T · · Systems

Specification of the Security Target TCOS Passport Version 2.0

Release 2/SLE66CLX800PE

Basic Access Control

Version: 2.0.2.e13

Dokumentenkennung:	CD.TCOS.ASE
Dateiname:	TCOS Passport Version 2.0 Release 2_BAC SLE66CLX800PEe13.doc
Stand:	16.07.2008
Version:	2.0.2.e13
Autor:	Ernst-G. Giessmann
Geltungsbereich:	TeleSec Entwicklungsgruppe
Vertraulichkeitsstufe:	**Öffentlich**

History

Version	Date	Remark
1.01	2005-10-27	Final Version
1.02	2005-12-02	Release update according to hardware updates
1.03	2006-07-11	Release update according to hardware updates, CertID checked
2.0.2	2008-01-22	Final Public Version 2.0 Release 2 BAC
2.0.2.e13	2008-07-16	Maintenance of the hardware platform

Contents

Abbreviations

ATS	Answer To Select
CC	Common Criteria Version
MRTD	Machine readable travel document

The Terminology follows the Protection Profile [MRTDPP].

1 ST Introduction

1.1 ST Identification

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

Title: Specification of the Security Target TCOS Passport Version 2.0 Release 2/SLE66CLX800PE Basic Access Control

Date: 16.07.2008

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

Certification ID: BSI-DSZ-CC-0507

TOE: TCOS Passport Version 2.0 Release 2/SLE66CLX800PE.

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 according to ICAO document [ICAOPKI] based on an Infineon chip SLE66CLX800PE and the TCOS operating system. The version of the operating systems follows the TOE identification. The TOE is supplied with a file system, that contains all the data that is used in the context of the ICAO application as described in [MRTDPP].

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 Release 2/SLE66CLX800PE" otherwise the notion "TCOS Passport version 2.0 Release 2" 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 MRTD [MRTDPP].

The evaluation assurance level of the TOE is EAL4 augmented with ADV_IMP.2 and ALC_DVS.2 as stated in [MRTDPP]

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) [LDS] and providing the Basic Access Control according to ICAO document [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 application.

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

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 [MRTDPP] 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.

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 disable the Basic Access Control provided by the TOE, it may be appropriate to use a pre-configured TOE with zero-allocated memory for the unnecessary data groups and a fixed non-visibility for the corresponding EFs. For this version of the TOE three pre-configured versions of the file system apply:

(FSV04) In this configuration of the TOE in the dedicated file of the ICAO application only the files EF.DG1, EF.DG2, EF.SOD, EF.COM and EF.GDO are visible and empty. Its maximal available memory is already allocated. The access rules allow access without restrictions. Other EFs are not visible and can not be initialized during Personalization.

(FSV05) In this configuration EF.DG1, EF.COM and EF.KEY1 are already initialized and its memory is assigned too. EFs corresponding to data groups, which are not neccessary for the BAC protocol are not visible and can not be initialized any more. Other data's initialization must be done during Personalization, and the access to these data groups is granted only after successful BAC authentication.

(FSV03) EF.DG1, EF.COM and EF.KEY1 are already initialized and its memory is assigned too. But in contrast to the configuration (FSV05) additional data groups remain non-initialized and must be deallocated during Personalization.

The latter is the most flexible version and can be used for a BAC and EAC implementation, but the Personalization of the TOE is in this case more time consuming. A detailed description of the sub-phases and the file system pre-configurations, including

the assigned maximal available memory sizes 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 (DG1), (ii) the digitized portrait (DG2), and (iii) the Document security object.

The signing of the Document security object by the Document signer [ICAOPKI]] finalizes the personalization of the genuine MRTD for the MRTD holder. 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 [MRTDPP]. 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 of 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

Assets are the elements of the TOE to be protected.

Logical MRTD Data

The logical MRTD data consists of the data groups DG1 to DG16 and the Document security object according to LDS [ICAOLDS]. These data are user data of the TOE. The data groups DG1 to DG14 and DG 16 contain personal data of the MRTD holder. The Active Authentication Public Key Info in DG 15 (if available at all) is used by the inspection system for Active Authentication of the chip. The Document security object is used by the inspection system for Passive Authentication of the logical MRTD.

An additional 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 authenticate himself as possessing a genuine MRTD.

Assets have to be protected in terms of confidentiality and/or integrity.

3.1 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 Active Authentication Public Key Info (DG15) if stored on the MRTD's chip, and

(iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip) on the MRTD's chip.

Application note: Because the Active Authentication Public Key Info (DG15) is not stored on the TOE, this assumption from the Protection Profile [MRTDPP] is not relevant.

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

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 Primary Inspection System for global interoperability contains the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization [ICAOPKI]. The Primary Inspection System performs the Passive Authentication to verify the logical MRTD if the logical MRTD is not protected by Basic Access Control. The Basic Inspection System in addition to the Primary Inspection System implements the terminal part of the Basic Access Control and reads the logical MRTD being under Basic access Control.

3.2 Subjects

The Protection Profile [MRTDPP] 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.

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.

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].

Inspection System

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.

The Primary Inspection System (PIS)

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

(ii) does not implement the terminals part of the Basic Access Control Mechanism. The Primary Inspection System can read the logical MRTD only if the Basic Access Control is disabled.

