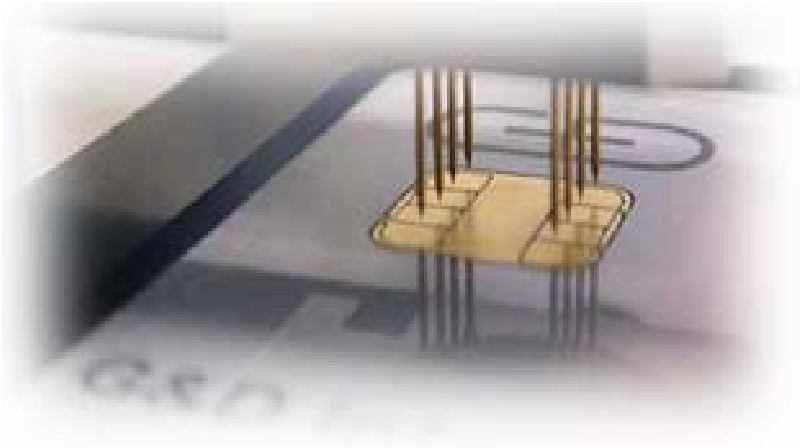
Security Target Lite
STARCOS 3.01 PE

Version 1.0 / Status 28.07.2006



Author: G&D/CSOP43
Status: Public/öffentlich

F&E

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

© Copyright 2006 by
Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München
This document as well as the information or material contained is copyrighted. Any use not explicitly permitted by copyright law requires prior consent of Giesecke & Devrient GmbH. This applies to any reproduction, revision, translation, storage on microfilm as well as its import and processing in electronical systems, in particular.
The information or material contained in this document is property of Giesecke & Devrient GmbH and any recipient of this document shall not disclose or divulge, directly or indirectly, this document or the information or material contained herein without the prior written consent of Giesecke & Devrient GmbH. All copyrights, trademarks, patents and other rights in connection herewith are expressly reserved to the Giesecke & Devrient group of companies and no license is created hereby.
Subject to technical changes.
All brand or product names mentioned are trademarks or registered trademarks of their respective holders.

Contents

1 Introduction 5
1.1 ST Identification 5
1.2 ST Overview 5
1.3 CC Conformance 6
1.4 Sections Overview 6
1.5 Change History 6
1.6 Tables 7
1.7 Application Notes of the PP 7
2 TOE Description 8
2.1 TOE definition 8
2.2 TOE usage and security features for operational use 9
2.3 TOE life cycle 10
2.3.1 Phase 1 “Development” 10
2.3.2 Phase 2 “Manufacturing” 11
2.3.3 Phase 3 “Personalization of the MRTD” 11
2.3.4 Phase 4 “Operational Use” 12
3 Security Problem Definition 13
3.1 Introduction 13
3.1.1 Assets 13
3.1.2 Subjects 13
3.2 Assumptions 14
3.2.1 A.Pers_Agent Personalization of the MRTD’s chip 14
3.2.2 A.Insp_Sys Inspection Systems for global interoperability 15
3.3 Threats 15
3.3.1 T.Chip_ID Identification of MRTD’s chip 15
3.3.2 T.Skimming Skimming the logical MRTD 15
3.3.3 T.Eavesdropping Eavesdropping to the communication between TOE and inspection system 15
3.3.4 T.Forgery Forgery of data on MRTD’s chip 15
3.3.5 T.Abuse-Func Abuse of Functionality 16
3.3.6 T.Information_Leakage Information Leakage from MRTD’s chip 16
3.3.7 T.Phys-Tamper Physical Tampering 16
3.3.8 T.Malfunction Malfunction due to Environmental Stress 17
3.4 Organisational Security Policies 17
3.4.1 P.Manufact Manufacturing of the MRTD’s chip 17
3.4.2 P.Personalization Personalization of the MRTD by issuing State or Organization only 17
3.4.3 P.Personal_Data Personal data protection policy 17
3.5 Security Objectives 18
3.5.1 Security Objectives for the TOE 18
3.5.2 Security Objectives for the Development and Manufacturing Environment 20
3.5.3 Security Objectives for the Operational Environment 21
4 Extended Components Definition 23
4.1 Definition of the Family FAU_SAS 23
4.1.1 FAU_SAS Audit data storage 23
4.1.2 FAU_SAS.1 Audit storage 23
4.2 Definition of the Family FCS_RND 23
4.2.1 FCS_RND Generation of random numbers 24
4.3 Definition of the Family FIA_API 24
4.3.1 FIA_API Authentication Prove of Identity 24
4.4 Definition of the Family FMT_LIM 25

4.4.1 FMT_LIM Limited capabilities and availability ... 25
4.5 Definition of the Family FPT_EMSEC ... 26
4.5.1 FPT_EMSEC.1 TOE Emanation ... 27
5 Security Requirements ... 28
5.1 Security Functional Requirements for the TOE ... 28
5.1.1 Class FAU Security Audit ... 28
5.1.2 Class Cryptographic Support (FCS) ... 29
5.1.3 Class FIA Identification and Authentication ... 31
5.1.4 Class FDP User Data Protection ... 34
5.1.5 Class FMT Security Management ... 38
5.1.6 Protection of the Security Functions ... 41
5.2 Security Assurance Requirements for the TOE ... 44
5.2.1 TOE Security Assurance Requirements ... 44
5.3 Security Requirements for the IT environment ... 44
5.3.1 Passive Authentication ... 44
5.3.2 Basic Inspection Systems ... 45
5.3.3 Personalization Terminals ... 49
6 TOE Summary Specification ... 51
6.1 TOE Security Functions ... 51
6.1.1 SF.ACCESS (Access Control) ... 51
6.1.2 SF.ADMIN (Administration of the TOE) ... 52
6.1.3 SF.AUTH (Authentication of the authorized TOE user) ... 52
6.1.4 SF.CRYPTO (Cryptographic Support) ... 53
6.1.5 SF.PROTECTION (Protection of TSC) ... 53
6.1.6 SF.IC (Security Functions of the IC) ... 54
6.2 Assurance Measures ... 54
7 PP Claims ... 56
7.1 PP Reference ... 56
8 Rationale ... 57
8.1 Security Objectives Rationale ... 57
8.2 Security Requirements Rationale ... 60
8.2.1 Security Functional Requirements Rationale ... 60
8.2.2 Dependency Rationale ... 65
8.2.3 Security Assurance Requirements Rationale ... 71
8.2.4 Security Requirements – Mutual Support and Internal Consistency ... 72
8.2.5 Rationale for Strength of Function High ... 73
8.3 Rationale for TOE Summary Specification ... 73
8.3.1 Rationale for TOE Security Functions ... 73
8.3.2 Rationale for Assurance Measures ... 84
8.4 Rationale for PP Claims ... 85
9 Appendix ... 86
9.1 Glossary and Acronyms ... 86
9.2 Acronyms ... 91
9.3 References ... 91

1 Introduction

1.1 ST Identification

Title: Security Target Lite STARCOS 3.01 PE (Passport Edition)
Reference: GDM_STA31_MRTD_ ASE_00
Version Number/Date: Version 1.0 / Status 28.07.2006
Origin: Giesecke & Devrient GmbH
Author: Dr. Ulrich Stutenbäumer
Compliant to: Common Criteria Protection Profile Machine Readable Travel Document with ”ICAO Application”, Basic Access Control, Version 1.0, 18.08.2005, BSI-PP-0017 [21a].
TOE name: STARCOS 3.01 PE
TOE version: 1.0
TOE documentation:
- Administrator Guidance
- User Guidance
- Installation, generation and start-up
- STARCOS301PETABLES

HW-Part of TOE: Philips P5CT072V0N (BSI-DSZ-CC-0312-2005).

1.2 ST Overview

The aim of this document is to describe the Security Target for STARCOS 3.01 PE for Passport Booklet IC.

The related product is the STARCOS 3.01 PE Operating System (OS) on a Smart Card Integrated Circuit. It is intended to be used as Passport Booklet IC in accordance with [21a] so the TOE consists of the related software in combination with the underlying hardware ('Composite Evaluation'). 'STARCOS 3.01 PE fulfils the requirements specified in [5].

STARCOS 3.01 PE is a fully interoperable ISO 7816 compliant multi-application Smart Card OS, including a cryptographic library enabling the user to apply TDES.

The software part of the TOE is implemented on the IC Philips P5CT072, which is certified according to CC EAL5+ [24]. So the TOE consists of the software part and the underlying hardware.

This document describes
- the Target of Evaluation (TOE)
- the security environment of the TOE
- the security objectives of the TOE and its environment
- and the TOE security functional and assurance requirements.

