the Terminal Authentication Protocol and the Access Control**.

Refinement: The certificate chain is valid at the Current Date if and only if

(1) the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,

(2) the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

[74] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[75] [assignment: *list of TSF data*]

[76] [assignment: *the authorized identified roles*]

(3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

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

5.1.6 Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information flow for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to 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 SFR “Non-bypassability of the TSP (FPT_RVM.1)” and “TSF domain separation (FPT_SEP.1)” together with “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below. For the extended components definition refer to [EACPP] chapter 4.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit *power variations, timing variations during command execution*[77] in excess of *non-useful information*[78] enabling access to Personalization Agent Authentication Key and Chip Authentication Key [79] and *none*[80].

[77] [assignment*: types of emissions*]

[78] [assignment: *specified limits*]

FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users[81] are unable to use the following interface smart card circuit contacts[82] to gain access to Personalization Agent Authentication Key and Chip Authentication Key[83] and *none*[84].

Dependencies: No other components.

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

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: (1) exposure to operating conditions where therefore a malfunction could occur, (2) failure detected by TSF according to FPT_TST.1[85].

Dependencies: ADV_SPM.1 Informal TOE security policy model

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation*[86] to demonstrate the correct operation of the TSF.

[79] [assignment: *list of types of TSF data*]

[80] [assignment: *list of types of user data*]

[81] [assignment: *type of users*]

[82] [assignment: *type of connection*]

[83] [assignment: *list of types of TSF data*]

[84] [assignment: *list of types of user data*]

[85] [assignment: *list of types of failures in the TSF*]

[86] [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*]]

FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Dependencies: FPT_AMT.1 Abstract machine testing.

The MRTD's chip, the NXP chip P5CD080V0B will run self tests at the request of the authorized user and some self tests automatically. A self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 will be executed during initial start-up by the Manufacturer in the life cycle phase 2 „Manufacturing". Self tests will be also run automatically to detect memory failures and to preserve of secure state according to FPT_FLS.1 in the life cycle phase 4 „Operational Use".

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[87] to the TSF[88] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

The TOE will use counter measures implemented by IC manufacturer continuously to prevent physical manipulation and physical probing [CR].

The following security functional requirements protect the TSF against bypassing. and support the separation of TOE parts.

The TOE shall meet the requirement "Non-bypassability of the TSP (FPT_RVM.1)" as specified below (Common Criteria Part 2).

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

[87] [assignment: *physical tampering scenarios*]

[88] [assignment: *list of TSF devices/elements*]

FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

The TOE shall meet the requirement “TSF domain separation (FPT_SEP.1)” as specified below (Common Criteria Part 2).

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

The parts of the TOE which support the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” are protected from interference of the other security enforcing parts of the MRTD’s chip Embedded Software.

5.2 Security Assurance Requirements for the TOE

The for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the MRTD’s chip especially for the absence of unintended functionality.

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 selection of the component AVA_MSU.3 provides additional assurance that the analysis and testing for insecure states is validated and confirmed through testing by the evaluator.

The selection of the component AVA_VLA.4 provides the assurance that the TOE is shown to be highly resistant to penetration attacks to meet the security objectives OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.

The Assurance Requirements for the selected level EAL 4 augmented are described in the Common Criteria for IT Security Evaluation documents. They are not listed in detail here.

The minimum strength of function is SOF-high.

5.3 Security Requirements for the IT environment

This section describes the security functional requirements for the IT environment using the CC part 2 components.

Due to CCIMB Final Interpretation #58 these components are editorial changed to express the security requirements for the components in the IT environment where the original components are directed for TOE security functions. The editorial changes are indicated in **bold**.

5.3.1 Passive Authentication

The ICAO, the Issuing States or Organizations and the Receiving States or Organization run a public key infrastructure for the Passive Authentication. This public key infrastructure distributes and protects the Country Signing CA Keys and the Document Signing Keys to support the signing of the User Data (DG1 to DG16) by means of the Document Security Object. The Technical Report [ICAOPKI] describes the requirements to the public key infrastructure for the Passive Authentication.

The Document Signer of the Issuing State or Organization shall meet the requirement “Basic data authentication (FDP_DAU.1)” as specified below (Common Criteria Part 2).

FDP_DAU.1/DS Basic data authentication – Passive Authentication

Hierarchical to: No other components.

FDP_DAU.1.1/DS The **Document Signer** shall provide a capability to generate

	evidence that can be used as a guarantee of the validity of logical the MRTD (EF.DG1 to EF.DG16) and the Document Security Object[89].
FDP_DAU.1.2/DS	The **Document Signer** shall provide Inspection Systems of Receiving States or Organization[90] with the ability to verify evidence of the validity of the indicated information.

5.3.2 Extended Access Control PKI

The CVCA and the DV shall establish a Document Verification PKI by generating asymmetric key pairs and certificates for the CVCA, DV and IS which may be verified by the TOE. The following SFR use the term "PKI" as synonym for entities like CVCA, DV and IS which may be responsible to perform the identified functionality.

The Basic Terminal shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2).

FCS_CKM.1/PKI Cryptographic key generation –Document Verification PKI Keys

Hierarchical to: No other components.

FCS_CKM.1.1/PKI	The **PKI** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDSA*[91] and specified cryptographic key sizes *192, 224, 256, 288 or 320 Bit*[92] that meet the following: [BSI], Annex A[93].

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/CERT_SIGN Cryptographic operation – Certificate Signing

[89] [assignment: *list of objects or information types*]

[90] [assignment: *list of subjects*]

[91] [*assignment: cryptographic key generation algorithm*]

[92] [*assignment: cryptographic key sizes*]

[93] [*assignment: list of standards*]

Hierarchical to: No other components.

FCS_CKM.1.1/ CERT_SIGN: The **PKI** shall digital signature creation[94] in accordance with a specified cryptographic algorithm *ECDSA*[95] and cryptographic key sizes *192, 224, 256, 288 or 320 Bit*[96] that meet the following: *[BSI], Annex A*[97].

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
FMT_MSA.2 Secure security attributes

5.3.3 Basic Terminal

This section describes common security functional requirements to the Basic Inspection Systems and the Personalization Agent if it uses the Basic Access Control Mechanism with the Personalization Agent Authentication Keys. Both are called “Basic Terminals” (BT) in this section.

The Basic Terminal shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (Common Criteria Part 2).

FCS_CKM.1/KDF_BT Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal

Hierarchical to: No other components.

FCS_CKM.1.1/ BAC_BT: The **Basic Terminal** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[98] and specified cryptographic key sizes 112 bit[99] that meet the following: *[ICAOPKI], Annex E*[100].

[94] [assignment: *list of cryptographic operations*]

[95] [*assignment: cryptographic key generation algorithm*]

[96] [*assignment: cryptographic key sizes*]

[97] [*assignment: list of standards*]

[98] [*assignment: cryptographic key generation algorithm*]

[99] [*assignment: cryptographic key sizes*]

[100] [*assignment: list of standards*]

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FDP_ITC.2 Import of user data with security attributes or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

A terminal derives the Document Basic Access Keys from the second line of the printed MRZ data by the algorithm described in [ICAOPKI], 3.2.2 and Annex E.1, use them to generate the Document Basic Access Keys. The Personalization Agent downloads these keys to the MRTD's chip as TSF data for FIA_UAU.4/ BAC_MRTD.

The Basic Terminal shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/BT Cryptographic key destruction - BT

Hierarchical to: No other components.

FCS_CKM.4.1/BT The **Basis Terminal** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with zeros or random data*[101] that meets the following: *none*[102].

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]
FMT_MSA.2 Secure security attributes

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

FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal

Hierarchical to: No other components.

[101] [*assignment: cryptographic key destruction method*]

[102] [*assignment: list of standards*]

FCS_COP.1.1/ SHA_BT	The **Basic Terminal** shall perform hashing[103] in accordance with a specified cryptographic algorithms SHA-1[104] and cryptographic key sizes none[105] that meet the following: FIPS 180-2[106].
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/ ENC_BT	The **Basic Terminal** shall perform secure messaging – encryption and decryption[107] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[108] and cryptographic key sizes 112 bit[109] that meet the following: FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)[110].
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/MAC_BT Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal

Hierarchical to: No other components.

[103] [assignment: *list of cryptographic operations*]

[104] [assignment: *cryptographic algorithm*]

[105] [assignment: *cryptographic key sizes*]

[106] [assignment: *list of standards*]

[107] [assignment: *list of cryptographic operations*]

[108] [assignment: *cryptographic algorithm*]

[109] [assignment: *cryptographic key sizes*]

[110] [assignment: *list of standards*]

FCS_COP.1.1/ MAC_BT	The **Basic Terminal** shall perform secure messaging – message authentication code[111] in accordance with a specified cryptographic algorithm Retail-MAC[112] and cryptographic key sizes 112 bit[113] that meet the following: FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)[114].

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
FMT_MSA.2 Secure security attributes

The Terminal shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below. For the extended components definition refer to [EACPP] chapter 4.

FCS_RND.1/BT Quality metric for random numbers by Basic Terminal

Hierarchical to: No other components.

FCS_RND.1.1/BT	The **Basic Terminal** shall provide a mechanism to generate random numbers that meets *the probability of repetition of keying material K IFD among* 10^8 *candidates is less than* 2^{-64}[115].

Dependencies: No dependencies.

This quality metric ensures the strength of function Basic Access Control Authentication for the challenges, since it prevent replay attacks. The quality of the keying material base as well on the quality metric that meets the TOE.

A random generator with an entropy of 7.976 Bit per Byte meets this requirement.

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

FIA_UAU.4/BT Single-use authentication mechanisms –Basic Terminal

[111] [assignment: *list of cryptographic operations*]

[112] [assignment: *cryptographic algorithm*]

[113] [assignment: *cryptographic key sizes*]

[114] [assignment: *list of standards*]

[115] [assignment: *a defined quality metric*]

Hierarchical to: No other components.