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 printed data in the MRZ or other parts of the passport book providing this information.

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

(i) implements the Active Authentication Mechanism,

(ii) supports the terminals part of the Extended Access Control Authentication Mechanism and

(iii) is authorized by the issuing State or Organization to read the optional biometric reference data.

Terminal

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

Attacker

A threat agent trying

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

(ii) to read or to manipulate the logical MRTD without authorization, or
(iii) to forge a genuine MRTD.

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 and does not know in advance the MRZ data printed on the MRTD data page.

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 can not read and does not know in advance the MRZ data printed on the MRTD data page.

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

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

Note in case of **T.Skimming** the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data printed on the MRTD data page and without a help of the inspection system which knows these data. In case of **T.Eavesdropping** the attacker uses the communication of the inspection system.

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.

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
to disclose TSF Data,
(i) 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 misuse of administration function. To exploit this an attacker needs information about the functional operation.

3.4 Organizational Security Policies

The TOE shall comply to the following organization security policies 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 (DG1), the printed portrait and the digitized portrait (DG2), the biometric reference data of finger(s) (DG3), the biometric reference data of iris image(s) (DG4) and data according to LDS (DG5 to DG14, DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAOPKI]. The issuing State or Organization decides (i) to enable the Basic Access Control for the protection of the MRTD holder personal data or (ii) to disable the Basic Access Control to allow Primary Inspection Systems of the receiving States and all other terminals to read the logical MRTD.

4 Security Objectives

4.1 Security Objectives for the TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data groups DG1 to DG16, the Document security object according to LDS [ICAOLDS] and the TSF data can be written by authorized Personalization Agents. The logical MRTD data groups DG1 to DG16 and the TSF data can be written only once and can not be changed after personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups DG 3 to DG16 are added. Only the Personalization Agent shall be allowed to enable or to disable the TSF Basic Access Control.

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. If the TOE is configured for the use with Basic Inspection Terminals only the TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

OT.Data_Conf Confidentiality of personal data

If the TOE is configured for the use with Basic Inspection Systems the TOE must ensure the confidentiality of the logical MRTD data groups DG1 to DG16 by granting read access to terminals successfully authenticated by (i) as Personalization Agent or as (ii) Basic Inspection System. The Basic Inspection System shall authenticate themselves by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

If the TOE is configured for the use with Primary Inspection Systems no protection in confidentiality of the logical MRTD is required.

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". If the TOE is configured for use with Basic Inspection Terminals only in Phase 4 "Operational Use" the TOE shall identify themselves only to a successful authenticated Basic Inspection System or Personalization Agent.

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

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

OT.Prot_Inf_Leak Protection against Information Leakage

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

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

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

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

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

OT.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.

4.2 Security Objectives for the Environment

Security Objectives are separated for the Development and Manufacturing Environment and an Operational Environment

Development and Manufacturing

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 low attack potential and against direct attacks with high attack potential against security function that uses probabilistic or permutational mechanisms.

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.

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 (including the digital signature in the Document Security Object).

The Personalization Agents enable or disable the Basic Access Control function of the TOE according to the decision of the Issuing State or Organization. If the Basic Access Control function is enabled the Personalization Agents generate the Document Basic Access Keys and store them in the MRTD's chip.

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 includes all data in the data groups DG1 to DG16 if stored in the LDS according to [ICAOLDS].

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.

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 MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and organizations must manage the Country Signing Public Key and the Document 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 ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems). The receiving State examining the logical MRTD with Primary Inspection Systems will prevent eavesdropping to the communication between TOE and inspection system.

MRTD Holder

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

OE.Secure_Handling Secure handling of the MRTD by MRTD holder

The holder of a MRTD configured for use with Primary Inspection Systems (i.e. MTRD with disabled Basic Access Control) will prevent unauthorized communication of the MRTD's chip with terminals through the contactless interface.

5 IT Security Requirements

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

5.1 TOE Security Functional Requirements for the TOE

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

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 [MRTDPP] 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/BAC_MRTD Cryptographic key generation – Generation of Document Basic Access Keys by the TOE

Hierarchical to: No other components.

FCS_CKM.1.1/ BAC_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 message authentication keys for secure messaging by the algorithm in [ICAOPKI], Annex E.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1/MRTD.

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 the new key*[6] that meets the following: *none*[7].

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

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

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

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

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

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 shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging after closing the secure channel or power-off.

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 [8] in accordance with a specified cryptographic algorithm SHA-1 [9] and cryptographic key sizes none [10] that meet the following: FIPS 180-2 [11].

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/TDES_MRTD Cryptographic operation – Encryption / Decryption Triple DES

Hierarchical to: No other components.

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

[9] [assignment: *cryptographic algorithm*]

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

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

FCS_COP.1.1/ TDES_MRTD	The TSF shall perform secure messaging – encryption and decryption [12] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode [13] and cryptographic key sizes 112 bit [14] that meet the following: FIPS 46-3 [FIPS46] and [ICAOPKI]; Annex E [15].

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_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 [16] in accordance with a specified cryptographic algorithm Retail MAC [17] and cryptographic key sizes 112 bit [18] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [19].