The assurance level for the TOE is CC **EAL4+**.
The minimum strength level for the TOE security functions is **high** (SOF high).

1.3 CC Conformance

This TOE claims conformance to: Common Criteria V2.1 (ISO 15408) (see [1], [2], [3]) (with Final Interpretation of CCIMB as of 14.06.2006)

as follows:
- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2 and ALC_DVS.2.

The TOE meets the specific BSI PP: Protection Profile Machine Readable Travel Document with "ICAO Application" as stated in [21a]).

1.4 Sections Overview

Section 1 provides the introductory material for the Security Target.
Section 2 provides general purpose and TOE description.
Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.
Section 4 defines the security objectives for both the TOE and the TOE environment.
Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [2] and Part 3 [3], that must be satisfied.
Section 6 contains the TOE Summary Specification.
Section 7 provides the compliance claims to the PP [21a].
Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 8 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the security target requirements
Section 9 provides a glossary and acronyms and identifies background material (References).

1.5 Change History

Version	Date	Changes	Remarks
1.0	28.07.06	Final Version.	stut

1.6 Tables

Table 1 Overview on authentication SFR 32
Table 2 Assurance Requirements: EAL(4+) 44
Table 3 SOF claims for TOE Security Functions 51
Table 4 References of Assurance Measures 55
Table 5 Security Objective Rationale 57
Table 6 Coverage of Security Objective for the TOE by SFR 60
Table 7 Coverage of Security Objectives for the IT environment by SFR 64
Table 8 Dependencies between the SFR for the TOE 68
Table 9 Dependencies between the SFR for the IT environment 71
Table 10 Functional Requirements to Security Function mapping 75
Table 11 Assurance Requirements to Assurance Measures mapping 85

1.7 Application Notes of the PP

When applicable the application notes of the PP are discussed in notes (1-26).

The following application notes of the PP are taken into account but are not explicitly discussed because they are either only important for the better understanding or are trivial:
Application Notes: 5, 13, 17, 19, 28-30, 32-36, 38-47, 48-53, 55-58.

2 TOE Description

Parts of this chapter have been taken from [21a].

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) [6] and providing the Basic Access Control according to the ICAO document [7].
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[1] and
- the associated guidance documentation.

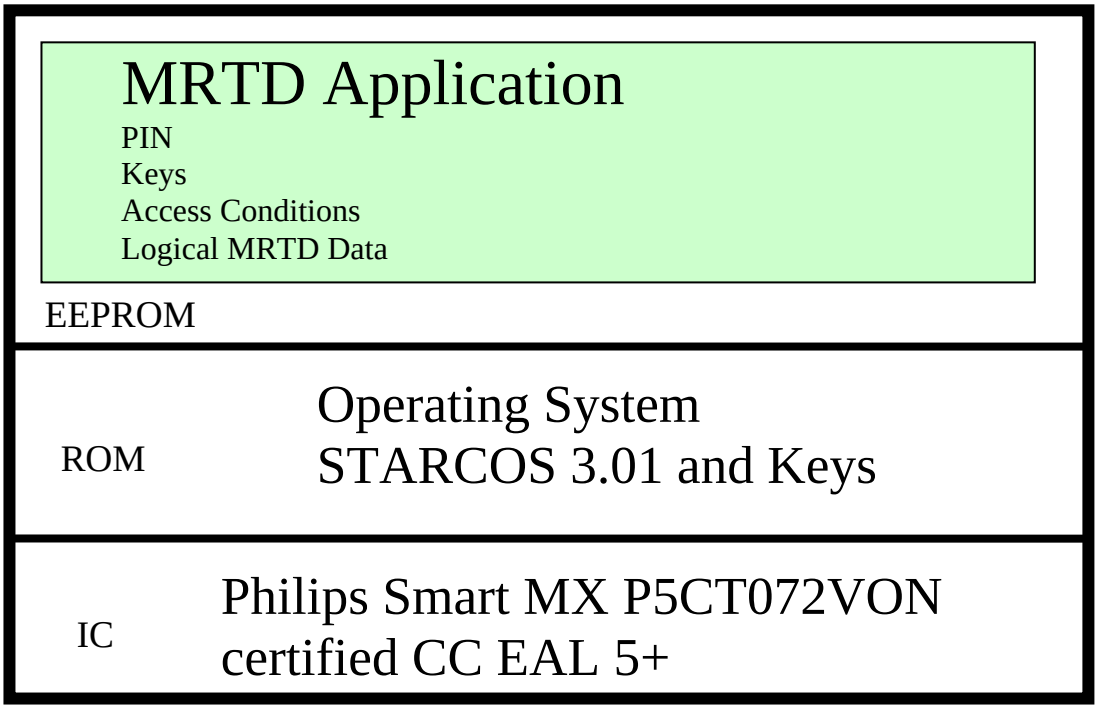


Figure 1 TOE description

[1] There is only one application part of the EEPROM: the MRTD application.

2.2 TOE usage and security features for operational use

State or organisation issues MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD. The issuing State or Organization ensure the authenticity of the data of genuine MRTD's. The receiving State trust a genuine MRTD of a issuing State or Organization. For this security target the MRTD is viewed as unit of

(a) the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder

(1) the biographical data on the biographical data page of the passport book,

(2) the printed data in the Machine-Readable Zone (MRZ) and

(3) the printed portrait.

(b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [6] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder

(1) the digital Machine Readable Zone Data (digital MRZ data, DG1),

(2) the digitized portraits (DG2),

(3) the optional biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both[2]

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

(5) the Document security object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the document number. The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organisational security measures (e.g. control of materials, personalization procedures) [8]. These security measures include the binding of the MRTD's chip to the passport book.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of additional biometrics as optional security measure in the ICAO Technical Report [7]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment. This security target addresses the protection of the logical MRTD (i) in integrity by

[2] These additional biometric reference data are optional

write-only-once access control[3] and by physical means, and (ii) in confidentiality by the
Basic Access Control Mechanism. This security target does not address the Active Authentication and the Extended Access Control as optional security mechanisms. The Basic Access Control is a security feature which shall be mandatory supported by the TOE but may be disabled by the Issuing State or Organization. The inspection system (i) reads the printed data in the MRZ, (ii) authenticates themselves as inspection system by means of keys derived form MRZ data. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [7], Annex E, and [6].

2.3 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases.

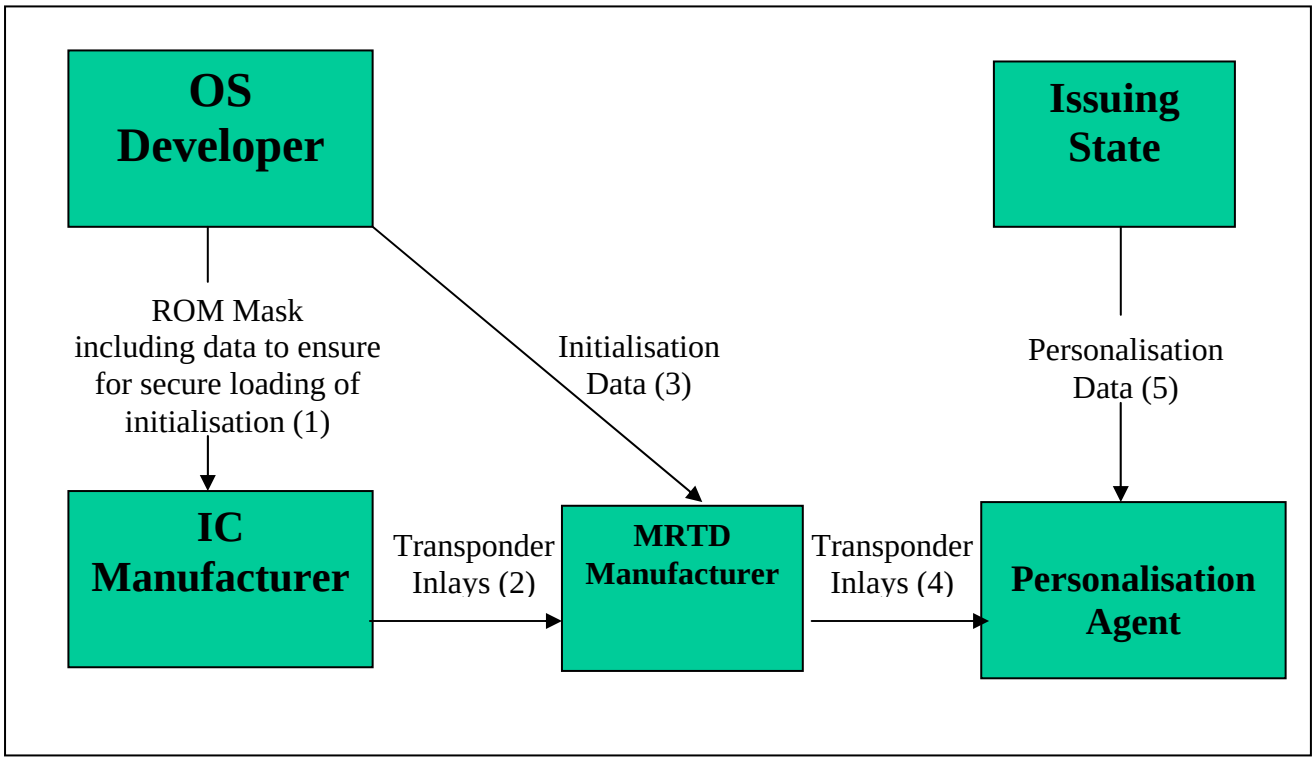


Figure 2 ROM Mask generation and delivery and Initialisation/Personalisation (example)

2.3.1 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.