FIA_UAU.4.1/BT	The **Basic Terminal** shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism[116].

Dependencies: No dependencies.

The Basic Access Control Authentication Mechanism [ICAOPKI] uses a challenge RND.IFD freshly and sufficiently randomly generated by the terminal to prevent reuse of a response generated by a MRTD's chip and of the session keys from a successful run of authentication protocol.

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

FIA_UAU.6/BT Re-authentication – Basic Terminal

Hierarchical to: No other components.

FIA_UAU.6.1/BT	The **Basic Terminal** shall re-authenticate the user under the conditions each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism[117].

Dependencies: No dependencies.

The authentication fails if an MRTD's response with an incorrect message authentication code is received.

5.3.4 General Inspection System

The General Inspection System (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism. Therefore it has to fulfill all security requirements of the Basic Inspection System as described above.

The General Inspection System verifies the authenticity of the MRTD's by the Chip Authentication Mechanism during inspection and establishes new secure messaging with keys. The reference data for the Chip Authentication Mechanism is the Chi p

[116] [assignment: *identified authentication mechanism(*s)]

[117] [assignment: *list of conditions under which re-authentication is required*]

Authentication Public Key read form the logical MRTD data group EF.DG14 and verified by Passive Authentication (cf. to FDP_DAU.1/DS). Note, that the Chip Authentication Mechanism requires the General Inspection System to verify at least one message authentication code of a response sent by the MRTD to check the authenticity of the chip.

The General Inspection System shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below:

FCS_CKM.1/DH_GIS Cryptographic key generation – Diffie-Hellman Keys by the GIS

Hierarchical to: No other components.

FCS_CKM.1.1/ DH_GIS	The **General Inspection System** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH*[118] and specified cryptographic key sizes *192, 224, 288 or 320 Bit*[119] that meet the following: [BSI], Annex A.1[120].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

A GIS generates a shared secret value with the terminal during the Chip Authentication Protocol (see [BSI], sec. 3.1 and Annex A.1, [ECCTR]). This protocol is based on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [BSI], Annex A.1 and [ISO15946-3]). The shared secret value is used to derive the 112 bit Triple-DES key for encryption and the 112 bit Retail-MAC keys according to the Document Basic Access Key Derivation Algorithm [ICAOPKI, Annex E.1], for the TSF required by FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD.

The General Inspection System shall meet the requirement "Cryptographic key operation (FCS_COP.1)" as specified below (Common Criteria Part 2).

FCS_COP.1/SHA_GIS Cryptographic operation – Hash for Key Derivation by GIS

Hierarchical to: No other components.

[118] [assignment: *cryptographic key generation algorithm*]

[119] [assignment: *cryptographic key sizes*]

[120] [assignment: *list of standards*]

FCS_COP.1.1/ SHA_GIS	The **General Inspection System** shall perform hashing[121] in accordance with a specified cryptographic algorithm *SHA-1*[122] and cryptographic key sizes none[123] that meet the following: FIPS 180-2[124].

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
FMT_MSA.2 Secure security attributes

The General Inspection System shall meet the requirement "Single-use authentication mechanisms (FIA_UAU.4)" as specified below:

FIA_UAU.4/GIS Single-use authentication mechanisms - Single-use authentication of the Terminal by the GIS

Hierarchical to: No other components.

FIA_UAU.4.1/GIS The **General Inspection System** shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication Protocol[125].

Dependencies: No dependencies.

The General Inspection System shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below:

FIA_UAU.5/GIS Multiple authentication mechanisms – General Inspection System

Hierarchical to: No other components.

FIA_UAU.5.1/GIS The **General Inspection System** shall provide

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication[126]

to support user authentication.

[121] [assignment: *list of cryptographic operations*]

[122] [assignment: *cryptographic algorithm*]

[123] [assignment: *cryptographic key sizes*]

[124] [assignment: *list of standards*]

[125] [assignment: *identified authentication mechanism(*s)]

FIA_UAU.5.2/GIS The **General Inspection System** shall authenticate any user's claimed identity according to the following rules:

1. The General Inspection System accepts the authentication attempt as MRTD only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
2. After successful authentication as MRTD and until the completion of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of secure messaging with key agreed with the authenticated MRTD by means of the Basic Access Control Authentication Mechanism.
3. After run of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.[127]

Dependencies: No dependencies.

The General Inspection System and the MRTD use secure messaging with the keys generated by the Chip Authentication Mechanism after the mutual authentication.

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

FIA_UAU.6/GIS Re-authenticating – Re-authenticating of Terminal by the General Inspection System

Hierarchical to: No other components.

FIA_UAU.6.1/GIS The **General Inspection System** shall re-authenticate the user under the conditions

1. Each response sent to the General Inspection System after successful authentication of the MRTD with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall have a correct MAC created by means of secure messaging keys agreed upon by the Basic Access Control Authentication Mechanism.

[126] [assignment: *list of multiple authentication mechanisms*]

[127] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

2. Each response sent to the General Inspection System after successful run of the Chip Authentication Protocol shall have a correct MAC created by means of secure messaging keys generated by Chip Authentication Protocol[128].

Dependencies: No dependencies.

The General Inspection System checks by secure messaging in MAC_ENC mode each response based on Retail-MAC whether it was sent by the successfully authenticated MRTD (see FCS_COP.1/MAC_MRTD for further details). The General Inspection System does not accept any response with incorrect message authentication code.

The General Inspection System shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below:

FDP_UCT.1/GIS Basic data exchange confidentiality - General Inspection System

Hierarchical to: No other components.

FDP_UCT.1.1/GIS	The **General Inspection System** shall enforce the Access Control SFP[129] to be able to transmit and receive[130] objects in a manner protected from unauthorized disclosure **after Chip Authentication**.
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]

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

FDP_UIT.1/GIS Data exchange integrity - General Inspection System

Hierarchical to: No other components.

FDP_UIT.1.1/GIS	The **General Inspection System** shall enforce the Basic Access Control SFP[131] to be able to transmit and receive[132] user data in a manner protected from modification, deletion, insertion and replay[133] errors **after Chip Authentication**.

[128] [assignment: *list of conditions under which re-authentication is required*]

[129] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[130] [selection*: transmit, receive*]

[131] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[132] [selection*: transmit, receive*]

[133] [selection: *modification, deletion, insertion, replay*]

FDP_UIT.1.2/GIS	The **General Inspection System** shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[134] has occurred **after Chip Authentication**.

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

5.3.5 Extended Inspection System

The **Extended Inspection System** (EIS) in addition to the General Inspection System implements the Terminal Authentication Protocol and is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

FCS_COP.1/SIG_SIGN_EIS Cryptographic operation – Signature creation by EIS

Hierarchical to: No other components.

FCS_COP.1.1/ SIG_SIGN_EIS	The **Extended Inspection System** shall perform signature creation[135] in accordance with a specified cryptographic algorithm *ECDSA*[136] and cryptographic key sizes *192, 224, 256, 288 or 320 Bit*[137] that meet the following: *ISO 15946 [ISO15946]*[138].

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
FMT_MSA.2 Secure security attributes

Application Note: The key sizes of 192, 224, 256, 288 and 320 Bits specified here imply that the MRTD chip can verify ECDSA-signatures based on SHA-1, SHA-224 and SHA-256.

FCS_COP.1/SHA_EIS Cryptographic operation – Hash for Key Derivation by EIS

Hierarchical to: No other components.

[134] [selection: *modification*, *deletion, insertion, replay*]

[135] [assignment: *list of cryptographic operations*]

[136] [assignment: *cryptographic algorithm*]

[137] [assignment: *cryptographic key sizes*]

[138] [assignment: *list of standards*]

FCS_COP.1.1/ SHA_EIS	The **Extended Inspection System** shall perform hashing[139] in accordance with a specified cryptographic algorithms *SHA-1*[140] and cryptographic key sizes none[141] that meet the following: FIPS 180-2[142].

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
FMT_MSA.2 Secure security attributes

The TOE implements the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism (cf. [ICAOPKI], annex E.1). The security of key derivation is not affected by the recent collision attacks on SHA-1.

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

FIA_API.1/EIS Authentication Proof of Identity – Extended Inspection System

Hierarchical to: No other components.

FIA_API.1.1/EIS	The **Extended Inspection System** shall provide a Terminal Authentication Protocol according to [BSI][143] to prove the identity of the Extended Inspection system[144].

Dependencies: No dependencies.

The Extended Inspection system requests a challenge of 8 Byte from the MRTD and generates a digital signature using ECDSA (cf. [BSI, Appendix A.2.1 for details).

[139] [assignment: *list of cryptographic operations*]

[140] [assignment: *cryptographic algorithm*]

[141] [assignment: *cryptographic key sizes*]

[142] [assignment: *list of standards*]

[143] [assignment: *authentication mechanism*]

[144] [assignment: *authorized user or rule*]

5.3.6 Personalization Terminals

The TOE supports different authentication and access control mechanisms which may be used for the Personalization Agent depending on the personalization scheme of the Issuing State or Organization:

(1) The Basic Access Control Mechanism which may be used by the Personalization Terminal with a Personalization Agent Secret Key Pair. The Basic Access Control Mechanism establishes strong cryptographic keys for the secure messaging to ensure the confidentiality by Triple-DES and integrity by Retail-MAC of the transmitted data. This approach may be used in a personalization environment where the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

(2) The Personalization Terminal may use the Terminal Authentication Protocol like an Extended Inspection System but using the Personalization Agent Keys to authenticate themselves to the TOE. This approach may be used in a personalization environment where (i) the Personalization Agent want to authenticate the MRTD's chip and (ii) the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

(3) In a centralized personalization scheme the major issue is high productivity of personalization in a high secure environment. In this case the personalization agent may wish to reduce the protocol to symmetric authentication of the terminal without secure messaging. Therefore the TOE and the Personalization Terminal support a simple the Symmetric Authentication Mechanism with Personalization Agent Key as requested by the SFR FIA_UAU.4/MRTD and FIA_API.1/ SYM_PT.