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

5.1.2.2 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

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

[13] [assignment: *cryptographic algorithm*]

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

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

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

[17] [assignment: *cryptographic algorithm*]

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

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

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]*[20].

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]
Basic Access Control Authentication Mechanism	FIA_UAU.4/MRTD and FIA_UAU.6/MRTD	FIA_UAU.4/BAC_T and FIA_UAU.6/T	Triple-DES, 112 bit keys and Retail-MAC, 112 bit keys
Symmetric Authentication Mechanism for Personaliza-tion Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys

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.

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

FIA_UID.1.1	The TSF shall allow (1) to read the Initialization Data in Phase 2 “Manufacturing”, (2) to read the ATS in Phase 3 “Personalization of the MRTD”, (3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”, (4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 “Operational Use” [21] 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.

The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”, this is described in more detail in the Administrator Guidance for TCOS Passport. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. If the TOE is configured for use with Primary Inspection Systems any terminal is assumed as Primary Inspection System and is allowed to read the logical MRTD. If the TOE is configured for use with Basic Inspection Systems only 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 according to the SFR FIA_UAU.4/T.

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 before the ATS is sent, therefore the **OT.Identification** is not violated here.

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

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 read the Initialization Data in Phase 2 “Manufacturing”, (2) to read the ATS in Phase 3 “Personalization of the MRTD”, (3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 “Operational Use”, (4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 “Operational Use” [22] 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. Authentication Mechanism based on Triple-DES [23].

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

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

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 TOE stops the communication with the terminal not successfully authenticated in the first step of the protocol to fulfill 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. Symmetric Authentication Mechanism based on Triple-DES [24]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:
1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms
   (a) the Basic Access Control Authentication Mechanism with the Personalization Agent Keys,
   (b) the Symmetric Authentication Mechanism with the Personalization Agent Key
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 [25].

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.

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

[25] [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 each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism [26].

Dependencies: No dependencies.

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 by means of BAC user.

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). The instantiations of FDP_ACC.1 are caused by the TSF management according to FMT_MOF.1.

FDP_ACC.1 Subset access control – Primary Access Control

Hierarchical to: No other components.

FDP_ACC.1.1/PRIM	The TSF shall enforce the Primary Access Control SFP [27] on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD [28].

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

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

Dependencies: FDP_ACF.1 Security attribute based access control

The data groups DG1 to DG16 of the logical MRTD as defined in [ICAOLDS] are the only TOE User data.

FDP_ACC.1 Subset access control – Basic Access control

Hierarchical to: No other components.

FDP_ACC.1.1/BASIC	The TSF shall enforce the Basic Access Control SFP [29] on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD [30].

Dependencies: FDP_ACF.1 Security attribute based access control

The Basic Access Control SFP addresses the configuration of the TOE for usage with Basic Inspection Systems only.

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). The instantiations of FDP_ACC.1 address different SFP.

FDP_ACF.1 Security attribute based access control – Primary Access Control

Hierarchical to: No other components.

FDP_ACF.1.1/PRIM	The TSF shall enforce the Primary Access Control SFP[31] to objects based on the following: 1. Subjects: a. Personalization Agent, b. Terminals, 2. Objects: data into the data groups DG1 to DG16 of the logical MRTD, 3. security attributes a. configuration of the TOE according to FMT_MOF.1 b. authentication status of terminals [32].

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

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

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

FDP_ACF.1.2/PRIM	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: in the TOE configuration for use with Primary Inspection Systems 1. the successfully authenticated Personalization Agent is allowed to write the data of the data groups DG1 to DG16 of the logical MRTD, 2. the Terminals are allowed to read the data of the groups DG1 to DG16 of the logical MRTD[33].
FDP_ACF.1.3/PRIM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[34].
FDP_ACF.1.4/PRIM	The TSF shall explicitly deny access of subjects to objects based on the rule: the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD[35].

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

The MRTD access control prevents changes of data groups by write access to the logical MRTD after their creation by the Personalization Agent (i.e. no update of successfully written data in the data groups DG1 to DG16). The Passive Authentication Mechanism detects any unauthorized changes.

FDP_ACF.1 Basic security attribute based access control – Basic Access Control

Hierarchical to: No other components.

FDP_ACF.1.1/BASIC	The TSF shall enforce the Basic Access Control SFP[36] to objects based on the following: 1. Subjects: a. Personalization Agent b. Basic Inspection System c. Terminal 2. Objects: data in the data groups DG1 to DG16 of the logical MRTD 3. Security attributes a. configuration of the TOE according to FMT_MOF.1 b. authentication status of terminals [37].

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

[32] [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*]

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

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

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

FDP_ACF.1.2/BASIC	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: in the TOE configuration for use with Basic Inspection Systems only 1. the successfully authenticated Personalization Agent is allowed to write data and to read data of the data groups DG1 to DG16 of the logical MRTD, 2. the successfully authenticated Basic Inspection System is allowed to read data of the groups DG1 to DG16 of the logical MRTD[38].
FDP_ACF.1.3/BASIC	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[39].
FDP_ACF.1.4/BASIC	The TSF shall explicitly deny access of subjects to objects based on the rule: Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD[40].