[3] 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 TOE does not allow the Re-Personalisation of the MRTD in the Phase 4 Operational Use.

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((1) of figure 2). The IC Embedded Software in the nonvolatile programmable memories, the MRTD application, the initialisation data ((3) of figure 2). and the guidance documentation is securely delivered to the MRTD manufacturer ((2) of figure 2).

2.3.2 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 nonvolatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer ((2) of figure 2)..
The MRTD manufacturer (i) add the parts of the IC Embedded Software in the nonvolatile programmable memories (for instance EEPROM) if necessary, (ii) creates the MRTD application, and (iii) equips MRTD’s chip with Per-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 ((4) of figure 2).. The MRTD manufacturer also
provides the relevant parts of the guidance documentation to the Personalization Agent.

2.3.3 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 and their secure transfer to the personalisation agent ((4) of figure 2)., (iv) the writing of 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 digitised portrait (DG2), and (iii) the Document security object.
The signing of the Document security object by the Document signer [7] 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.

- Note 1: This security target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [7]. This approach allows but does not enforce the separation of these role. The TOE supports asymmetric and symmetric authentication of the Personalization Agent.

2.3.4 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.

- Note 2: The TOE does not allow the Re-Personalisation of the MRTD in the Phase 4 Operational Use.

- Note 3: The point of TOE delivery according to CC in this ST is after phase 2. The secure transfer of the TOE between the manufacturer and the personalisation site has to be realised.

3 Security Problem Definition

This chapter has been taken from [21a] without modification.

3.1 Introduction

3.1.1 Assets

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

3.1.1.1 Logical MRTD Data

The logical MRTD data consists of the data groups DG1 to DG16 and the Document security object according to LDS [6]. 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 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.

3.1.1.2 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.

3.1.2 Subjects

This security target considers the following subjects:

3.1.2.1 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.

3.1.2.2 MRTD Holder

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

3.1.2.3 Traveller

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

3.1.2.4 Personalization Agent

The agent is acting on the behalf of the issuing State or Organisation 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 [6].

3.1.2.5 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.

– Note: 4 This security target does not distinguish between the BIS and EIS because the Active Authentication and the Extended Access Control is outside the scope.

3.1.2.6 Terminal

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

3.1.2.7 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.

3.2 Assumptions

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

3.2.1 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). 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.

3.2.2 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 [7]. 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.

– Note 5: The TOE allows the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems.

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.

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 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 holders 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 MTRD's chip leaving their digital MZR 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.

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

3.3.6 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).

3.3.7 T.Phys-Tamper Physical Tampering

An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (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 prerequisite.
The modification may result in the deactivation of a security function.
Changes of circuitry or data can be permanent or temporary.

3.3.8 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 Organisational Security Policies

The TOE shall comply to the following organisation security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations (see CC part 1 [1], sec. 3.2).

3.4.1 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.

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

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitised 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.

3.4.3 P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (DG1), the printed portrait and the digitised 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 [7]. 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.

– Note 6: The organisational security policy P.Personal_Data is drawn from the ICAO Technical Report [7]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

3.5 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

3.5.1 Security Objectives for the TOE

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

3.5.1.1 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 [6] 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.

– Note 7: The TOE does not allow the Re-Personalisation of the MRTD in the Phase 4 Operational Use.

3.5.1.2 OT.Data_Int Integrity of personal data

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. 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.

3.5.1.3 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.

- Note 8: The TOE provides read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys The TOE to ensures the strength of the security function Basic Access Control Authentication independent on the quality of the Document Basic Access Keys which is defined by the TOE environment and loaded into the TOE by the Personalization Argent.

3.5.1.4 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 an 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.

- Note 9:. If the TOE is configured to allow a Basic Inspection System only to read these data the output of any other IC (e.g. integrated circuit serial number ICCSN) or a MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent is forbidden.

3.5.1.5 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.
Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.
The following TOE security objectives address the protection provided by the MRTD’s chip independent on the TOE environment.

3.5.1.6 OT.Prot_Inf_Leak Protection against Information Leakage

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD’s chip
- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

- Note 10: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker..

3.5.1.7 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.

– Note 11: The TOE is designed and fabricated so that it requires a high 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 such a physical attack.

3.5.1.8 OT.Prot_Malfunction Protection against Malfunctions

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

3.5.2 Security Objectives for the Development and Manufacturing Environment

3.5.2.1 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.

3.5.2.2 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 initialise, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.

3.5.3 Security Objectives for the Operational Environment

3.5.3.1 Issuing State or Organization

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

3.5.3.1.1 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 Organisation (i) establish the correct identity the holder and create biographic data for the MRTD, (ii) enrol 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

3.5.3.1.2 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 include all data in the data groups DG1 to DG16 if stored in the LDS according to [6].

3.5.3.2 Receiving State or organization

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

3.5.3.2.1 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.

3.5.3.2.2 OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the Receiving State uses the inspection system to verify the 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.

3.5.3.2.3 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.

- Note 12: The Primary Inspection System may prevent unauthorized listening to or manipulation of the communication with the MRTD's chip e.g. by a Faraday cage.

3.5.3.3 MRTD Holder

3.5.3.3.1 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.

- Note 13: The MRTD holder may prevent unauthorized communication of the MRTD's chip with terminals e.g. by carrying the MRTD in a metal box working as a Faraday cage.

4 Extended Components Definition

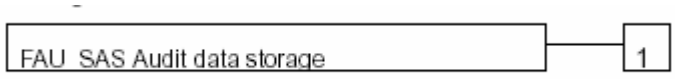
This security target uses components defined as extensions to CC part 2 [2]. Some of these components are defined in [20], other components are defined in [21a].
This chapter has been taken from [21a] without modification.

4.1 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined in [21a]. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.
The family “Audit data storage (FAU_SAS)” is specified as follows.

4.1.1 FAU_SAS Audit data storage

Family behaviour
This family defines functional requirements for the storage of audit data.
Component levelling



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.
Management: FAU_SAS.1
There are no management activities foreseen.
Audit: FAU_SAS.1
There are no actions defined to be auditable.

4.1.2 FAU_SAS.1 Audit storage

Hierarchical to: No other components.
FAU_SAS.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.
Dependencies: No dependencies.

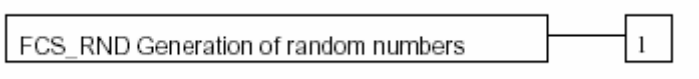
4.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined in [21a]. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

The family “Generation of random numbers (FCS_RND)” is specified as follows.

4.2.1 FCS_RND Generation of random numbers

Family behaviour
This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
Component levelling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.
Management: FCS_RND.1
There are no management activities foreseen.
Audit: FCS_RND.1
There are no actions defined to be auditable.
FCS_RND.1 Quality metric for random numbers
Hierarchical to: No other components.
FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].
Dependencies: No dependencies.

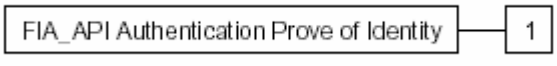
4.3 Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE an additional family (FIA_API) of the Class FIA (Identification and authentication) is defined in [21a]. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

- Note 14: This security target uses this explicit stated SFR for the personalization terminal in the IT environment only. Therefore the word "TSF" is substituted by the word "Personalization terminal".

4.3.1 FIA_API Authentication Prove of Identity

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



FIA_API.1 Authentication Prove of Identity.
Management: FIA_API.1
The following actions could be considered for the management functions in FMT:
Management of authentication information used to prove the claimed identity.
Audit: FCS_RND.1
There are no actions defined to be auditable.