The Personalization Terminal shall meet the requirement "Authentication Proof of Identity (FIA_API)" as specified below (Common Criteria Part 2 extended) if it uses the Symmetric Authentication Mechanism with Personalization Agent Key.

FIA_API.1/SYM_PT Authentication Proof of Identity – Personalization Terminal Authentication with Symmetric Key

Hierarchical to: No other components.

FIA_API.1.1/ SYM_PT	The **Personalization Terminal** shall provide an Authentication Mechanism based on Triple-DES[145] to prove the identity of the Personalization Agent[146].

[145] [assignment: *authentication mechanism*]

Dependencies: No dependencies.

The Symmetric Authentication Mechanism for Personalization Agents is intended to be used in a high secure personalization environment only. It uses the symmetric cryptographic Personalization Agent Authentication Secret key of 112 bits to encrypt a challenge of 8 Bytes with Triple-DES which the terminal receives from the MRTD's chip e.g. as response of a GET CHALLENGE. The answer may be sent by means of the EXTERNAL AUTHENTICATE command according to ISO 7816-4 [ISO7816] command. In this case the communication may be performed without secure messaging (note, that FIA_UAU.5.2 requires secure messaging only after run of Basic Access Control Authentication).

5.4 Security Assurance Requirements Rationale/ Strength of Function

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 additional security specific engineering costs.

The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the MRTD's chip especially for the absence of unintended functionality.

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 minimal strength of function "high" was selected to ensure resistance against direct attacks on functions based on probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE to fulfill OT.AC_PERS and OT.Data_Conf if the TOE is configured for the use with Basic Inspection Systems. This is consistent with the security objective OD.Assurance.

The components ADV_IMP.2 and ALC_DVS.2 augmented to EAL4 has dependencies to other security requirements fulfilled within EAL4

[146] [assignment: *authorized user or rule*]

Dependencies ADV_IMP.2

ADV_LLD.1 Descriptive low-level design

ALC_TAT.1 Well-defined development tools

Dependencies ALC_DVS.2: no.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 SF2 (SF_HA): Identification and Authentication based on Challenge-Response

SF2 allows the authentication of a user or an application. SF2 stores appropriate keys.

SF2 uses unilateral and mutual authentication mechanisms based on a Challenge-Response-Protocol, which makes use of random numbers during the authentication process, the Basic Access Control Authentication Mechanism, the Terminal Authentication and the Authentication based on Triple DES (FIA_UAU.4, FIA_UAU.5) with 112 bit key length. The challenge contains the random number of 8 bytes depending on the selected mechanism and will be sent from one party to the other. The latter answers with a response that can be verified by the first. A mutual authentication is a combination of two Challenge-Response procedures, where both parties act as claimant and verifier.

SF2 accepts authentication attempt as Personalization Agent by the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key and the Terminal Authentication Protocol with Personalization Agent Keys. It accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. SF2 accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism. After successfull authentication the assigned access rights are maintained by the TOE.

Ahead the protocol SF2 allows the access to unprotected data that is necessary to complete the protocol (FIA_UID.1, FIA_UAU.1)

SF2 detects each unsuccessful authentication attempt. In such a case it warns the entity connected. The number of allowed authentications for a user may be bounded by a usage counter. The number of consecutive unsuccessfull authentication attempts during a single power-on session is bounded by a retry counter set to 1.

In case of regular termination of the protocol both parties possess authentic key material known only by them. The key derivation algorithm uses the hash function SHA-1 [FIPS180] which remains appropriate despite of the recently successful collision

attacks. Because the TSF uses freshly generated random numbers of 8 bytes in the protocol it prevents the replay of old authentication data in the Basic Access Control Authentication Mechanism, the Terminal Authentication and the Authentication based on Triple DES (FIA_UAU.4) with 112 bit key length.

This TSF is implemented in the Basic Access Control Protocol [ICAOPKI] as a mutual authentication, and in the Chip Authentication and the Terminal Authentication Protocols as a unilateral authentication procedures (FCS_CKM.1/KDF_MRTD, FCS_CKM.1/ DH_MRTD). The described in the Technical Report [BSI] binding of these two authentications gives a mutual authentication as well. Note that the mutual authentication in the BAC Protocol starts with challenge $RND.ICC$ from the TOE whereas the latter begins with a challenge $\widetilde{PK_{IFD}}$ from the Inspection System.

The ability for writing of Initialization Data and Pre-personalization Data is restricted to the successful authenticated Manufacturer (FMT_MTD.1/INI_ENA). The Manufacturer is allowed to read the IC Identification Data (FAU_SAS.1). The application of SF2 in this context is only possible in life cycle phase 2.

Only the successfully authenticated Personalization Agent is allowed to write the initial CVCA key, initial CVCA certificate and the initial Current Date (FMT_MTD.1/ CVCA_INI) and to disable the read access to Initialization Data (FMT_MTD.1/INI_DIS).

The SOF claimed for SF2 is high. The SOM claimed for the random number generator is high, the functionality class of its application is P2 according to [AIS31].

6.1.2 SF3 (SF_SM): Data exchange under secure messaging

A communication channel between the TOE and the Inspection System will be encrypted with a session key, such that the TOE is able to verify the integrity and authenticity of data received (FCS_CKM.1, FCS_COP, FCS_RND FIA_UAU.6). The channel will be closed if an unrecognized message (malformed cryptogram) in the channel appears. The session key is generated according to the Document Basic Access Control Key Derivation Algorithm as defined in [ICAOPKI, Annex E.1]. This document requires the usage of SHA-1 in the key derivation procedure (FCS_COP.1/ SHA_MRTD) and of Triple-DES with 112 bit key length in CBC mode as encryption algorithm (FCS_COP.1/ TDES_MRTD) and as Retail MAC algorithm (FCS_COP.1.1/ MAC_MRTD).

The communication under secure messaging provides implicitly a permanent user authentication (FIA_UAU.5).

The SOF claimed for SF3 is high. The SOM claimed for the random number generator is high, the functionality class of its application is P2 according to [AIS31].

6.1.3 SF5 (SF_AC): Access Control of stored data objects

SF5 enforces the Security Policies as required in FDP_ACF.1 on terminals gaining write and read access to the data based on the Subjects Personalization Agent, Basic Inspection System, Extended Inspection System, Terminal and the Objects: data EF.DG1 to EF.DG16, EF.COM, EF.SOD of the logical MRTD and Security attributes authentication status and authorization of terminals. The rules on which the access control is based can not be changed or disabled. The successfully authenticated Personalization Agent is allowed to write data and to read data of the EF.COM, EF:SOD, EF.DG1 to EF.DG16 of the logical MRTD, the successfully authenticated Basic Inspection System is allowed to read data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, the successfully authenticated Extended Inspection System is allowed to read data in EF.COM, EF:SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, the successfully authenticated Extended Inspection System is allowed to read data in EF.DG3 according to the Terminal Authorization, the successfully authenticated Extended Inspection System is allowed to read data in EF.DG4 according to the Terminal Authorization. A terminal authenticated as CVCA or DV is not allowed to read data in the EF.DG3 nor EF.DG4. The Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD. Depending on the authorization status other restrictions for the access applies, this includes the encryption and the integrity check of accessed data after authentication as Basic Inspection System (FCS_COP.1/ENC_BT) or the Chip Authentication (FDP_UCT.1/MRTD, FDP_UIT.1/MRTD) as well as the update of the CVCA Public Key or the CVCA certificate after authentication as CVCA (FMT_MTD.1.1/CVCA_UPD).

The read access to the Document Basic Access Keys, Chip Authentication Private Key, Personalization Agent Keys is disabled in the access rules for all users (FMT_MTD.1/ KEY_READ).

This SF protects the assets in the dedicated file of the ICAO application as well as the assets from the hardware as defined in [CR]. Any application from an other dedicated file can access any assets of the ICAO application only if it is allowed under the control of this SF which is in force before any other funtion is allowed to proceed (FPT_RVM.1).

This SF controls the reading and writing access in different phases of the production (i.e. Initialization and Pre-Personalization) and during Personalization and Operational

Use. The modification of data is not allowed. Data object can only be written completly, if the access is granted.

The Document Basic Access Keys, the initial CVCA Public Key, the CVCA certificate and an initial date will be written during Personalization (FMT_MTD.1/ KEY_WRITE, FMT_MTD.1/CVCA_INI). The SF5 restricts the ability to write the keys to the Personalization Agent only.

6.1.4 SF6 (SF_SV): Verification of digital signatures

SF6 enforces the verification of a digital signature of stored or received data. This security function is applied to the verification of certificates of public keys.

The signatures to be verified are based on ECDSA according to ISO 15946 (FCS_COP.1/SIG_VER) with key lengths of 192, 224, 256, 288 and 320 bit. The signature verification includes the mathematical correctness of the digital signature input processing, the check of the certificate chain up to a trust anchor (FMT_MTD.3) and the current date handling (cf. [BSI, 2.2.4]). The verified as valid signature in a certificate allows the TSF to maintain security roles (FMT_SMR.1) and the update of the CVCA certificate and the current date (FMT_MTD.1/CVCA_UPD, FMT_MTD.1/ DATE). A certificate chain is valid at the Current Date if and only if

(i) the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,

(ii) the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

(iii) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

Due to the algorithmic complexity brute force attacks for digital signature verification are excluded. Therefore an audit of unsuccessful verification events is not necessary.

6.1.5 SF7 (SF_RE): Reliability

The certified hardware (part of the TOE) features the following TSF. The exact formulation can be found in [CR]. This depends on the underlying hardware. The TCOS operating system ensures that they give the same functionality to this SFR.