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

5.1.4.3 Inter-TSF-Transfer

FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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.

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

[37] [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*]

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

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

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

FDP_UCT.1.1/MRTD	The TSF shall enforce the Basic Access Control SFP[41] to be able to transmit and receive[42] objects in a manner protected from unauthorized disclosure.

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.

FDP_UIT.1.1/MRTD	The TSF shall enforce the Basic Access Control SFP [43] to be able to transmit and receive [44] user data in a manner protected from modification, deletion, insertion and replay [45] errors.
FDP_UIT.1.2/MRTD	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [46] has occurred.

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]

5.1.5 Class FMT Security Management

The TOE shall meet the requirement "Management of functions in TSF (FMT_MOF.1)" as specified below (Common Criteria Part 2).

FMT_MOF.1 Management of functions in TSF

Hierarchical to: No other components.

FMT_MOF.1.1	The TSF shall restrict the ability to enable and disable [47] the functions TSF Basic Access Control [48] to Personalization Agent[49].

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

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

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

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

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

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

Dependencies: No Dependencies

The Basic Access Control Authentication Mechanism is available even if the TOE is configured for use in the phase 4 “Operational Use” with Primary Inspection systems only. The Personalization Agent may use this mechanism with the Personalization Agent Authentication Keys.

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 [50].

Dependencies: No Dependencies

Application Note: Because the Initialization Data is written already before the TOE is ready made, we consider as management functions in the following the Personalization and Configuration 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. Primary Inspection System, 4. Basic Inspection System [51].

[47] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[48] [assignment: *list of functions*]

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

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

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

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Hierarchical to: FIA_UID.1 Timing of identification.

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 [MRTDPP] chapter 4.

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 capabilities (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[52].

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 [MRTDPP] 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[53].

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

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

Dependencies: FMT_LIM.1 Limited capabilities.

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

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

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

Hierarchical to: No other components.

FMT_MTD.1/INI_ENA	The TSF shall restrict the ability to write [54] the Initialization Data and Pre-personalization Data [55] to the Manufacturer[56].

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.

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 [57] the Initialization Data [58] to the Personalization Agent[59].

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

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

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

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

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

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

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.

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 [60] the Document Basic Access Keys [61] to the Personalization Agent[62].

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

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 [63] the Document Basic Access Keys and Personalization Agent keys [64] to none[65].

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

The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys if the Basic Access Control is enabled.

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

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

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

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

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

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

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 [MRTDPP] 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*[66] in excess of *non-useful information*[67] enabling access to Personalization Agent Authentication Key [68] and *none*[69].
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users [70] are unable to use the following interface smart card circuit contacts [71] to gain access to Personalization Agent Authentication Key [72] and *none*[73].

Dependencies: No other components.

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

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

[67] [assignment: *specified limits*]

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

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

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

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

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

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

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[74].

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*[75] to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of 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 Infineon chip SLE66CLX800PE 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).

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

[75] [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_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing [76] to the TSF [77] 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.

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.

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

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

Dependencies: No dependencies.

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 and ALC_DVS.2

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

The minimum strength of function is SOF-high.

This protection profile does not contain any security functional requirement for which an explicit stated strength of function claim is required.

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 (DG1 to DG16) and the Document Security Object[78].
FDP_DAU.1.2/DS	The **Document Signer** shall provide Inspection Systems of Receiving States or Organization[79] with the ability to verify evidence of the validity of the indicated information.

There are no other SFR for Passive Authentication for the Environment, because this verification does not require processing capabilities of the chip and any reaction of the MRTD. Passive authentication proves only that the contents of the Document Security Object (SOD) and LDS are authentic and not changed.

In contrast to that there are some SFRs for Basic Inspection Systems listed in the following. Without these requirements, e.g. if the Inspection Systems uses a weak key, data that must be protected against disclosure becomes accessible for an attacker. The MRTD must rely on that the following SFRs are met.

5.3.2 Basic Inspection Systems

This section describes common security functional requirements to the Basic Inspection Systems and the Personalization Agent if it uses the Basic Access Control Me-

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

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

chanism 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/BAC_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 [80] and specified cryptographic key sizes 112 bit [81] that meet the following: [ICAOPKI], Annex E[82].

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

The terminals derive 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.

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*[83] that meets the following:*none*[84].

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

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

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

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

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

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.

FCS_COP.1.1/ SHA_BT	The **Basic Terminal** shall perform hashing[85] in accordance with a specified cryptographic algorithms SHA-1 [86] and cryptographic key sizes none [87] that meet the following: FIPS 180-2[88].

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[89] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[90] and cryptographic key sizes 112 bit[91] that meet the following: FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)[92].

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

[86] [assignment: *cryptographic algorithm*]

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

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

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

[90] [assignment: *cryptographic algorithm*]

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

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

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.

FCS_COP.1.1/ MAC_BT	The **Basic Terminal** shall perform secure messaging – message authentication code[93] in accordance with a specified cryptographic algorithm Retail-MAC[94] and cryptographic key sizes 112 bit[95] that meet the following: FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)[96].

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 [MRTDPP] 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}[97].