4.3.1.1 FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.
FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or rule*].
Dependencies: No dependencies.

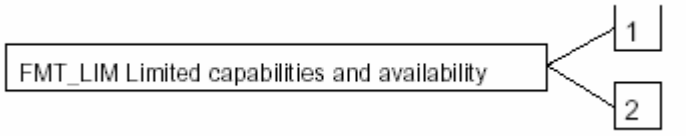
4.4 Definition of the Family FMT_LIM

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

The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

4.4.1 FMT_LIM Limited capabilities and availability

Family behaviour
This family defines requirements that limits the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.
Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.
Management: FMT_LIM.1, FMT_LIM.2
There are no management activities foreseen.
Audit: FMT_LIM.1, FMT_LIM.2
There are no actions defined to be auditable.
To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

4.4.1.1 FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.
FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: *Limited capability and availability policy*].
Dependencies: FMT_LIM.2 Limited availability.
The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

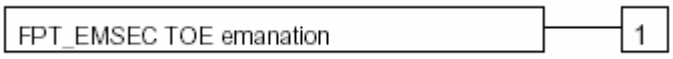
FMT_LIM.2 Limited availability

Hierarchical to: No other components.
FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].
Dependencies: FMT_LIM.1 Limited capabilities.

4.5 Definition of the Family FPT_EMSEC

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in [21a]. to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the logical MRTD data and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [2].

The family “TOE Emanation (FPT_EMSEC)” is specified as follows.
Family behaviour
This family defines requirements to mitigate intelligible emanations.
Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:
FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.
Management: FPT_EMSEC.1
There are no management activities foreseen.
Audit: FPT_EMSEC.1
There are no actions defined to be auditable.

4.5.1 FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.
FPT_EMSEC.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
Dependencies: No other components.

5 Security Requirements

This chapter has been taken from [21a] with some modifications[4].

The CC allows several operations to be performed on functional requirements; *refinement, selection, assignment,* and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this security target.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in bold text and the added/changed words are in bold text. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections filled in by the ST author appear as double underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are filled in this ST as underlined text..
The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

5.1 Security Functional Requirements for the TOE

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

5.1.1 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below.

FAU_SAS.1 Audit storage
Hierarchical to: No other components.

FAU_SAS.1.1
The TSF shall provide the Manufacturer[5] with the capability to store the IC Identification Data[6] in the audit records.

[4] The assignments filled in by the ST author are double underlined and when applicable the application notes of the PP are discussed in notes (see chapter 1.7).

[5] assignment: authorised users]

[6] [assignment: list of audit information]

Dependencies: No dependencies.

- Note 15: The TOE supports the security objective OD.Assurance by automatic tests in the Phase 3 "Personalization of the MRTD".

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 Key Derivation Algorithm[7] and specified cryptographic key sizes 112 bit[8] that meet the following: [7], Annex E.[9]

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 shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2).

FCS_CKM.4 Cryptographic key destruction - MRTD
Hierarchical to: No other components.

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

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

- Note 16**:** The TOE destroys the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

[7] [assignment: cryptographic key generation algorithm]

[8] [assignment: cryptographic key sizes]

[9] [assignment: list of standards]

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[10] in accordance with a specified cryptographic algorithm SHA-1[11] and cryptographic key sizes none[12] that meet the following: FIPS 180-2[13].

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

- Note 17: The TOE implements the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4/BAC_MRTD) according to [7].

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

Hierarchical to: No other components.

FCS_COP.1.1/ TDES_MRTD

The TSF shall perform secure messaging – encryption and decryption[14] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[15] and cryptographic key sizes 112 bit[16] that meet the following: FIPS 46-3 [14] and [7]; Annex E[17].

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

- Note 18: The TOE implements the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the

[10] [assignment: list of cryptographic operations]

[11] [assignment: cryptographic algorithm]

[12] [assignment: cryptographic key sizes]

[13] [assignment: list of standards]

[14] [assignment: list of cryptographic operations]

[15] [assignment: cryptographic algorithm]

[16] [assignment: cryptographic key sizes]

[17] [assignment: list of standards]

FCS_CKM.1/BAC_MRTD and FIA_UAU.4/BAC_BT. Note the Triple-DES in CBC mode with zero initial vector include also the Triple-DES in ECB mode for blocks of 8 byte used to check the authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

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[18] in accordance with a specified cryptographic algorithm Retail MAC[19] and cryptographic key sizes 112 bit[20] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[21].

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

- Note 19: The TOE implements the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/BAC_MRTD and FIA_UAU.4/BAC_MRTD.

5.1.2.2 Random Number Generation (FCS_RND.1)

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

FCS_RND.1/MRTD Quality metric for random numbers
Hierarchical to: No other components.

FCS_RND.1.1/ MRTD
The TSF shall provide a mechanism to generate random numbers that meet AIS 20 [5a].

Dependencies: No dependencies.

- Note 20: The TOE generates random numbers used for the authentication protocols as required by FIA_UAU.4/BAC_MRTD.

5.1.3 Class FIA Identification and Authentication

- Note 21: The Table 1 provides an overview on the authentication mechanisms used.

[18] [assignment: list of cryptographic operations]

[19] [assignment: cryptographic algorithm]

[20] [assignment: cryptographic key sizes]

[21] [assignment: list of standards]

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [7], Annex E, and [22]
Basic Access Control Authentication Mechanism	FIA_UAU.4/MRTD FIA_UAU.6/MRTD	FIA_UAU.4/BAC_T FIA_UAU.6/T	Triple-DES, 112 bit keys, Retail-MAC, 112 bit keys
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys

Table 1 Overview on authentication SFR

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

FIA_UID.1 Timing of identification
Hierarchical to: No other components.

FIA_UID.1.1
The TSF shall allow
(1) to read the Initialization Data and Pre-personalization 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 s in Phase 4 "Operational Use"[22]
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.

- Note 22: In this ST the user role Personalization Agent for the transition from Phase 2 to Phase 3 "Personalization of the MRTD" is possible. 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.

- Note 23: In the operation phase the MRTD must not allow anybody to read the ICCSN or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal for communication with more then one RFID. For the TOE this identifier is randomly selected and will not violate the OT.Identification.

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

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 s in Phase 4 “Operational Use”[23] 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.

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[24].

Dependencies: No dependencies.

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

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.

FIA_UAU.5.1
The TSF shall provide
1. Basic Access Control Authentication Mechanism

[23] [assignment: list of TSF-mediated actions]

[24] [assignment: identified authentication mechanism(s)]

2. Symmetric Authentication Mechanism based on Triple-DES[25]
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[26].

Dependencies: No dependencies.

- Note 24: The successful authenticated Personalization Agent may disable the Basic Access Control Mechanism before Phase 4

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[27].

Dependencies: No dependencies.

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.

[25] [assignment: list of multiple authentication mechanisms]

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

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

FDP_ACC.1.1/ PRIM
The TSF shall enforce the Primary Access Control SFP[28] on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD[29].

Dependencies: FDP_ACF.1 Security attribute based access control

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[30] on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD[31].

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.4.2 Security attribute based access control (FDP_ACF.1)

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2). 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[32] 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[33].

FDP_ACF.1.2/ PRIM

[28] [assignment: access control SFP]

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

[30] [assignment: access control SFP]

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

[32] [assignment: access control SFP]

[33] [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]

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[34].

FDP_ACF.1.3/ PRIM
The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[35].

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[36].

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

FDP_ACF.1 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[37] to objects based on the following:
1. Subjects:
   a. Personalization Agent
   b. Primary Inspection System
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[38].

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 and to read the 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[39].

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

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

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

[37] [assignment: access control SFP]

[38] [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]

FDP_ACF.1.3/ BASIC
The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[40].

FDP_ACF.1.4/ BASIC
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[41].

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

5.1.4.3 Inter-TSF-Transfer

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

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD
Hierarchical to: No other components.

FDP_UCT.1.1/ MRTD
The TSF shall enforce the Basic Access Control SFP[42] to be able to transmit and receive[43] objects in a manner protected from unauthorised 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[44] to be able to transmit and receive[45] user data in a manner protected from modification, deletion, insertion and replay[46] errors.

---

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

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

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

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

[43] [selection: transmit, receive]

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

[45] [selection: transmit, receive]

FDP_UIT.1.2/ MRTD
The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[47] 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 "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

FMT_MOF.1 Specification of Management Functions
Hierarchical to: No other components.

FMT_MOF.1.1
The TSF shall restrict the ability to enable and disable[48] the functions TSF Basic Access Control[49] to Personalization Agent[50].