P5CD080V0B:

1. Random Number Generator (F.RNG)
2. Triple-DES Co-processor (F.HW_DES)
3. Control of Operating Conditions (F.OPC)
4. Protection against Physical Manipulation (F.PHY)
5. Logical Protection (F.LOG)
6. Protection of Mode Control (F.COMP)
7. Memory Access Control (F.MEM_ACC)
8. Special Function Register Access Control (F.SFR_ACC)

These hardware based security functions are used in the TSF SF_RE and their function is periodically tested as required by the hardware specification. Details are contained in the functional specification and the high level design documents ADV_FSP and ADV_HLD.

SF7 monitors the following events:

- self test error,
- stored data integrity failure (checksum error over data stored in files or applications),

Each part of the program code not stored in ROM as well as every file stored in the file system is protected by integrity checks. If an integrity check for program code fails, then the TOE enters a secure state.

If an integrity check of a file fails, then the binary data may be still accessible according to the access rules if the integrity of the structure of the file is not affected. The status bytes indicate the data integrity error and thus warn the entity connected. A reading, update or writing in a transparent file or of a single record in a linear fixed record-oriented EF may be nevertheless allowed if the structural information remains correct. Any access of a file with corrupted structure is no more possible.

This SF warns the entity connected upon detection of a data integrity error of the user data stored within the TSC. Upon detection of a self test error the TOE warns the entity connected (FPT_TST.1.1).

After initialization phase is completed, all data testing-specific commands and actions are disabled. It is not possible to override these controls and restore them for use.

The TOE does not allow to analyze, debug or modify TOE's software in the field. Inputs from external sources will not be accepted as executable code (FPT_SEP.1).

The TOE preserves a secure state during power supply cut-off or variations. If power is cut (or if power variations occur) from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE will be reset cleanly (FPT_FLS.1). All non-permanently stored data is lost and will be overwritten during the next power-on. This includes e.g. all derived session keys (FCS_CKM.4).

The software part of the TOE reacts properly to all security relevant events being generated by the chip in response to any physical attack attempts as required by the chip evaluation results (cf. [CR]). This fulfils the software-part of FPT_PHP.3. Note that this functionality is partially implemented by the underlying hardware, cf. [CR].

During the execution of commands the TOE monitors the uniformity and stability of the operating system in order to avoid overloading or stressing of single components. This is implemented in the operating systems as well as in the underlying hardware.

Based on the physical protection of the TOE maintains a security domain that protects it from interference and tampering (FPT_SEP.1). The embedded software (i.e. the operating system) enforces the application of the TSF before any function is allowed to proceed (FPT_RVM.1).

The TOE ensures that the content of temporarily allocated resources is made unavailable after de-allocation by overwriting this content with zeros. This includes also the destruction of sessions keys (FCS_CKM.4) after detection of an error, because of the automatic de-allocation of these keys.

6.1.6 SF8 (SF_RN): Random Number Generation

The random number generation is a security function provided by the hardware. It is already evaluated ([CR]) as conformant to [AIS31] functionality class P2 with SOM level 'high'. This fulfils the requirement (FCS_RND.1/MRTD) of generation of random numbers with an sufficient entropy.

This security function can therefore be included here without additional considerations.

6.2 SOF claim for TSF

For TSF identified in section 6.1 the SOF-high is claimed. The following TSF base on probabilistic or permutational mechanisms:

SF2 Identification and Authentication based on Challenge-Response

The source of randomness for the session key and the strength of the encryption algorithm define the strength of this probabilistic and permutational mechanism.

SF3 Data exchange under secure messaging

The source of randomness for the session key and the strength of the encryption algorithm define the strength of this probabilistic and permutational mechanism.

The SOM claimed for the random number generator used in the TSFs is high according to [AIS31].

6.3 Assurance Measures

The documentation is produced compliant to the CC. The following documents provide the necessary information to fulfill the assurance requirements listed in 5.2.

ACM_AUT.1, ACM_CAP.4, ACM_SCP.2: Documentation for Configuration Management

ADO_DEL.2, ADO_IGS.1: Documentation for Delivery and Operation

ADV_FSP.2: Functional Specification for TCOS Passport

ADV_HLD.2: High-Level Design for TCOS Passport

ADV_IMP.2: Source Code for TCOS Passport

ADV_LLD.1: Low-Level Design for TCOS Passport

ADV_RCR.1: Correspondence Demonstration for TCOS Passport

ADV_SPM.1: Security Policy Model for TCOS Passport

AGD_ADM.1: Administrator Guidance for TCOS Passport

AGD_USR.1: User Guidance for TCOS Passport

ALC_DVS.2: Documentation for development security

ALC_LCD.1: Life-cycle model documentation

ALC_TAT.1: Documentation of the development tools

ATE_COV.2: Test Documentation for TCOS Passport

ATE_DPT.1: Test Documentation for High-Level Design for TCOS Passport

ATE_FUN.1: Test Documentation of the Functional Testing for TCOS Passport

AVA_MSU.3: Validation of analysis

AVA_SOF.1: Analysis of Strength of TSF for TCOS Passport

AVA_VLA.4: Independent vulnerability analysis for TCOS Passport

The developer team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, user documentation, administrator documentation, and security flaws. The security of the configuration management is described in detail in a separate document.

The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developer's master copy and the user's version. The Administrator and the User are provided with necessary documentation for initialization and start-up of the TOE.

The implementation is based on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements. The correspondence of the abstract specification of TSF in 6.1 with less abstract representations will be demonstrated in a separate document. This addresses ADV_FSP, ADV_HLD, ADV_LLD. ADV_IMP and ADV_RCR.

The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life-cycle model of the TOE. The development tools are well–defined and use semiformal methods, i.e. a security model.

The development department is equipped with organizational and personnel means that are necessary to develop the TOE. The testing and the vulnerability analysis require technical and theoretical know-how available at T-Systems International GmbH.

As the evaluation is identified as a composite evaluation based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.

7 PP Claims

The ST for the TOE claims conformance with the Protection Profile [EACPP] “Machine Readable Travel Document with ICAO Application“.

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR]. The IC and its primary embedded software are evaluated at level EAL 5 with a minimum strength level for its security functions of SOF-high.

8 Rationale

8.1 Security Objectives Rationale

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OD.Assurance	OD.Material	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System
T.Chip-ID			x		x														x	
T.Skimming			x																	
T.Read_Sensitive_Data				x												x				x
T.Forgery	x	x							x					x			x	x		
T.Counterfeit						x									x		x			
T.Abuse-Func							x													
T.Information_Leakage								x												
T.Phys-tamper									x											
T.Malfunction										x										
P.Manufact											x	x								
P.Personalization	x										x		x							
P.Personal_Data		x	x																x	
P.Sensitive_Data				x												x				x
A.Pers_Agent													x							
A.Insp_Sys																	x		x	
A.Signature_PKI														x			x			
A.Auth_PKI																x				x

Table 8.1.T1: Security Objective Rationale

The OSP **P.Manufact** “Manufacturing of the MRTD’s chip” requires the quality and integrity of the manufacturing process and control the MRTD’s material in the Phase 2 Manufacturing including unique identification of the IC by means of the Initialization

Data and the writing of the Pre-personalization Data. The security objective for the TOE environment **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment” address these obligations of the IC Manufacturer and MRTD Manufacturer. **OD.Material** “Control over MRTD material” ensures that materials, equipment and tools used to produce genuine and authentic MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs.

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 Authentication key(s) according to **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment”. The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

The OSP **P.Personal_Data** “Personal data protection policy” requires that the logical MRTD can be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an inspection system. This OSP is covered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the secure messaging based on session keys agreed in this protocol. The security objective **OT.Data_Conf** requires the TOE to implement the Basic Access Control as defined by ICAO [ICAOPKI] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The security objective **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD” requires the inspection system to protect their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. After successful Chip Authentication the security objective **OT.Data_Conf** “Confidentiality of personal data” ensures the confidentiality and **OT.Data_Int** “Integrity of personal data” the integrity of the logical MRTD data during their transmission to the General Inspection System.

The OSP **P.Sensitive_Data** “Privacy of sensitive biometric reference data” is fulfilled and the threat **T.Read_Sensitive_Data** “Read the sensitive biometric reference data” is countered by the TOE-objective **OT.Sens_Data_Conf** “Confidentiality of sensitive biometric reference data” requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data’s confidentiality. The authorization bases on Document Verifier certificates issued by the issuing state or organization as required by

OE.Authoriz_Sens_Data “Authorization for use of sensitive biometric reference data”. The Document Verifier of the receiving state has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems”.

The 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 by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the secure messaging based on session keys agreed in this protocol. The security objective **OT.Identification** “Identification and Authentication of the TOE” by limiting the TOE chip identification to the Basic Inspection System. The security objective **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD” requires the inspection system to protect to their communication (as Basic Inspection System) with the TOE before secure messaging based on the Chip Authentication Protocol is successfully established. After successful Chip Authentication the security objective **OT.Data_Conf** “Confidentiality of personal data” ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System.

The threat **T.Skimming** “Skimming digital MRZ data or the digital portrait” addresses the reading of the logical MRTD trough the contactless interface outside the communication between the MRTD’s chip and Inspection System. This threat is countered by the security **objective OT.Data_Conf** “Confidentiality of personal data” through Basic Access Control allowing read data access only after successful authentication of the Basic Inspection System.

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.Counterfeit** “MRTD’s chip” addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** “Proof of MRTD’s chip authentication” using an authentication key pair to be generated by the issuing state or organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by OE**.Auth_Key_MRTD** “MRTD Authentication Key”. According to **OE.Exam_MRTD** “Examination of the MRTD passport book” the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD’s chip. MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs targeted on by **OD.Material**.

The threat **T.Abuse-Func** “Abuse of Functionality” addresses attacks of misusing MRTD’s functionality to disable or bypass the TSFs. The security objective for the TOE **OT.Prot_Abuse-Func** “Protection against abuse of functionality” ensures that the usage of functions which may not be used in the operational phase is effectively prevented. Therefore attacks intending to abuse functionality in order to disclose or manipulate critical (User) Data or to affect the TOE in such a way that security features or TOE’s functions may be bypassed, deactivated, changed or explored shall be effectively countered.