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

[94] [assignment: *cryptographic algorithm*]

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

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

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

Dependencies: No dependencies.

This quality metric ensures the strength of function Basic Access Control Authentication for the challenges. The Terminal shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

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

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

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[98].

Dependencies: No dependencies.

The Basic Access Control Authentication Mechanism [ICAOPKI] uses a challenge RND.IFD freshly and 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[99].

Dependencies: No dependencies.

The authentication fails if any response is received with incorrect message authentication code.

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

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

The Basic Access Control SFP of the TOE requires to protect the User Data by access control (cf. FDP_ACC.1/BASIC and FDP.1/BASIC) and by secure messaging (cf. FDP_UCT.1/MRTD and FDP_UIT.1/MRTD) for the communication between the TOE and the Basic Terminal. This secure messaging requires the Basic Terminal to support the protection of the TOE data by decryption and checking MAC and to protect its own data by secure messaging as well. The SFP of the Basic Terminal drawn from the TOE "Basic Access Control SFP" is named "BT part of Basic Access Control SFP" and the related SFR is described by FDP_UCT.1/BT and FDP_UIT.1/BT corresponding to FDP_UCT.1/MRTD and FDP_UIT.1/MRTD of the communication partner (i.e. the TOE). Note the Basic Terminal does not enforce any named access control policy or information control policy to be defined by FDP_ACC and FDP_ACF or FDP_IFC and FDP_IFF families (respectively). The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

FDP_UCT.1/BT Basic data exchange confidentiality - Basic Terminal

Hierarchical to: No other components.

FDP_UCT.1.1/BT	The **Basic Terminal** shall enforce the BT part of Basic Access Control SFP[100] to be able to transmit and receive[101] objects in a manner protected from unauthorized disclosure.
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 Terminal shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

FDP_UIT.1/BT Data exchange integrity - Basic Terminal

Hierarchical to: No other components.

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

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

FDP_UIT.1.1/BT	The **Basic Terminal** shall enforce the BT part of Basic Access Control SFP[102] to be able to transmit and receive[103] user data in a manner protected from modification, deletion, insertion and replay[104] errors.
FDP_UIT.1.2/BT	The **Basic Terminal** shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [105] has occurred.

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]

5.3.3 Personalization Terminals

The TOE supports different authentication and access control mechanisms which may be use 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 Agent 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 listen or manipulated.

(2) 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 protocol 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 (cf. [MRTDPP]).

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

Hierarchical to: No other components.

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

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

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

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

FIA_API.1.1/ SYM_PT	The **Personalization Terminal** shall provide an Authentication Mechanism based on Triple-DES [106] to prove the identity of the Personalization Agent[107].

Dependencies: No dependencies.

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

Dependencies ADV_IMP.2

ADV_LLD.1 Descriptive low-level design

ALC_TAT.1 Well-defined development tools

[106] [assignment: *authentication mechanism*]

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

Dependencies ALC_DVS.2: no.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 SF_HA: Identification and Authentication based on Challenge-Response

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

SF_HA uses a mutual authentication mechanism that is based on a Challenge-Response-Protocol, which makes use of random numbers during the authentication process. The challenge contains the random number and will be send 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.

SF_HA 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.

In case of regular termination of the protocol both parties possess authentic key material known only by them.

The ability for writing of Initialization Data and Pre-personalization Data is restricted to the successful authenticated Manufacturer (FMT_MTD.1/INI_ENA). During personalization only the Personalization Agent is allowed to disable the read access to Initialization Data (FMT_MTD.1/INI_DIS).

The SOF claimed for SF_HA is high.

6.1.2 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 SOF claimed for SF_SM is high.

6.1.3 SF_AC: Access Control of stored data objects

SF_AC enforces the Security Policies as required in FDP_ACF.1.

It 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 by the defined during initialization access conditions.

This SF controls the reading and writing access in different phases of the production and during end-usage.

The Document Basic Access Keys will be computed and written during Personalization. The SF_AC restricts the ability to write the keys to the Personalization Agent only, and does not allow any read access to these key data (FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ).

6.1.4 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.

The TOE's chip SLE66CLX680PE provides:

SEF1: Operating state checking

SEF2: Phase management with test mode lock-out

SEF3: Protection against snooping

SEF4: Data encryption and data disguising

SEF5: Random number generation

SEF6: TSF self test

SEF7: Notification of physical attack

SEF8: Memory Management Unit (MMU)

SEF9: Cryptographic support

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.

SF_RE 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 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. An 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).

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 SW-part of FPT_PHP.3.

Note that this functionality is partially implemented by the underlying hardware, cf. [CR].

The TOE ensures that the content of temporarily allocated resources is made unavailable after de-allocation by overwriting this content with zeros.

6.1.5 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 P1 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:

SF_HA 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.

SF_SM 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.

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.2: Validation of analysis

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

AVA_VLA.2: 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 Enterprice Sevices 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 [MRTDPP] “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 is 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.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Malfuntion	OD.Assurance	OD.Material	OE.Personalization	OE.Pass_Auth_Sign	OE.Exam_MRTD	OE.pass_Auth_verif	OE.Prot_Logical_MRTD	OE.Secure_Handling
T.Chip-ID				x												x
T.Skimming			x	x												x
T.Eavesdropping			x	x												
T.Forgery	x	x					x					x	x	x		
T.Abuse-Func					x				x	x	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													
A.Pers_Agent											x					
A.Insp_Sys													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.