Dependencies: No Dependencies

Note 25: The TSF Basic Access Control can only be enabled and disabled once by the Personalisation Agent before the phase 4 "Operational Use. The disabling of the TSF Basic Access Control is not accompanied with the disabling of the Basic Access Control Authentication Mechanism.

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[51].

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

[47] [selection: modification, deletion, insertion, replay]

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

[49] [assignment: list of functions]

[50] [assignment: the authorised identified roles]

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

Dependencies: No Dependencies

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[52].

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

Hierarchical to: No other components.

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below (Common Criteria Part 2 extended).

FMT_LIM.1 Limited capabilities
Hierarchical to: No other components.

FMT_LIM.1.1
The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: 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.

Dependencies: FMT_LIM.2 Limited availability.

The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below (Common Criteria Part 2 extended).

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

[52] [assignment: the authorised identified roles]

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.

Dependencies: FMT_LIM.1 Limited capabilities.

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

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data
Hierarchical to: No other components.

FMT_MTD.1.1/ INI_ENA
The TSF shall restrict the ability to write[53] the Initialization Data and Pre-personalization Data[54] to the Manufacturer[55].

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

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

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

FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write
Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_WRITE

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

[54] [assignment: list of TSF data]

[55] [assignment: the authorised identified roles]

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

[57] [assignment: list of TSF data]

[58] [assignment: the authorised identified roles]

The TSF shall restrict the ability to write[59] the Document Basic Access Keys[60] to the Personalization Agent[61].
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[62] the Document Basic Access Keys and Personalization Agent Keys[63] to none[64].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security 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 “Subset information flow control (FDP_IFC.1)” as specified below:

FPT_EMSEC.1 TOE Emanation
Hierarchical to: No other components.

FPT_EMSEC.1.1
The TOE shall not emit information about IC power consumption and command execution time in excess of non useful information enabling access to Personalization Agent Authentication Key[65] and logical MRTD data.

FPT_EMSEC.1.2

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

[60] [assignment: list of TSF data]

[61] [assignment: the authorised identified roles]

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

[63] [assignment: list of TSF data]

[64] [assignment: the authorised identified roles]

[65] [assignment: list of types of TSF data]

The TSF shall ensure any unauthorized users[66] are unable to use the following interface smart card circuit contacts[67] to gain access to Personalization Agent Authentication Key[68] and logical MRTD data.

Dependencies: No other components.

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

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

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.

FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur:
(1) exposure to operating conditions where therefore a malfunction could occur,
(2) failure detected by TSF according to FPT_TST.1[69].

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, at the condition Reset of the TOE to demonstrate the correct operation of the TSF.

FPT_TST.1.2
The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

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

Dependencies: FPT_AMT.1 Abstract machine testing.

[66] [assignment: type of users]

[67] [assignment: type of connection]

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

[69] [assignment: list of types of failures in the TSF]

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

FPT_PHP.3 Resistance to physical attack
Hierarchical to: No other components.

FPT_PHP.3.1
The TSF shall resist physical manipulation and physical probing[70] to the TSF[71] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

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.

Dependencies: No dependencies.

[70] [assignment: physical tampering scenarios]

[71] [assignment: list of TSF devices/elements]

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 minimum strength of function is SOF-high.

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

5.2.1 TOE Security Assurance Requirements

The following table list the required assurance requirement classes according [21a] with the components ADV_IMP.2 and ALC_DVS.2 augmented to EAL4.

All final interpretations till now (17.02.2006) are applied.

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.2 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.2 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.2 AVA_SOF.1 AVA_VLA.2

Table 2 Assurance Requirements: EAL(4+)

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 [7] 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[72].

FDP_DAU.1.2/ DS
The **Document Signer** shall provide Inspection Systems of Receiving States or Organization[73] with the ability to verify evidence of the validity of the indicated information.

Dependencies: No dependencies

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 Mechanism with the Personalization Agent Authentication Keys. Both are called "Basic Terminals" (BT) in this section.

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

FCS_CKM.1/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[74] and specified cryptographic key sizes 112 bit[75] that meet the following: [7], Annex E[76].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FDP_ITC.2 Import of user data with security attributes, or

[72] [assignment: list of objects or information types]

[73] [assignment: list of subjects]

[74] [assignment: cryptographic key generation algorithm]

[75] [assignment: cryptographic key sizes]

[76] [assignment: list of standards]

FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4/BT Cryptographic key destruction - BT
Hierarchical to: No other components.

FCS_CKM.4.1/BT
The **Basic 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 that meets the following: none.

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 Basic 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[77] in accordance with a specified cryptographic algorithms SHA-1[78] and cryptographic key sizes none[79] that meet the following: FIPS 180- 2[80].

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.

[77] [assignment: list of cryptographic operations]

[78] [assignment: cryptographic algorithm]

[79] [assignment: cryptographic key sizes]

[80] [assignment: list of standards]

FCS_COP.1.1/ ENC_BT
The **Basic Terminal** shall perform secure messaging – encryption and decryption[81] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[82] and cryptographic key sizes 112 bit[83] that meet the following: FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)[84].

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[85] in accordance with a specified cryptographic algorithm Retail-MAC[86] and cryptographic key sizes 112 bit[87] that meet the following: FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 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

The Basic Terminal shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

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 AIS 20 [5a].

[81] [assignment: list of cryptographic operations]

[82] [assignment: cryptographic algorithm]

[83] [assignment: cryptographic key sizes]

[84] [assignment: list of standards]

[85] [assignment: list of cryptographic operations]

[86] [assignment: cryptographic algorithm]

[87] [assignment: cryptographic key sizes]

[88] [assignment: list of standards]

Dependencies: No dependencies.

- Note 26: The quality metric chosen ensures at least the strength of function Basic Access Control Authentication for the challenges.

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

FIA_UAU.4/BT Single-use authentication mechanisms –Basic Terminal
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 [89].

Dependencies: No dependencies.

The Basic 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[90].
Dependencies: No dependencies.

The Basic 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 Basic Access Control SFP[91] to be able to transmit and receive[92] objects in a manner protected from unauthorised 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 Basic Terminal shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

[89] [assignment: identified authentication mechanism(s)]

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

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

[92] [selection: transmit, receive]

FDP_UIT.1/BT Data exchange integrity - Basic Terminal
Hierarchical to: No other components.

FDP_UIT.1.1/BT
The **Basic Terminal** shall enforce the Basic Access Control SFP[93] to be able to transmit and receive[94] user data in a manner protected from modification, deletion, insertion and replay[95] 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[96] 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 establish 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 Prove of Identity (FIA_API)" as specified below (Common Criteria Part 2 extended).

FIA_API.1/SYM_PT Authentication Prove of Identity - Personalization Terminal Authentication with Symmetric Key
Hierarchical to: No other components.

FIA_API.1.1/SYM_PT

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

[94] [selection: transmit, receive]

[95] [selection: modification, deletion, insertion, replay]

[96] [selection: modification, deletion, insertion, replay]

The **Personalization Terminal** shall provide a Authentication Mechanism based on Triple-DES[97] to prove the identity of the Personalization Agent[98].

Dependencies: No dependencies.

[97] [assignment: authentication mechanism]

[98] [assignment: authorized user or rule]

6 TOE Summary Specification

This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

6.1 TOE Security Functions

This chapter gives the overview description of the different TOE Security Functions composing the TSF.
In the following table all TOE Security Functions are listed and if appropriate a SOF claim is stated. The assessment of cryptographic algorithms is not part of this CC evaluation.

TOE Security Function	SOF claim	Description
SF.ACCESS	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational nocryptographic mechanism.
SF.ADMIN	High	There is a probabilistic authentication mechanism of the card manufacturer during initialisation phase.
SF.AUTH	High	There is a probabilistic authentication mechanism of the card manufacturer during initialisation phase and a probabilistic authentication mechanism for BAC. .
SF.CRYPTO	High	The random number generators and hash functions are probabilistic mechanisms. The deterministic random number generator is rated K3 (high) according to AIS20 [5a].
SF.PROTECTION	not appropriate	This TOE Security Function is not realised by a probabilistic or permutational noncryptographic mechanism.
SF.IC	High	Several Security Functions of the IC are realised by probabilistic or permutational noncryptographic mechanisms. For the rating of the HW-RNG according to AIS31 [5] see[24]

Table 3 SOF claims for TOE Security Functions

The SFs described in 6.1.1 to 6.1.5 are realised by software components supported by the underlying hardware in accordance with the description in 6.1.6 (hardware related SF). The SF.IC.2, covering a failure with preservation of secure state, is not realised by a probabilistic or permutational noncryptographic mechanism; either a failure is detected or not.