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

The assumption **A.Pers_Agent** “Personalization of the MRTD’s chip” is covered by the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD” including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data and the enabling of security features of the TOE according to the decision of the Issuing State or Organization concerning the Basic Access Control.

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” which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the

Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

The assumption **A.Signature_PKI** "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment **OE.Pass_Auth_Sign "**Authentication of logical MRTD by Signature" covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_MRTD** "Examination of the MRTD passport book".

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

8.2 Security Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT:Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
FAU_SAS.1					x					
FCS_CKM.1/KDF_MRTD	x	x	x	x		x				
FCS_CKM.1/DH_MRTD	x	x		x		x				
FCS_CKM.4/MRTD	x	x	x	x						
FCS_COP.1/SHA_MRTD	x	x	x	x		x				
FCS_COP.1/TDES_MRTD	x	x	x			x				
FCS_COP.1/MAC_MRTD	x	x	x	x		x				
FCS_COP.1/SIG_VER	x			x						

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT:Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
FCS_COP.1/TDES_MRTD	x			x						
FIA_UID.1	x	x	x	x	x					
FIA_UAU.1	x	x	x	x	x					
FIA_UAU.4/MRTD	x	x	x	x						
FIA_UAU.5/MRTD	x	x	x	x						
FIA_UAU.6/MRTD	x	x	x	x						
FIA_AFL.1			x							
FIA_API.1/CAP						x				
FDP_ACC.1	x	x	x	x						
FDP_ACF.1	x	x	x	x						
FDP_UCT.1/MRTD			x	x						
FDP_UIT.1/MRTD		x		x						
FMT_SMF.1	x	x	x							
FMT_SMR.1	x	x	x							
FMT_LIM.1							x			
FMT_LIM.2							x			
FMT_MTD.1/INI_ENA					x					
FMT_MTD.1/INI_DIS					x					
FMT_MTD.1/CVCA_INI				x						
FMT_MTD.1/CVCA_UPD				x						
FMT_MTD.1/DATE				x						
FMT_MTD.1/KEY_WRITE	x		x							
FMT_MTD.1/CAPK		x	x	x		x				
FMT_MTD.1/KEY_READ	x	x	x	x		x				
FMT_MTD.3				x						
FPT_EMSEC.1	x							x		
FPT_TST.1								x		x
FPT_RVM.1							x			
FPT_FLS.1								x		x
FPT_PHP.3								x	x	
FPT_SEP.1							x			x

Table 8.2.T1: Coverage of Security Objective for the TOE by SFR

The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD and the management of the TSF for Basic Access Control. The write access to the logical MRTD data are defined by the SFR FIA_UID.1, FIA_UAU.1, FDP_ACC.1 and FDP_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. 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 Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4/MRTD and FIA_UAU.5/MRTD. If the Basic Access Control Authentication Mechanism with the Personalization Agent Authentication Key is used the TOE will use the FCS_RND.1/MRTD (for the generation of the challenge), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the MAC_ENC_Mode secure messaging) and FIA_UAU.6/MRTD (for the re-authentication). If the Personalization Terminal want to authenticate themselves to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1/MRTD (for the generation of the challenge), FCS_CKM.1/DH_MRTD, FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the MAC_ENC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6/MRTD (for the re-authentication). If the Personalization Terminal wants to authenticate themselves to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1/MRTD (for the generation of the challenge) and FCS_COP.1/TDES_MRTD (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMSEC.1 the confidentially of these keys.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the

Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD. The SFR FIA_UAU.6/MRTD and FDP_UIT.1/MRTD requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the MAC_ENC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data in 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. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: only the successful authenticated Personalization Agent, Basic Inspection Systems[147] and Extended Inspection Systems are allowed to read the data of the logical MRTD. 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 FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

The SFR FIA_AFL.1 strengthens the authentication function as terminal part of the Basic Access Control Authentication Protocol or other authentication functions if necessary. The SFR FIA_UAU.4/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5/MRTD enforces the TOE (i) to accept the authentication attempt as Basic Inspection System only by means

[147] Note the General Inspection Systems use the role Basic Inspection System.

of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and (ii) to accept chip authentication only after successful authentication as Basic Inspection System. Moreover, the SFR FIA_UAU.6/MRTD requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

After Chip authentication the TOE and the General Inspection System establish protection of the communication by secure messaging (cf. the SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD) in MAC_ENC_Mode by means of the cryptographic functions according to FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the MAC_ENC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

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

The SFR FIA_UID.1 and FIA_UAU.1 requires authentication of the inspection systems. The SFR FIA_UAU.5/MRTD requires the successful Chip Authentication before any authentication attempt as Extended Inspection System. The SFR FIA_UAU.6/MRTD and FDP_UCT.1/MRTD requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1/MRTD (for the generation of the terminal authentication challenge), FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/ MAC_MRTD for the MAC_ENC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

The security objective **OT.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.

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. The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their use 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.

The security objective **OT.Chip_Auth_Proof** "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol provided by FIA_API.1/CAP proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/DH_MRTD is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol [BSI] requires additional TSF according to FCS_CKM.1/ KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the MAC_ENC_Mode secure messaging).

The security objective **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality" is ensured by (i) the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other which may not be used after TOE Delivery, (ii) the SFR FPT_RVM.1 which prevents by monitoring the bypass and deactivation of security features or functions of the TOE, and (iii) the SFR FPT_SEP.1 which prevents change or explore security features or functions of the TOE by means of separation the other TOE functions.

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.

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

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

The security objectives **OD.Assurance** and **OD.Material** for the IT environment will be supported by non-IT security measures only.

The security objective OE.Authoriz_Sens_Data is directed to establish the Document Verifier PKI and will be supported by non-IT security measures only.

The following table provides an overview how security functional requirements for the IT environment cover security objectives for the TOE environment. The protection profile describes only those SFR of the IT environment directly related to the SFR for the TOE.

	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System
Document Signer								
FDP_DAU.1/DS		x	x		x	x		
Document Verification PKI								
FCS_CKM.1/PKI				x				
FCS_COP.1/CERT_SIGN				x				
Basic Inspection System								
FCS_CKM.1/KDF_BT	x				x		x	
FCS_CKM.4/BT					x		x	

FCS_COP.1/SHA_BT	x				x		x	
FCS_COP.1/ENC_BT	x				x		x	
FCS_COP.1/MAC_BT	x				x		x	
FCS_RND.1/BT	x				x		x	
FIA_UAU.4/BT	x				x		x	
FIA_UAU.6/BT	x				x		x	
General Inspection System								
FCS_CKM.1DH_GIS	x				x			
FCS_COP.1/SHA_GIS	x				x			
FIA_UAU.4/GIS					x			
FIA_UAU.5/GIS					x		x	
FIA_UAU.6/GIS					x		x	
FDP_UCT.1/GIS	x				x		x	
FDP_UIT.1/GIS	x				x		x	
Extended Inspection System								
FCS_COP.1/SIG_SIGN_EIS	x							x
FCS_COP.1/SHA_EIS	x							x
FIA_API.1/EIS	x							x
Personalization Agent								
FIA_API.1/SYM_PT	x							

Table 8.2.T2: Coverage of Security Objectives for the IT environment by SFR

The **OE.Personalization** “Personalization of logical MRTD” requires the Personalization Terminal to authenticate themselves to the MRTD’s chip to get the write authorization.

If the Basic Access Control Authentication Mechanism with the Personalization Agent Authentication Key is used the Personalization Terminal will use the FCS_RND.1/BT (for the generation of the challenge), FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_BT (for the derivation of the session keys), and FCS_COP.1/ENC_BT and FCS_COP.1/ MAC_BT (for the MAC_ENC_Mode secure messaging) to authenticate themselves and to protect the personalization data during transfer.

If the Personalization Terminal want to authenticate themselves to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the Personalization Terminal will use TSF according to the FCS_RND.1/BT (for the generation of the challenge), FCS_CKM.1/DH_GIS, FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_GIS (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/TDES_MRTD and FCS_COP.1/ MAC_MRTD (for the MAC_ENC_Mode secure messaging), FCS_COP.1/

SIG_SIGN_EIS, FCS_COP.1/SHA_EIS and FIA_API.1/EIS (as part of the Terminal Authentication Protocol).

If the Personalization Terminal wants to authenticate themselves to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the SFR FIA_API.1/SYM_PT, FCS_RND.1/MRTD (for the generation of the challenge) and FCS_COP.1/TDES_MRTD (to verify the authentication attempt). Using the keys derived by means of the Chip Authentication Mechanism the Personalization Agent will transfer MRTD holder's personalization data (identity, biographic data, and correctly enrolled biometric reference data) in a confidential and integrity protected manner as required by FDP_UCT.1/GIS and FDP_UIT.1/GIS.

The **OE.Pass_Auth_Sign** "Authentication of logical MRTD Signature" is covered by FDP_DAU.1/DS which requires the Document Signer to provide a capability to generate evidence for the validity of EF.DG1 to EF.DG16 and the Document Security Objects and therefore, to support the inspection system to verify the logical MRTD.

The **OE.Auth_Key_MRTD** "MRTD Authentication Key" is covered by FDP_DAU.1/DS which requires the Document Signer to provide a capability to generate evidence for the validity of chip authentication public key in DG 14. There is no need for the PP to provide any specific requirement for the method of generation, distribution and handling of the Chip Authentication Private Key by the IT environment.

The **OE.Authoriz_Sens_Data** "Authorization for Use of Sensitive Biometric Reference Data" addresses the establishment of the Document Verification PKI which include cryptographic key generation for the Document Verification PKI Keys and the signing of the certificates. The SFR FCS_CKM.1/PKI and FCS_COP.1/CERT_SIGN enforce that these cryptographic functions fit the signature verification function for the certificates and the terminal authentication addressed by FCS_COP.1/SIG_VER.