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 (enabling and disabling of the TSF Basic Access Control) to the Personalization Agent.

The OSP **P.Personal_Data** "Personal data protection policy" requires the TOE (i) to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives OT.Data_Int "Integrity of personal data" which describes the unconditional protection of the integrity of the stored data and the configurable integrity protection during the transmission. The security objective OT.Data_Conf "Confidentiality of personal data" describes the protection of the confidentiality as configured by the Personalization Agent acting in charge of the issuing State or Organization.

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. In case of TOE configuration for use with Basic Inspection Terminals only this threat is countered as described by the security objective OT.Identification by Basic Access Control. If the TOE is configured for use with Primary Inspection Systems this threat shall be adverted by the TOE environment as described by OE.Secure_Handling.

The threat **T.Skimming** "Skimming digital MRZ data or the digital portrait" and **T.Eavesdropping** *"*Eavesdropping to the communication between TOE and inspection system" address the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD's chip and a terminal. In case of TOE configuration for use with Basic Inspection Terminals only this threat is countered by the security objective OT.Identification through Basic Access Control. If the TOE is configured for use with Primary Inspection Systems the threat T.Skimming shall be adverted by the TOE environment according to **OE.Secure_Handling** "Secure handling of the MRTD by MRTD holder" and the threat T.Eavesdropping shall be adverted by **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD".

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 an additional contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** **“**Authentication of logical MRTD by Signature” and verified by the inspection system according to **OE.Passive_Auth_Verif** “Verification by Passive Authentication”.

The threat **T.Abuse-Func** “Abuse of Functionality” addresses attacks using the MRTD’s chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. The security objectives for the TOE environment **OD.Material** “Control over MRTD Material” ensures the control of the MRTD material. The security objectives for the TOE environment **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment” and **OE.Personalization** “Personalization of logical MRTD” ensure that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

The threats **T.Information_Leakage** “Information Leakage from MRTD’s chip”, **T.Phys-Tamper** “Physical Tampering” and **T.Malfunction** “Malfunction due to Environmental Stress” are typical for integrated circuits like smart cards under direct attack with high 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”. If the Issuing State of Organization decides to protect confidentiality of the logical MRTD than the security objectives for the TOE environment **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD” will require the Basic

Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling. If the Issuing State of Organization decides to configure the TOE for use with Primary Inspection Systems than no protection of the logical MRTD data is required by the inspection system.

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.Identification	OT:Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Malfuntion	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1/BAC_MRTD	(x)	x	(x)					
FCS_CKM.4	(x)		x					
FCS_COP.1/SHA_MRTD	x	x	(x)					
FCS_COP.1/TDES_MRTD	x	x	x					
FCS_COP.1/MAC_MRTD	x	x	x					
FCS_RND.1/MRTD	(x)	x	x					
FIA_UID.1			x	x				
FIA_UAU.1			x					
FIA_UAU.4/MRTD	x	x	x					
FIA_UAU.5/MRTD	x	x	x					
FIA_UAU.6/MRTD	x	x	x					
FDP_ACC.1/PRIM	x	x						
FDP_ACF.1/PRIM	x	x						
FDP_ACC.1/BASIC	x	x	x					
FDP_ACF.1/BASIC	x	x	x					
FDP_UCT.1/MRTD	x	x	x					
FDP_UIT.1/MRTD	x	x	x					
FMT_MOF.1	x	x	x					
FMT_SMF.1	x	x	x					
FMT_SMR.1	x	x	x					
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA				x				
FMT_MTD.1/INI_DIS				x				
FMT_MTD.1/KEY_WRITE	x	x	x					
FMT_MTD.1/KEY_READ	x	x	x					
FPT_EMSEC.1	x				x			
FPT_TST.1					x		x	
FPT_RVM.1								x
FPT_FLS.1	x				x		x	
FPT_PHP.3	x				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” address 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 FDP_ACC.1/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/PRIM and FDP_ACF.1/BASIC in the same way: only the successfully authenticated Personalization Agent is allowed to write data the data of the groups DG1 to DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD and FIA_UAU.5/MRTD. In case the Basic Access Control Authentication Mechanism was used the SFR FIA_UAU.6/MRTD describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/BAC_MRTD, FCS_COP.1/SHA_MRTD, FCS_RND.1 (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode. The personalization data can be written only once and the session keys assigned to the personalization session can not be used twice. Therefore after personalization a secure deletion according to FCS_CKM.4 is not necessary.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) because the Personalization Agent handles the configuration of the TSF Basic Access according to the SFR FMT_MOF.1 and the Document Basic Access Control Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data if Basic Access Control is enabled. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 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/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/PRIM and FDP_ACF.1/BASIC in the same way: only the Personalization Agent is allowed to write data the data of the groups DG1 to DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization)

If the TOE is configured for the use with Basic Inspection Terminals only by means of FMT_MOF.1 the security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to ensure that the inspection system is able to detect any modification of the

transmitted logical MRTD data. 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, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/ BAC_MRTD, FCS_COP.1/SHA_MRD, FCS_RND.1 (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/ MAC_MRTD for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY requires the Personalization Agent to establish the Document Basic Access Keys.