6.1.1 SF.ACCESS (Access Control)

Before the TSF performs an operation requested by a user, this Security function checks if the operation specific requirements on user authorisation and protection of communication data are fulfilled.
This Security Function is composed of

1) in the TOE configuration for use with Primary Inspection Systems:
   - Allowing only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,
   - Allowing the terminals to read only the data of the groups DG1 to DG16 of the logical MRTD.
2) in the TOE configuration for use with Basic Inspection Systems
   - Allowing only the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
   - Allowing only the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD [[7]].
3) Not allowing anybody to modify any of the data groups DG1 to DG16 of the logical MRTD in the usage phase.
4) TSF mediated actions on behalf of an user require his prior successful identification and authentication if Basic Access Control [[7]] is activated and if it is not specified in this chapter otherwise.
5) Only the Personalization Agent is allowed to write the Document Basic Access Keys.
6) Nobody is allowed to read the Document Basic Access Keys and Personalization Agent Keys.

6.1.2 SF.ADMIN (Administration of the TOE)

The administration of the TOE is managed by this Security Function.
This Security Function is composed of:

1) Storage of IC Identification Data in audit records through the Manufacturer.
2) Possibility to read before user identification and authentication:
   - the Initialization Data in Phase 2 “Manufacturing”,
   - the ATR (different for and after Initialisation)
   - the logical MRTD if the TOE is configured for use with Primary Inspection Systems in Phase 4 “Operational Use”.
3) Enabling and disabling the TSF Basic Access Control only through the Personalization Agent.
4) Initialization, personalisation and configuration of the TOE are only allowed for the Manufacturer and the Personalisation Agent.
5) Ability to write the Initialization Data and Pre-personalization Data restricted to the Manufacturer.
6) Ability to disable read access for users to the Initialization Data restricted to the Personalization Agent.
7) Ability to write the Document Basic Access Keys.
8) Test Features of the TOE are not available for the user in Phase 4 “Operational Use”. If Test Features are performed by the TOE than no User Data can be disclosed or manipulated, no TSF data can be disclosed or manipulated, no software can be reconstructed and no substantial information about construction of TSF can be gathered which may enable other attacks.
9) Maintenance of the security roles: Manufacturer, Personalization Agent, Primary Inspection System, Basic Inspection System.
10) Ability to write the data of the data groups DG1 to DG16 of the logical MRTD.

.

6.1.3 SF.AUTH (Authentication of the authorized TOE user)

The authentication for the authorized TOE user is managed by this Security Function.

This Security Function is composed of:

1) User authentication provided through:
   - Basic Access Control Authentication Mechanism
2) Prevention of reuse of authentication data.
3) User authentication for the Personalisation Agent:
   (a) for the Basic Access Control Authentication Mechanism with the Personalization Agent Keys,
   (b) for the Symmetric Authentication Mechanism with the Personalization Agent Key
4) User authentication for the Basic Inspection System through:
   - the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
5) Enabling the authentication of an user under the conditions that each command is sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism.
6) Ability to read the data of the groups DG1 to DG16 of the logical MRTD.

6.1.4 SF.CRYPTO (Cryptographic Support)

This Security Function provides the cryptographic support for the other Security Functions.

This Security Function is composed of:

1) DES key generation in accordance with the Document Basic Access Control Key Derivation Algorithm with key sizes of 112 bit that meet: [7], Annex E.
2) Hashing in accordance with SHA-1 that meet the following: FIPS 180-2.
3) Secure messaging – encryption and decryption with Triple-DES in CBC mode and key sizes of 112 bit that meet: FIPS 46-3 [14]and [7]; Annex E.
4) Secure messaging – message authentication with Retail MAC and key sizes of 112 bit that meet: ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2).
5) Random number generation according AIS20 [5a] for key generation and authentication process.
6) After each BAC session the relevant Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging are destroyed.

This Security Function has the level of strength SOF-high.

6.1.5 SF.PROTECTION (Protection of TSC)

This Security Function protects the TSF functionality, TSF data and user data. If BAC is enabled, no unencrypted data transmission between TOE and the outside of the TOE is allowed.

This Security Function is composed of:

1) Ensuring that transmitted and received user data is protected from modification, deletion, insertion and replay errors through secure messaging when BAC is enabled.
2) Ensuring that transmitted and received objects are protected from unauthorised disclosure through secure messaging when BAC is enabled.
3) Determination on receipt of user data if modification, deletion, insertion and replay have occurred through secure messaging when BAC is enabled.

4) Hiding information about IC power consumption and command execution time.
5) Demonstrating the correct operation of the TSF.
6) The TOE ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
7) Maintaining a security domain for the TSF execution that protects it from interference and tampering by untrusted subjects.
8) Enforcing separation between the security domains of subjects in the TSC.

6.1.6 SF.IC (Security Functions of the IC)

This Security Function covers the Security Functions of the IC [5].
This Security Function is composed of:

1) Detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.
2) Resistance to physical tampering of the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analysing and physical tampering.
3) Random number generation.
4) Cryptographic support for DES calculations.

This Security Function has the level of strength SOF-high.

6.2 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 5 Security Requirements.
The following table lists the Assurance measures and references the corresponding documents describing the measures.

Assurance Measures	Description
AM_ACM	The configuration management is described in GDM_STA31_MRTD_ACM_00.
AM_ADO	The delivery, installation, generation and start-up of the TOE is described in GDM_STA31_MRTD _ADO_00.
AM_ADV	The representing of the TSF is described in GDM_STA31_MRTD _ADV_SPM_00 for security policy modelling, in GDM_STA31_MRTD _ADV_FSP_00 for functional specification, in GDM_STA31_MRTD _ADV_HLD_00 for high level design, in GDM_STA31_MRTD _ADV_LLD_00 for low level design, in GDM_STA31_MRTD _ADV_IMP_00 for implementation representation and in GDM_STA31_MRTD _ADV_RCR_00 for representation correspondence.
AM_AGD	The guidance documentation is described in GDM_STA31_MRTD _AGD_USR_00 for the user and in GDM_STA31_MRTD _AGD_ADM_00 for the administrator.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in GDM_STA31_MRTD _ALC_00

Assurance Measures	Description
AM_ATE	The testing of the TOE is described in GDM_STA31_MRTD _ATE_00.
AM_AVA	The vulnerability assessment for the TOE is described in GDM_STA31_MRTD _AVA_MSU_00 for the misuse, in GDM_STA31_MRTD _AVA_SOF_00 for the strength of TOE security functions and in GDM_STA31_MRTD _AVA_VLA_00 for the vulnerability analysis.

Table 4 References of Assurance Measures

Note: Reference end numbers may change during evaluation process (e.g. GDM_STA31_MRTD _AVA_VLA_00 may become GDM_STA31_MRTD _AVA_VLA_02).

7 PP Claims

7.1 PP Reference

The conformance of this ST to the Protection Profile Common Criteria Protection Profile Machine Readable Travel Document with ”ICAO Application”, Basic Access Control, Version 1.0, 18.08.2005, BSI-PP-0017 [21a] is claimed.

8 Rationale

The chapters 8.1 and 8.2 have been taken from [21a] without modification and show that the security objectives cover the TOE security environment and IT security requirements are appropriate to satisfy the security objectives.

The tables in sub-sections 8.1, 8.2 and 8.3.1 Rationale for TOE Security Functions provide the mapping of the security objectives and security requirements for the TOE.

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
T.Eavesdropping			x													
T.Forgery	x	x					x					x	x	x		
T.Abuse-Func					x											
T.Information_Leakage						x										
T.Phys-tamper							x									
T.Malfunction								x								
P.Manufact									x	x						
P.Personalization	x								x		x					
P.Personal_Data		x	x													
A.Pers_Agent											x					
A.Insp_Sys													x		x	

Table 5 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 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".
240 The threat **T.Forgery** "Forgery of data on MRTD's chip" address 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 are 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 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

8.2.1 Security Functional 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-Tampe	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	
FPT_PHP.3					x	x		
FPT_SEP.1							x	x

Table 6 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 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_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_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 Control according to the SFR FMT_MOF.1 and the Document Basic Access 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 preventing 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 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 Control Keys and the Personalization Agent handles the configuration of the TSF Basic Access Control according to the SFR FMT_MOF.1.

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. 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 Control Keys).
The SFR FIA_UAU.4/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The FIA_UAU.5 enforce 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 request 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 allow the Personalization
Agent to disable Initialization Data if their use in the phase 4 “Operational Use” violate the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD’s chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application note 28). The FMT_MTD.1/INI_ENA restricts the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

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 demonstare 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.