The **OE.Exam_MRTD** "Examination of the MRTD passport book" requires the Basic Inspection System for global interoperability to implement the terminal part of the Basic Access Control [ICAOPKI] as required by FCS_CKM.1/KDF_BT, FCS_CKM.4/BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT, FCS_RND.1/BT, FIA_UAU.4/BT and FIA_UAU.6/BT. The verification of the authenticity of the MRTD's chip by General Inspection Systems and Extended Inspection Systems (including the functionality of the GIS) is covered by the FCS_CKM.1/DH_GIS, FCS_COP.1/ SHA_GIS, FIA_UAU.4/GIS, FIA_UAU.5/GIS and FIA_UAU.6/GIS providing the Chip Authentication Protocol and checking continuously the messages received from the MRTD's chip. The authenticity of the Chip Authentication Public Key (EF.DG14) is ensured by FDP_DAU.1/DS.

The **OE.Pass_Auth_Verif** “Verification by Passive Authentication” is covered by the SFR FDP_DAU.1/DS.

The security objective **OE.Prot_Logical_MRTD** ”Protection of data of the logical MRTD” addresses the protection of the logical MRTD during the transmission and internal handling. The SFR FIA_UAU.4/BT, FIA_UAU.5/GIS and FIA_UAU.6/BT address the terminal part of the Basic Access Control Authentication Mechanism and FDP_UCT.1/GIS and FDP_UIT.1/BT the secure messaging established by the Chip Authentication mechanism. The SFR FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT and FCS_RND.1/BT as well as FCS_CKM.4/BT are necessary to implement this mechanism. The BIS shall destroy the Document Access Control Key and the secure messaging keys after inspection of the MRTD according to FCS_CKM.4 because they are not needed any more.

The **OE.Ext_Insp_System** “Authorization of Extended Inspection Systems” is covered by the Terminal Authentication Protocol proving the identity of the EIS as required by FIA_API.1/EIS basing on signature creation as required by FCS_COP.1/ SIG_SIGN_EIS and including a hash calculation according FCS_COP.1/SHA_EIS.

8.3 Dependency Rationale

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

The following table shows the dependencies between the SFR and of the SFR to the SAR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1/KDF_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD justification 1 for non-satisfied dependencies
FCS_CKM.1/DH_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1	FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD

SFR	Dependencies	Support of the Dependencies
	Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 2 for non-satisfied dependencies
FCS_CKM.4/MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 1 for non-satisfied dependencies
FCS_COP.1/SHA_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 3 for non-satisfied dependencies
FCS_COP.1/TDES_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 4 for non-satisfied dependencies
FCS_COP.1/MAC_MRTD	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 4 for non-satisfied dependencies
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or	FCS_CKM.1, FCS_CKM.4, justification 5 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	
FCS_RND.1/MRTD	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UAU.1 Timing of authentication	Fulfilled
FIA_UAU.4/MRTD	No dependencies	n.a.
FIA_UAU.5/MRTD	No dependencies	n.a.
FIA_UAU.6/MRTD	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled
FIA_API.1/CAP	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, FMT_MSA.3 Static attribute initialization	FDP_ACC.1, justification 6 for non-satisfied dependencies
FDP_UCT.1/MRTD	[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_ACC.1, justification 7 for non-satisfied dependencies
FDP_UIT.1/MRTD	[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_ACC.1, justification 7 for non-satisfied dependencies
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled
FMT_LIM.1	FMT_LIM.2	Fulfilled
FMT_LIM.2	FMT_LIM.1	fulfilled

SFR	Dependencies	Support of the Dependencies
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.3	ADV_SPM.1, FMT_MTD.1	fulfilled
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	ADV_SPM.1	fulfilled by EAL4
FPT_PHP.3	No dependencies	n.a.
FPT_RVM.1	No dependencies	n.a.
FPT_SEP.1	No dependencies	n.a.
FPT_TST.1	FPT_AMT.1 Abstract machine testing	See justification 8 for non-satisfied dependencies

Table 8.3.T.1: Dependencies between the SFR for the TOE

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

No. 1: The SFR FCS_CKM.1/KDF_MRTD uses only the Document Basic Access Keys or other shared secrets to generate the secure messaging keys used for FCS_COP.1/TDES and FCS_COP.1/MAC. The SFR FCS_CKM.4/MRTD destroys these keys automatically. These simple processes do not need any special security attributes for the secure messaging keys.

No. 2: The SFR FCS_CKM.1/DH_MRTD calculates shared secrets to generate the secure messaging keys used for FCS_COP.1/TDES and FCS_COP.1/MAC. The SFR FCS_CKM.4/MRTD destroys these keys automatically. These simple processes do not need any special security attributes for the secure messaging keys.

No. 3: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFRs are needed to be defined for this specific instantiation of FCS_COP.1.

No. 4: The SFR FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD use the automatically generated secure messaging keys assigned to the session with the successfully authenticated BIS only. There is no need for any special security attributes for the secure messaging keys.

No. 5: The SFR FCS_COP.1/SIG_VER uses the initial public key Country Verifying Certification Authority and the public keys in certificates provided by the terminals as TSF data for the Terminal Authentication Protocol and the Access Control. Their validity verified according to FMT_MDT.3 and their security attributes are managed by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. There is no need to import user data or manage their security attributes.

No. 6: 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.2) is necessary here.

No. 7: The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the use secure messaging between the MRTD and the BIS. There is no need for sensitive SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels it is the only one.

No. 8: The TOE consists of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

The following table shows the dependencies between the SFR for the IT environment and of the SFR to the SAR of the TOE.

SFR	Dependencies	Support of the Dependencies
FDP_DAU.1	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/PKI	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 9 for non-satisfied dependencies
FCS_COP.1/CERT_SIGN	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 9 for non-satisfied dependencies
FCS_CKM.1/KDF_BT	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS_COP.1/TDES_BT, FCS_COP.1/MAC_BT justification 10 for non-satisfied dependencies
FCS_CKM.4/BT	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 10 for non-satisfied dependencies
FCS_COP.1/SHA_BT	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 11 for non-satisfied dependencies
FCS_COP.1/ENC_BT	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 12 for non-satisfied dependencies
FCS_COP.1/MAC_BT	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or	FCS_CKM.1, FCS_CKM.4, justification 12 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	
FCS_RND.1/BT	No dependencies	n.a.
FIA_UAU.4/BT	No dependencies	n.a.
FIA_UAU.6/BT	No dependencies	n.a.
FCS_CKM.1/DH_GIS	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_COP.1/MAC_BT, FCS_CKM.4/BT, justification 13 for non-satisfied dependencies
FCS_COP.1/SHA_GIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_COP.1/MAC_BT, FCS_CKM.4/BT, justification 13 for non-satisfied dependencies
FIA_UAU.4/GIS	No dependencies	n.a.
FIA_UAU.5/GIS	No dependencies	n.a.
FIA_UAU.6/GIS	No dependencies	n.a.
FDP_UCT.1/GIS	[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]	justification 14 for non-satisfied dependencies
FDP_UIT.1/GIS	[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]	justification 14 for non-satisfied dependencies
FCS_COP.1/SIG_SIGN_EIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 15 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/SHA_EIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 15 for non-satisfied dependencies
FIA_API.1/EIS	No dependencies	n.a.
FIA_API.1/SYM_PT	No dependencies	n.a.

Table 8.3.T.2: Dependencies between the SFR for the IT environment

Justification for non-satisfied dependencies between the SFR for the IT environment.

No. 9: The TOE does not have specific functional security requirements to the IT environment establishing Document Verification PKI which have to be described by the listed dependency here.

No. 10: The SFR FCS_CKM.1/KDF_BT derives the Document Basic Access Keys and uses this key to generate the secure messaging keys used for FCS_COP.1/TDES and FCS_COP.1/MAC. The SFR FCS_CKM.4/BT destroys these keys. These processes do not need any special security attributes for the secure messaging keys.

No. 11: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR is needed to be defined for this specific instantiation of FCS_COP.1.

No. 12: The SFR FCS_COP.1/TDES_BT and FCS_COP.1/MAC_BT use the automatically generated secure messaging keys assigned to the session with the successfully authenticated MRTD only. There is no need for any special security attributes for the secure messaging keys.

No. 13: The SFR FCS_CKM.1/DH_GIS and FCS_COP.1/SHA_GIS are used for generation of secure messaging session keys by means of the Chip Authentication Protocol. These session keys are destroyed by the same function as for the Basic Terminal (cf. FCS_CKM.4/BT). There is no need for import or management of security attributes of these session keys.

No. 14: The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the use secure messaging between the MRTD and the GIS as described by the FDP_UCT.1/GIS and FDP_UIT.1/GIS. There is no need to provide further description of this communication.

No. 15: The SFR FCS_COP.1/SIGN_EIS and FCS_COP.1/SHA_EIS are used by the Extended Inspection System for the proof of identity to the TOE by means of the Terminal Authentication Key Pair. The TOE does not have any specific requirements for the method of importing (cf. FDP_ITC.1 or FDP_ITC.2) or generation (cf. FCS_CKM.1) of the Terminal Authentication Key Pair, which is completely up to the IT environment.

8.4 Evaluation Assurance Level Rationale

The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the MRTD's chip especially for the absence of unintended functionality.

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 selection of the component AVA_MSU.3 provides a higher assurance of the security of the MRTD's usage especially in phase 3 "Personalization of the MRTD" and Phase 4 "Operational Use". It is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

The minimal strength of function "high" was selected to ensure resistance against direct attacks on functions based on probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE to fulfil the OT.Sens_Data_Conf and OT.Chip_Auth_Proof. This is consistent with the security objective OD.Assurance.

The selection of the component AVA_VLA.4 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives OT.Sens_Data_Conf, OT.Chip_Auth_Proof and OD.Assurance.