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups DG1 to DG16 if the TOE is configured for the use with Basic Inspection Systems by means of FMT_MOF.1. 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/BASIC and FDP_ACF.1.2/BASIC: only the successful authenticated Personalization Agent and the successful authenticated Basic Inspection System are allowed to read the data of the logical MRTD by means of SFR FIA_UID.1, FIA_UAU.1, FIA_UAU.4/MRTD, where the session key for data encryption is established. The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

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

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

secure messaging. If the TOE is configured for the use with Primary Inspection Systems no protection in confidentiality of the logical MRTD is needed to ensure.

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 ensure by TSF according to SFR FAU_SAS.1.

Furthermore, if the TOE is configured for use with Basic Inspection Terminals the TOE shall identify themselves 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.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 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. It does not state any SFR for the IT environment supporting the security objectives OD.Assurance and OD.Material. The OE.Exam_MRTD uses only security function of the IT environment, i.e. the passive authentication. The security objective OE.Prot_Logical_MRTD is directed to Basic Inspection Systems only which cooperate with the TOE in protection of the logical MRTD.

	OD.Assurance	OD.Material	OE.Personalization	OE.Pass_Auth_Sign	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
Document Signer							
FDP_DAU.1/DS				x	x	x	
Terminal							
FCS_CKM.1/BAC_BT			x				x
FCS_CKM.4/BT							x
FCS_COP.1/SHA_BT			x				x
FCS_COP.1/ENC_BT			x				x
FCS_COP.1/MAC_BT			x				x
FCS_RND.1/BT			x				x
FIA_UAU.4/BT			x				x
FIA_UAU.6/BT			x				x
FDP_UCT.1/BT			x				x
FDP_UIT.1/BT			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 document signer provides the security function Passive Authentication according to FDP_DAU.1/DS to support the inspection system to verify the logical MRTD, this is related to **OE.Pass_Auth_Sign** and **OE.Pass_Auth_Verif**.

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 and FIA_UAU.6/BT address the terminal part of the Basic Access Control Authentication Mechanism and FDP_UCT.1/BT and FDP_UIT.1/BT the secure messaging established by this mechanism. The SFR FCS_CKM.1/BAC_BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT and FCS_RND.1/BT are necessary to implement this mechanism. The BIS shall destroy the Document Access Control Key and the secure messaging key after inspection of the MRTD because they are not needed any more, this implements FCS_CKM.4/BT.

The **OE.Personalization** “Personalization of logical MRTD” requires the personalization terminal to authenticate themselves to the MRTD’s chip to get the write authorization. This implies to implement the Basic Access Control Authentication Mechanism with the Personalization Agent Authentication Keys or support the symmetric authentication protocol according to the SFR FIA_API.1/SYM_PT.

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/BAC_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.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

SFR	Dependencies	Support of the 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 2 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 3 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 3 for non-satisfied dependencies
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.
FDP_ACC.1/PRIM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/PRIM
FDP_ACC.1/BASIC	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/BASIC
FDP_ACF.1/PRIM	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.1/PRIM, justification 4 for non-satisfied dependencies
FDP_ACF.1/BASIC	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.1/BASIC, justification 4 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/BASIC, justification 5 for non-satisfied dependencies

SFR	Dependencies	Support of the 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/BASIC, justification 5 for non-satisfied dependencies
FMT_MOF.1	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
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
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/KEY_WRITE	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
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 6 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/BAC_MRTD uses only the Document Basic Access Keys to generate the secure messaging keys used for FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD. 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 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. 3: 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. 4: 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. 5: 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 additional 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. 6: 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.
FCS_CKM.1/BAC_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/TENC_BT, FCS_COP.1/MAC_BT justification 7 for non-satisfied dependencies
FCS_CKM.4/BT	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes	FCS_CKM.1, justification 7 for non-satisfied dependencies
FCS_COP.1/SHA_BT	[FDP_ITC.1 Import of user data without 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 8 for non-satisfied dependencies
FCS_COP.1/ENC_BT	[FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction,	FCS_CKM.1, FCS_CKM.4, justification 9 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	FMT_MSA.2 Secure security attributes	
FCS_COP.1/MAC_BT	[FDP_ITC.1 Import of user data without 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 9 for non-satisfied dependencies
FCS_RND.1/BT	No dependencies	n.a.
FIA_UAU.4/BT	No dependencies	n.a.
FIA_UAU.6/BT	No dependencies	n.a.
FDP_UCT.1/BT	[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/BASIC, justification 10 for non-satisfied dependencies
FDP_UIT.1/BT	[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/BASIC, justification 10 for non-satisfied dependencies
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. 7: The SFR FCS_CKM.1/BT derives the Document Basic Access Keys and uses this key to generate the secure messaging keys used for FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD. The SFR FCS_CKM.4/BT destroys these keys. These processes do not need any special security attributes for the secure messaging keys.

No. 8: 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. 9: The SFR FCS_COP.1/ENC_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. 10: 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 to provide further description of this communication.