	OE.Personalization	OE.Exam_MRTD	OE.Prot_Logical_MRTD
Document Signer			
FDP_DAU.1/DS		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 7 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. The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical address the protection of 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.

The **OE.Personalization** "Personalization of logical MRTD" requires the MRTD" 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.

8.2.2 Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.
The table 7 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_M RTD	[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 or 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 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_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 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_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 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_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.

SFR	Dependencies	Support of the Dependencies
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
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

SFR	Dependencies	Support of the 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	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_READ	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
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 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 and FCS_COP.1/MAC. The SFR FCS_CKM.4/MRTD destroys these keys automatically. These simple processes do not need any special security attributes for the secure messaging keys.

No. 2: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR are 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 consist of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

The table 8 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/TDES BT, FCS_COP.1/MAC_BT justification 7 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
FCS_CKM.4/BT	[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	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 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 8 for non-satisfied dependencies
FCS_COP.1/ENC_BT	[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_CKM.1, FCS_CKM.4, justification 9 for non-satisfied dependencies
FCS_COP.1/MAC_BT	[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_CKM.1, FCS_CKM.4, justification 9 for non-satisfied dependencies
FCS_RND.1/BT	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
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 I nter-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 9 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 and FCS_COP.1/MAC. The SFR FCS_CKM.4/BT destroys these keys. These processes do not need any special security attributes for the secure messaging keys.

No. 8: The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR are needed to be defined for this specific instantiation of FCS_COP.1.

No. 9: The SFR FCS_COP.1/TDES_BT and FCS_COP.1/MAC_BT use the automatically generated secure messaging keys assigned to the session with the successfully authenticated MRTD only. There is no need for any special security attributes for the secure messaging keys.

No. 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.

8.2.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in

conventional commodity TOEs and are prepared to incur 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 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
Dependencies ALC_DVS.2: no.

8.2.4 Security Requirements – Mutual Support and Internal Consistency

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

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

The dependency analysis in section 8.2.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the additional assurance components in section 8.2.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

The Personalization Agent may configure the TOE according to the organisational security policy (i) for use with Primary Inspection Systems or (ii) for use with Basic Inspection Systems. According to the security objective OT.Data_Conf the TOE enforces different security functional policies for the chosen (by means of the SFr FMT_MOF.1) configurations (i.e. the Primary Access Control SFP for the use with Primary Inspection Systems and the Basic Access Control SFP for the use with Basic

Inspection Systems). These SFP are implemented by two internally consistent sets of SFR for the cryptographic functions, the user identification, the user authentication, the access control and - in case of the Basic Access Control SFP - for the data export protection. All TSF are protected by a common set of SFR of the FPT against any attempt to bypass, to deactivate, to manipulate or to misuse the TOE security features or TSF.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 8.2.2 Dependency Rationale and 8.2.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 8.2.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

8.2.5 Rationale for Strength of Function High

The TOE shall demonstrate to be highly resistant against penetration attacks in order to meet the requirements of the Protection Profile [[21a].] (see 5.2) and its correspondent SFRs (FIA_UAU.4 , FCS_RND.1 and FPT_FLS.1). The protection against attacks with a high attack potential dictates a strength of function high rating for functions in the TOE that are realised by probabilistic or permutational mechanisms (SF.ADMIN (Administration of the TOE), SF.AUTH (Authentication of the authorized TOE user), SF.CRYPTO (Cryptographic Support), SF.IC (Security Functions of the IC)).

8.3 Rationale for TOE Summary Specification

8.3.1 Rationale for TOE Security Functions

The following table gives the coverage of the TOE Security Functional Requirements by the TOE Security Functions. The numbers in the table give the corresponding component of the Security Function covering the requirement.
The identified components obviously satisfy the requirements.

TOE SFR / Security Function	SF.ACCESS (Access Control	SF.ADMIN (Administration of the TOE	SF.AUTH (Authentication of the	SF.CRYPTO (Cryptographic Support	SF.PROTECTION (Protection of TSC	SF.IC (Security Functions of the IC
FAU_SAS.1.1		1)				
FCS_CKM.1.1/ BAC_MRTD				0		
FCS_CKM.4.1/ MRTD				5)		
FCS_COP.1.1/ SHA_MRTD				1)		
FCS_COP.1.1/ TDES_MRTD				2)		4)

TOE SFR / Security Function	SF.ACCESS (Access Control	SF.ADMIN (Administration of the TOE	SF.AUTH (Authentication of the	SF.CRYPTO (Cryptographic Support	SF.PROTECTION (Protection of TSC	SF.IC (Security Functions of the IC
FCS_COP.1.1/MAC_MRTD				3)		
FCS_RND.1.1/ MRTD				4)		3)
FIA_UID.1.1		2)				
FIA_UID.1.2	4)					
FIA_UAU.1.1		2)				
FIA_UAU.1.2		4)				
FIA_UAU.4.1/ MRTD			2)			
FIA_UAU.5.1			1)			
FIA_UAU.5.2			3), 4)			
FIA_UAU.6.1/MRTD			5)			
FDP_ACC.1.1/ PRIM	1)					
FDP_ACC.1.1/ BASIC	2)					
FDP_ACF.1.1/PRIM	1)					
FDP_ACF.1.2/ PRIM	1)	10)	6)			
FDP_ACF.1.3/ PRIM	1)					
FDP_ACF.1.4/ PRIM	3)					
FDP_ACF.1.1/ BASIC	2)					
FDP_ACF.1.2/ BASIC	2)	10)	6)			
FDP_ACF.1.3/ BASIC	2)					
FDP_ACF.1.4/ BASIC	3)					
FDP_UCT.1.1/ MRTD					2)	
FDP_UIT.1.1/ MRTD					1)	
FDP_UIT.1.2/ MRTD					3)	
FMT_MOF.1.1		3)				
FMT_SMF.1.1		4)				
FMT_SMR.1.1		9)				
FMT_SMR.1.2		9)				
FMT_LIM.1.1		8)				
FMT_LIM.2.1		8)				
FMT_MTD.1.1/ INI_ENA		5)				
FMT_MTD.1.1/ INI_DIS		6)				
FMT_MTD.1.1/ KEY_WRITE	5)	7)				
FMT_MTD.1.1/ KEY_READ	6)					
FPT_EMSEC.1.1					4)	
FPT_EMSEC.1.2					4)	
FPT_FLS.1.1						2)
FPT_TST.1.1					5)	
FPT_TST.1.2					5)	
FPT_TST.1.3					5)	

TOE SFR / Security Function	SF.ACCESS (Access Control	SF.ADMIN (Administration of the TOE	SF.AUTH (Authentication of the	SF.CRYPTO (Cryptographic Support	SF.PROTECTION (Protection of TSC	SF.IC (Security Functions of the IC
FPT_PHP.3.1						1)
FPT_RVM.1.1					5)	
FPT_SEP.1.1					7)	
FPT_SEP.1.2					7)	

Table 10 Functional Requirements to Security Function mapping

8.3.1.1 Justifications for the correspondence between functional requirements and security functions

8.3.1.1.1 FAU_SAS.1.1

The storage of IC Identification Data in audit records through the Manufacturer is managed by the TSF.ADMIN (Administration of the TOE).
FAU_SAS.1.1 requires that the Manufacturer has the capability to store the IC Identification Data in the audit records. SF.ADMIN.1 states that the Storage of IC Identification Data in audit records through the Manufacturer is supported by the TOE and therefore meets the above stated TOE SFR.

8.3.1.1.2 FCS_CKM.1.1/ BAC_MRTD, FCS_COP.1.1/ SHA_MRTD, FCS_RND.1.1/ MRTD

The cryptographic support for the other Security Functions is managed by TSF.CRYPTO (Cryptographic Support).

FCS_CKM.1.1/ BAC_MRTD requires that the Document Basic Access Control Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [7], Annex E. are applied. SF.Crypro.1 states that DES key generation in accordance with the Document Basic Access Control Key Derivation Algorithm with key sizes of 112 bit that meet: [7], Annex E are supported by the TOE and therefore meets the above stated TOE SFR.

FCS_CKM.4.1/ MRTD requires that cryptographic keys are destroyed in accordance with a specified cryptographic key destruction method physical deletion by overwriting the memory data with zeros or random data that meets the following: none.
SF.Crypto.6 states that after each BAC session the relevant Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging are destroyed and therefore meets the above stated TOE SFR.