The component ADV_IMP.2 has the following dependencies:

- ADV_LLD.1 Descriptive low-level design
- ADV_RCR.1 Informal correspondence demonstration
- ALC_TAT.1 Well-defined development tools

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

The component ALC_DVS.2 has no dependencies.

The component AVA_MSU.3 has the following dependencies:

- ADO_IGS.1 Installation, generation, and start-up procedures
- ADV_FSP.1 Informal functional specification
- AGD_ADM.1 Administrator guidance

- AGD_USR.1 User guidance

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

The component AVA_VLA.4 has the following dependencies:

- ADV_FSP.1 Informal functional specification
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

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

8.5 Assurance and Functional Requirement to Security Objective Mapping

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL 4
ACM_CAP.4	EAL 4
ACM_SCP.2	EAL 4
ADO_DEL.2	EAL 4
ADO_IGS.1	EAL 4
ADV_FSP.2	EAL 4
ADV_HLD.2	EAL 4
ADV_IMP.2	EAL 4, Augmentation
ADV_LLD.1	EAL 4
ADV_RCR.1	EAL 4
ADV_SPM.1	EAL 4
AGD_ADM.1	EAL 4
AGD_USR.1	EAL 4
ALC_DVS.2	EAL 4, Augmentation
ALC_LCD.1	EAL 4
ALC_TAT.1	EAL 4
ATE_COV.2	EAL 4
ATE_DPT.1	EAL 4

ATE_FUN.1	EAL 4
ATE_IND.2	EAL 4
AVA_MSU.3	EAL 4, Augmentation
AVA_SOF.1	EAL 4
AVA_VLA.4	EAL 4, Augmentation

Table 8.5.T1 Assurance and Requirements mapping

8.6 TOE Summary Specification Rationale

This summary specification shows that the TSF and assurance measures are appropriate to fulfill the TOE security requirements.

8.6.1 Mapping of TOE Security Requirements and TOE Security Functions

Each TOE security functional requirement is implemented by at least one security function. The mapping of TOE Security Requirements and TOE Security Functions is given in the following table. If iterations of a TOE security requirement are covered by the same TOE security function the mapping will appear only once. The description of the TSF is given in section 6.1.

TOE Security Functional Requirements / TOE Security Functions	**SF 2 (SF_HA)**	**SF 3 (SF_SM)**	**SF 5 (SF_AC)**	**SF 6 (SF_SV)**	**SF 7 (SF_RE)**	**SF 8 (SF_RN)**
FAU_SAS.1	x					
FCS_CKM.1/KDF_MRTD	x					x
FCS_CKM.1/DH_MRTD	x					x
FCS_CKM.4/MRTD					x	
FCS_COP.1/SHA_MRTD		x				
FCS_COP.1/TDES_MRTD	x	x				
FCS_COP.1/MAC_MRTD		x				
FCS_COP.1/SIG_VER				x		
FCS_RND.1/MRTD	x					x
FIA_UID.1	x		x			
FIA_UAU.1	x					
FIA_UAU.4/MRTD	x					

FIA_UAU.5/MRTD	**x**	**x**				
FIA_UAU.6/MRTD		**x**				
FIA_AFL.1	**x**					
FIA_API.1/CAP	**x**	**x**				
FDP_ACC.1			**x**			
FDP_ACF.1			**x**			
FDP_UCT.1/MRTD			**x**			
FDP_UIT.1/MRTD	**x**		**x**			
FMT_SMF.1			**x**			
FMT_SMR.1	**x**		**x**	**x**		
FMT_LIM.1					**x**	
FMT_LIM.2					**x**	
FMT_MTD.1/INI_ENA	**x**		**x**			
FMT_MTD.1/INI_DIS	**x**		**x**			
FMT_MTD.1/CVCA_INI	**x**		**x**			
FMT_MTD.1/CVCA_UPD				**x**		
FMT_MTD.1/DATE				**x**		
FMT_MTD.1/KEY_WRITE	**x**		**x**			
FMT_MTD.1/KEY_READ			**x**			
FMT_MTD.1/CAPK	**x**		**x**			
FMT_MTD.3				**x**		
FPT_EMSEC.1					**x**	
FPT_FLS.1					**x**	
FPT_PHP.3					**x**	
FPT_RVM.1			**x**			
FPT_SEP.1					**x**	
FPT_TST.1					**x**	

Table 8.6.1.T1

In the following the rationale for the table 8.6.1.T1 is given.

The more detailed technical information how and whether the security functions actually implement the TOE security functional requirements is contained in the functional specification and the high level design documents ADV_FSP and ADV_HLD.

FAU_SAS.1: The IC Identification Data can be read by the successfully authenticated Manufacturer which is (SF2), which allows the Manufacturer to store this data in audit records. After Personalization the read access to IC Identification Data is disabled.

FCS_CKM.1/KDF_MRTD: The Document Basic Access Control Key Deriviation Algorithm specified in [ICAOPKI, Annex E.1] uses a Challenge-Response-Protocol for the derivation (SF2) of the session keys. The correctness of the keys is verified implicitly by the correct realization of the secure messaging exchange.

FCS_CKM.1/DH_MRTD: The EC Diffie Hellman Session Key Derivation Algorithm specified in [BSI, Annex A] uses a Challenge-Response-Protocol for the derivation (SF2) of the session keys. The correctness of the keys is verified implicitly by the correct realization of the secure messaging exchange.

FCS_CKM.4/MRTD: Each session key is used only by the authenticated user and is destroyed if the authentication fails or is restarted again (SF7). Additionally in case of loss of power the keys are also erased, because they are not stored permanently.

FCS_COP.1/SHA_MRTD: In [ICAOPKI, Annex E.1] the hash algorithm SHA-1 is required to be used as part of the session key derivation algorithm (SF3).

FCS_COP.1/TDES_MRTD: In [ICAOPKI, Annex E.1] the Triple DES algorithm in CBC mode is required to be used as encryption algorithm in the secure messaging(SF3).

FCS_COP.1/MAC_MRTD: In [ICAOPKI, Annex E.1] the Triple DES algorithm is required to be used as Retail MAC algorithm in the secure messaging (SF3).

FCS_COP.1/SIG_VER: The verification of the digital signatures ensures the correctness and the integrity of certificate data and the TOE challenge in the Terminal Authentication Protocol (SF6).

FCS_RND.1/MRTD The randomness of challenges used in SF2 will be provided by SF8. To acchieve an SOF “high” the generated data must have a sufficient entropy. This is fulfilled automatically if the random number generator is certified as P2 according [AIS31].

FIA_UID.1: The identification data used by SF2 is maintained by the TOE and can not be changed. The access rules allow to establish a communication channel before the user is identified (SF2). The access rules prevent the use of other commands for non identified users.

FIA_UAU.1: The access rules allow to establish a communication channel before the user is authenticated. After successful authentication provided by SF2 a security status is maintained. Based on that status the access rules apply that allow or disallow the execution of commands and the access to security data controled under SF5.

FIA_UAU.4/MRTD, The data used after authentication in SF2 is generated based on a randomly chosen challenge each time the authentication is started, therefore a re-use of old data is not possible.

FIA_UAU.5/MRTD: The authentication of a Personalization Agent and a Inspection System both use SF2, nethertheless they represent different roles controlled by SF5. SF2 accepts authentication attempt as Personalization Agent by the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key and the Terminal Authentication Protocol with Personalization Agent Keys. It accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. SF2 accepts the

authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging (SF3) with key agreed with the authenticated terminal by means of the Basic Access Control Authentication Mechanism. After run of the Chip Authentication Mechanism the TOE accepts only received commands with correct message authentication code sent by means of secure messaging (SF3) with key agreed with the terminal by means of the Chip Authentication Mechanism.

FIA_UAU.6/MRTD: SF3 guarantees based on the inherent MAC verification in the secure messaging mechanism that the reauthentication of the user (Personalization Agent, Terminal) is possible for every command after successful authentication.

FIA_AFL.1: The unsuccessful authentication attempts will be detected by SF2, if 1 consecutive attempts occur the TOE blocks until a power-on reset.

FIA_API.1/CAP: The Chip Authentication Protocol is one mechanism based on a Challenge-Response-Protocol provided by SF2, it is completed if the implicit verify-cation based on SF3 succeeds.

FDP_ACC.1: The modification of data is not allowed by SF5, according to the Access Control SFP access rules data may only be read or written anew.

FDP_ACF.1: The access control is enforced by SF5 based on the following rules that can not be changed or disabled. The successfully authenticated Personalization Agent is allowed to write data and to read data of the EF.COM, EF:SOD, EF.DG1 to EF.DG16 of the logical MRTD, the successfully authenticated Basic Inspection System is allowed to read data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, the successfully authenticated Extended Inspection System is allowed to read data in EF.COM, EF:SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, the successfully authenticated Extended Inspection System is allowed to read data in EF.DG3 according to the Terminal Authorization, the successfully authenticated Extended Inspection System is allowed to read data in EF.DG4 according to the Terminal Authorization. A terminal authenticated as CVCA or DV is not allowed to read data in the EF.DG3 nor EF.DG4. the Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.

FDP_UCT.1/MRTD: The enforcement of the the access rules implies the application of encryption to the communication after successful Chip Authentication via SF3 The encryption key is derived from the Chip Authentication Protocol provided by SF2.

FDP_UIT.1/MRTD: The data integrity is enforced implicitly by the access control mechanism of SF5, requiring to supply the accessed data with a MAC. The integrity check key is derived from the Chip Authentication Protocol provided by SF2.

FMT_SMF.1, FMT_SMR.1, FPT_RVM.1: Maintaining the different role and different functions uses the defined access control rules that can not be changed or disabled. The assignment of a specific role is supported by an authentication based on SF2 and/ or SF3. The embedded software (i.e. the operating system) enforces the application of the TSF before any function is allowed to proceed.

FMT_LIM.1, FMT_LIM.2: Limitations of capabilities or availability are enforced by SF7 controlling the integrity of the stored access rules and the used functions. After Initialization all data testing-specific commands and actions are disabled. It is not possible to override these controls and restore them for use.