8.4 Evaluation Assurance Level Rationale

The assurance level for the TOE is EAL4 augmented with components ADV_IMP.2 and ALC_DVS.2. EAL4 is appropriate for commercial products that can be applied to moderate up to high security functions. The TOE described in this ST is just such a product.

Augmentation results from the selection of:

- **ADV_IMP.2** Implementation of the TSF
- **ALC_DVS.2** Sufficiency of security measures

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.

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.2	EAL 4
AVA_SOF.1	EAL 4
AVA_VLA.2	EAL 4

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_HA**	**SF_SM**	**SF_AC**	**SF_RE**	**SF_RN**
FAU_SAS.1	**x**				
FCS_CKM.1		**x**			
FCS_CKM.4	**x**				
FCS_COP.1		**x**			
FCS_RND.1					**x**
FIA_UID.1	**x**				
FIA_UAU.1	**x**				
FIA_UAU.4	**x**				
FIA_UAU.5	**x**				
FIA_UAU.6		**x**			
FDP_ACC.1			**x**		
FDP_ACF.1			**x**		

FDP_UCT.1			x		
FDP_UIT.1			x		
FMT_MOF.1			x		
FMT_SMF.1			x		
FMT_SMR.1			x		
FMT_LIM.1				x	
FMT_LIM.2				x	
FMT_MTD.1	x		x		
FPT_EMSEC.1				x	
FPT_FLS.1				x	
FPT_TST.1				x	
FPT_PHP.3				x	
FPT_RVM.1			x		
FPT_SEP.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 requirement 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 Manufacturer is successfully authenticated (SF_HA), which allows the Manufacturer to store this data in audit records..

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

FIA_UAU.1: After successful authentication provided by SF_HA a security status is maintained. Based on that status the access rules apply that allow or disallow the execution of commands.

FIA_UAU.4, The data used after authentication in SF_HA is generated based on a randomly chosen challenge of 8 Bytes or a secret key of 112 Bit each time the authentication is started again, therefore a re-use of old data is not possible.

FIA_UAU.5: The authentication of a Personalization Agent and a Inspection System both use SF_HA, nethertheless they represent different roles controlled by SF_AC. A Basic Inspection System is not allowed to authenticate itself by other means than the Basic Access Control Mechanism.

FIA_UID.1: The identification data used by SF_HA is maintained by the TOE and can not be changed. The access rules prevent the use of other commands for non identified users.

FMT_MTD.1: The write access in the Initialization and Pre-Personalization phases is based on a command that uses the SF_HA authentication for the Manufacturer. It can be used in these phases only and is disabled later..

FCS_CKM.1, FCS_COP.1: The secure messaging mechanism used by SF_SM implements these requirements, the keys are generated according to [ICAOPKI].

FCS_RND.1: The randomness of challenges used in SF_HA will be provided by SF_RN. 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 P1 according [AIS31].

FIA_UAU.6: SF_SM guarantees based on the secure messaging mechanism that the reauthentication of the user is possible for every command after successful authentic-cation.

FDP_ACC.1, FDP_ACF.1, FDP_UCT.1: The access control is enforced by SF_AC based on defined rules that can not be changed or disabled.

FDP_UIT.1: The data integrity is enforced implicitly by the access control mechanism of SF_AC, because only integrity checked security data can be accessed.

FMT_MOF.1: The access control is enforced by SF_AC based on defined rules that can not be changed or disabled, and these rules restrict the ability to enable or disable the Basic Access Control to Personalization Agents.

FMT_SMF.1, FMT_SMR.1, FPT_RVM.1: Maintaining different roles and different func-tions uses the defined access control rules rules that can not be changed or disabled. The assignment of a specific role is supported by an authentication based on SF_HA and/ or SF_SM.

FMT_LIM.1, FMT_LIM.2: Limitations of capabilities or availability are enforced by SF_RE controlling the integrity of the stored access rules and the used functions.

FPT_EMSEC.1: SF_RE monitors the regular execution of commands, and if variations occur with test failures or integrity mismatch the communication is closed. The Perso-nalization Agent Authentication Key is protected by access rules of SF 5 that can not be changed.

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

FPT_PHP.3: SF_RE 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: Because of monitoring the integrity of access control rules by SF_RE the domain separation in the TOE is enforced.

FPT_TST.1: The self-tests of the underlying hardware and additional test maintained by SF_RE 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 [MRTDPP]. 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.

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

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

9 References

[AIS36]
Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), Version 1 vom 29.07.2002, BSI

[BSI]
Dennis Kügler, Advanced Security Mechanisms for Machine Readable Travel Documents, version 0.8, BSI

[CR]
Certification Reports of underlying hardware
BSI-DSZ-CC-0482-2007 for SLE66CLX800PE/e13

[FIPS46]
Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. DoC/NIST

[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

[ISO7816]
ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004

[MRTDPP]
Protection Profile Machine Readable Travel Document with “ICAO Application", Version 1.0, BSI-PP-0017, 2005-08-18

[PP0002]
Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik as BSI-PP-0002

[TCOSADM]
Administrator Handbuch TCOS Passport Version 2.0, Release 2/SLE66CLX800PE, T-Systems Enterprise Services GmbH, 2008