FMT_MTD.1/INI_ENA: The role of the Manufacturer is disabled for the TOE, because the Initialization and Pre-Personalization is finished before the TOE is completed. It is nevertheless included here, because the Manufacturer uses the means provided by SF2, SF3 and SF5 already in these life cycle phases. The write access in the Initialization and Pre-Personalization phases is based on a command of the Operating System that uses the SF2 authentication for the Manufacturer. It can be used in Life Cycle Phase 2 only and is disabled later.

FMT_MTD.1/INI_DIS: Based on the authentication provided by SF2 the Personalization Agent disables the read access for the Initialization Data. This access rule can not be disabled. Note that the read access for other users than the Personalzation Agent was not allowed already before.

FMT_MTD.1/CVCA_INI: Based on the authentication provided by SF2 only the Personalization Agent Agent is allowed to write the initial CVCA key, initial CVCA certificate and the initial Current Date. This access rule can not be disabled.

FMT_MTD.1/CVCA_UPD: The update of the CVCA key and CVCA certificate is allowed only if the terminal authenticates itself as a valid CVCA based on SF6 (cf. FMT_MTD.3). This access rule can not be disabled.

FMT_MTD.1/DATE: The data of the Current Date can be overwritten by an terminal that authenticates itself as CVCA, DV or domestic EIS. This is based on the validation provided by SF6 of a certificate containing the holder authorization/access rights. This access rule can not be disabled.

FMT_MTD.1/KEY_WRITE: The Document Basic Access Keys can only be written during Personalization and only by the sucessfully authenticated Personalization Agent (SF2). This access rule can not be disabled (SF5).

FMT_MTD.1/CAPK: Only during Personalization the Chip Authentication Private Key can be written and only by the sucessfully authenticated Personalization Agent (SF2). If the Chip Authentication Private Key is already contained in the file system, i.e. was loaded by the Manufacturer during Manufacturing then the Personalization Agent validates key, i.e. checks the correspondence of this private key and MRTD's public key contained in EF.DG14. This access rule can not be disabled (SF5).

FMT_MTD.1/KEY_READ: The read access to the Document Basic Access Keys, Chip Authentication Private Key, Personalization Agent Keys is disabled in the access rules (SF6).

FMT_MTD.3: SF6 guarantees that only valid certificates and this includes the existence of a valid certificate chain up to the trust anchor (CVCA certifiacte) are accepted.

FPT_EMSEC.1: SF7 monitors the regular execution of commands, and if variations occur with test failures or integrity mismatch the communication is closed. The strict care of uniformity and non-overloading single components is implemented in the Operating System and will be described detailed in ADV, ATE und AVA documentation.

This implies the leakage of information about the Personalization Agent Authentication Key and the Chip Authentication Key.

FPT_FLS.1: SF7 guarantees that the TOE preserves a secure state if a test failure or integrity check mismatch occur.

FPT_PHP.3: SF7 monitors the regular execution of commands, and if variations occur with test failures or integrity mismatch the communication will be closed immediately.

FPT_SEP.1: Based on the physical protection of the TOE maintains a security domain that protects it from interference and tampering. The embedded software (i.e. the operating system) enforces the application of the TSF before any function is allowed to proceed (FPT_RVM.1).

FPT_TST.1: The self-tests of the underlying hardware and additional test maintained by SF7 provide the means for demonstrating that the TSF operation is correct and that the data is not manipulated.

8.6.2 Assurance measure rationale

Assurance measures from chapter 6.3 cover the assurance requirements from 5.4.

8.6.3 Rationale for Minimum Strength of Function High

The TOE shall demonstrate to be medium resistant against penetration attacks in order to meet the security objectives from [EACPP]. The protection against attacks with a high attack potential against the security functions dictates a high rating for strength of functions in the TOE that are realized by probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE to fulfill OT.AC_PERS and OT.Data_Conf if the TOE is configured for the use with Basic Inspection Systems. This is also consistent with the security objective OD.Assurance.

A metric for the entropy of randomly generated numbers of 0.75 for each bit is sufficient if the key length is 112 bit. This implies that at least 2^{84} different keys are used, which is impossible to break by brute force even with high attack potential.

The SOF of SF is consistent with SOF of the functional requirement because all are selected 'high'.

8.7 PP Claims Rationale

There are no deviations in the ST security objectives and requirements from those of [EACPP] to which conformance is claimed.

Appendix 1. Glossary

This is the unchanged chapter from [EACPP], more detailed can be found there, too.

Term	Definition
Active Authentication	Security mechanism defined in [ICAOPKI] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD 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 (cf. CC part 1, section B.2.7).
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [ICAOPKI] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with 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 themselves to the MRTD's chip using the Document Basic Access Keys. drawn form printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa.
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (selfsigned certificate).
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Country Signing CA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing Country or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD. It is
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [ICAOPKI], Annex E.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [ICAOPKI]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the

	passport book.
Document Security Object (SOD)	An 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 MRTD's chip. It may carry the Document Signer Certificate (CDS). [ICAOPKI]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations
Eavesdropper	A threat agent with low 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.
Extended Access Control	Security mechanism identified in [ICAOPKI] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the Biographical data or the portrait.
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in differentStates throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document.
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required.
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 MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity.
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit. *Integrity* Ability to confirm the MRTD and its

	data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
IssuingOrganization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer).]
Issuing State	The Country issuing the MRTD.
Logical DataStructure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAOLDS]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [ICAOLDS] 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).
Logical travel Document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
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.
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.
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods.
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.
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 [ICAOLDS], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13 and EF.DG16) 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 ICAO.
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 MRTD holder in the MRTD'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 portrait, signature and biographical data are applied to the

	document.
Personalization Agent	The agent acting on the behalf of the issuing State or organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.
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 Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.
Receiving State	The Country to which the MRTD holder is applying for entry.
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.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.
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 MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be all valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or organization which may be used by the rightful holder for international travel.
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE
Unpersonalized MRTD	MRTD material prepared to produce a personalized MRTD containing an initialised and pre-personalized MRTD's chip
User data	Data created by and for the user that does not affect the operation of the TSF.
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template.
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.

Appendix 2. Extended Components Definition

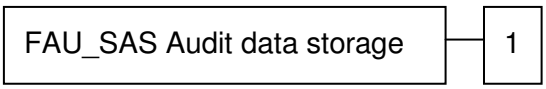
This appendix contains the extended Components Definitions of chapter 4 of [EACPP].

1. FAU_SAS Audit data storage

The family “Audit data storage (FAU_SAS)” is specified as follows.

Family behaviour

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



Component levelling

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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.

Dependencies: No dependencies.

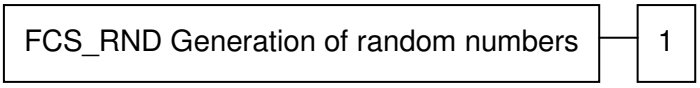
2. FCS_RND Generation of random numbers

The family “Generation of random numbers (FCS_RND)” is specified as follows.

Family behaviour

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

Component levelling:



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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

Dependencies: No dependencies.

3. FIA_API Authentication Proof of Identity

The family “ Authentication Proof of Identity (FIA_API)” is specified as follows.

Family behaviour

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

Component levelling:

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or rule*].

Dependencies: No dependencies.

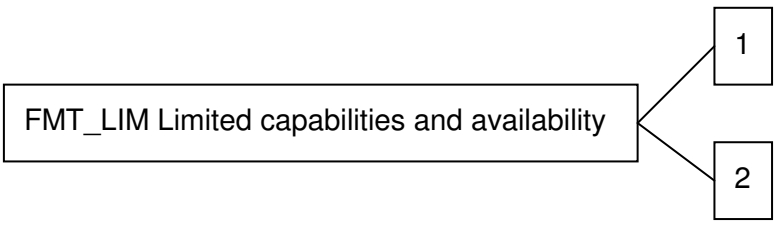
4. FMT_LIM Limited capabilities and availability

The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

Family behaviour

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

Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's lifecycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: Limited capability and availability policy].

Dependencies: FMT_LIM.2 Limited availability.

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: Limited capability and availability policy].

Dependencies: FMT_LIM.1 Limited capabilities.

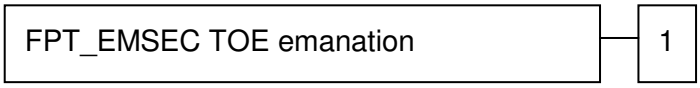
5. FPT_EMSEC

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

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access

to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Dependencies: No other components.

9 References

[AIS31]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, Version 1 vom 25.09.2001, BSI

[AIS36]

Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36Version 1 vom 29.07.2002, BSI

[BSI]

Dennis Kuegler, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.01, BSI, TR-03110, 2006-11-14

[CR]

Certification Reports of underlying hardware
BSI-DSZ-CC-0410-2007 for P5CD080V0B

[CC]

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

[EACPP]

CC Protection Profile Machine Readable Travel Document with „ICAO Application" Extended Access Control, Version 1.2, BSI-PP-0026, 2007-11-19

[ECCTR]

Technical Guideline: Elliptic Curve Cryptography (ECC) based on ISO 15946,TR-03111, Version 1.01 (BETA), BSI 2006.

[FIPS46]

Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. DoC/NIST

[FIPS180]

Federal Information Processing Standards Publication FIPS PUB 180-2, Specifications for the Secure Hash Standard (SHS), February 2004

[ICAOPKI]

Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[ICAOLDS]

Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7,

published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

[ISO15946]

ISO 15946, Information technology – Security techniques – Cryptographic techniques based on elliptic curves, 2002ff

[ISO7816]

ISO 7816-4:2005, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, 2005-01-05

[PP0002]

Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0002

[TCOSADM]

Administrator Handbuch TCOS Passport Version 2.0 Release 1.1, T-Systems International GmbH, March 2008