FCS_COP.1.1/ SHA_MRTD requires that hashing is performed in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: FIPS 180-2. SF.Crypto.2 states that hashing by the TOE is performed in accordance with SHA-1 that meet the following: FIPS 180-2 and therefore meets the above stated TOE SFR.

FCS_COP.1.1/ TDES_MRTD requires that secure messaging – encryption and decryption is performed in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [14] and [7]; Annex E. SF.Crypto.3 states that secure messaging – encryption and decryption is performed with Triple-DES in CBC mode and key sizes of 112 bit that meet: FIPS 46-3 [14]and [7]; Annex E and SF. IC.4 supports the cryptographic support for DES calculations and therefore meets the above stated TOE SFR.

FCS_COP.1.1/MAC_MRTD requires that secure messaging – message authentication code is performed in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2). SF.Crypto.4 states that secure messaging – message authentication is performed with Retail MAC and key sizes of 112 bit that meet: ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2) and therefore meets the above stated TOE SFR.

FCS_RND.1.1/ MRTD requires that the TSF shall provide a mechanism to generate random numbers that meet AIS 20 [5a]. SF.Crypto.5 states that random number generation according AIS20 [5a] for key generation and authentication process is supported by the TOE and SF.IC.3 states that the TOE supports random number generation and therefore meets the above stated TOE SFR.

8.3.1.1.3 **FIA_UID.1.1** , **FIA_UAU.1.1**

The Timing of identification and authentication is managed by TSF.ADMIN (Administration of the TOE) if the administrator is involved and additionally by TSF.AUTH (Authentication of the TOE).

FIA_UID.1.1 requires that the TSF shall allow
(1) to read the Initialization Data and Pre-personalization 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 s in Phase 4 "Operational Use"
on behalf of the user to be performed before the user is identified.
SF.ADMIN.2 states that the TOE realises the possibility to read before user identification and authentication:

- the Initialization Data in Phase 2 "Manufacturing",
- the ATR in Phase 3 "Personalization of the MRTD",
- the ATR if the TOE is configured for use with Basic Inspection Systems only in Phase 4 "Operational Use",
- the logical MRTD if the TOE is configured for use with Primary Inspection Systems in Phase 4 "Operational Use"

and therefore meets the above stated TOE SFR.

FIA_UID.1.2 requires that TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
SF.ACCESS states that the TSF mediated actions on behalf of an user require his prior successful identification and authentication if it is not specified in this chapter otherwise and therefore meets the above stated TOE SFR.

FIA_UAU.1.1 requires that 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 s in Phase 4 "Operational Use" on behalf of the user to be performed before the user is authenticated.
SF.ADMIN.2 states that the TOE realises the possibility to read before user identification and authentication:

- the Initialization Data in Phase 2 "Manufacturing",
- the ATR in Phase 3 "Personalization of the MRTD",
- the ATR if the TOE is configured for use with Basic Inspection Systems only in Phase 4 "Operational Use",
- the logical MRTD if the TOE is configured for use with Primary Inspection Systems in Phase 4 "Operational Use"

and therefore meets the above stated TOE SFR.

FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
SF.ADMIN.4 states that the TSF mediated actions on behalf of an user require his prior successful identification and authentication if it is not specified in this chapter otherwise and therefore meets the above stated TOE SFR.

FIA_UAU.4.1/ MRTD requires that the TSF shall prevent reuse of authentication data related to
1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on Triple-DES.
SF.AUTH.2 realises the prevention of reuse of authentication data and therefore meets the above stated TOE SFR.

FIA_UAU.5.1 requires that the TSF shall provide
1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on Triple-DES
to support user authentication.

SF.AUTH.1 realises user authentication provided through:

- Basic Access Control Authentication Mechanism
- Symmetric Authentication Mechanism

based on Triple-DES and therefore meets the above stated TOE SFR.

FIA_UAU.5.2 requires that 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.

SF.AUTH.3 and .4 realises user authentication for the Personalisation Agent:

(a) for the Basic Access Control Authentication Mechanism with the Personalization Agent Keys,
(b) for the Symmetric Authentication Mechanism with the Personalization Agent Key

and user authentication for the Basic Inspection System through:

- the Basic Access Control Authentication Mechanism with the Document Basic Access Keys

and therefore meets the above stated TOE SFR.

FIA_UAU.6.1/MRTD requires that 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.
SF.AUTH.5 enables the authentication of an user under the conditions that each command is sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and therefore meets the above stated TOE SFR.

8.3.1.1.4 FDP_ACC.1.1/ PRIM, FDP_ACF.1.1/PRIM

The TSF.ACCESS (Access Control) performs an operation requested by an user, this Security function checks if the operation specific requirements on user authorisation and protection of communication data are fulfilled.

FDP_ACC.1.1/ PRIM requires that the TSF shall enforce the Primary Access Control SFP on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD.
SF.ACCESS.1 in the TOE configuration for use with Primary Inspection Systems:

- allows only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,
- allows only the terminals to read the data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACC.1.1/ BASIC requires that the TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD.
SF.ACCESS.2 in the TOE configuration for use with Basic Inspection Systems only

- allows the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
- allows the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.1/PRIM requires that the TSF shall enforce the Primary Access Control SFP 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.

SF.ACCESS.1 in the TOE configuration for use with Primary Inspection Systems:
- allows only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,
- allows only the terminals to read the data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.2/ PRIM requires that 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.

SF.ACCESS.1 in the TOE configuration for use with Primary Inspection Systems:
- allows only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,
- allows only the terminals to read the data of the groups DG1 to DG16 of the logical MRTD

SF.ADMIN.10 realises the ability to write the data of the data groups DG1 to DG16 of the logical MRTD.
SF.AUTH.6 realises the ability to read the data of the groups DG1 to DG16 of the logical MRTD and therefore meets the above stated TOE SFR.

FDP_ACF.1.3/ PRIM requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
SF.ACCESS.1 in the TOE configuration for use with Primary Inspection Systems:
- allows only the successfully authenticated Personalization Agent to write the data of the data groups DG1 to DG16 of the logical MRTD,
- allows only the terminals to read the data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.4/ PRIM requires that 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.

SF.ACCESS.3 is not allowing the terminals to modify any of the data groups DG1 to DG16 of the logical MRTD and therefore meets the above stated TOE SFR.

FDP_ACF.1.1/ BASIC requires that the TSF shall enforce the Basic Access Control SFP to objects based on the following:
1. Subjects:
   a. Personalization Agent
   b. Primary Inspection System
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.

SF.ACCESS.2 in the TOE configuration for use with Basic Inspection Systems only
- allows the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
- allows the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.2/ BASIC requires that 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 and to read the 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.

SF.ACCESS.2 in the TOE configuration for use with Basic Inspection Systems only
- allows the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
- allows the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD

SF.ADMIN.10 realises the ability to write the data of the data groups DG1 to DG16 of the logical MRTD.
SF.AUTH.6 realises the ability to read the data of the groups DG1 to DG16 of the logical MRTD and therefore meets the above stated TOE SFR.

FDP_ACF.1.3/ BASIC requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
SF.ACCESS.2 in the TOE configuration for use with Basic Inspection Systems only
- allows the successfully authenticated Personalization Agent to write and read the data of the data groups DG1 to DG16 of the logical MRTD,
- allows the successfully authenticated Basic Inspection System to read data of the groups DG1 to DG16 of the logical MRTD

and therefore meets the above stated TOE SFR.

FDP_ACF.1.4/ BASIC requires that 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.

SF.ACCESS.3 is not allowing the terminals to modify any of the data groups DG1 to DG16 of the logical MRTD and therefore meets the above stated TOE SFR.

8.3.1.1.5 **FDP_UCT.1.1/ MRTD**, **FDP_UIT.1.1/ MRTD**

The Security Function TSF.PROTECTION (Protection of TSC) protects the TSF functionality, TSF data and user data.

FDP_UCT.1.1/ MRTD requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorised disclosure.
SF.PROTECTION.2 ensures that transmitted and received objects are protected from unauthorised disclosure and therefore meets the above stated TOE SFR.

FDP_UIT.1.1/ MRTD requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.
SF.PROTECTION.1 ensures that transmitted and received user data is protected from modification, deletion, insertion and replay errors and therefore meets the above stated TOE SFR.

FDP_UIT.1.2/ MRTD requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.
SF.PROTECTION.3 determines on receipt of user data if modification, deletion, insertion and replay has occurred and therefore meets the above stated TOE SFR.

8.3.1.1.6 **FMT_MOF.1.1** , **FMT_SMF.1.1** , **FMT_MTD.1.1/ INI_ENA** e.g.

The administration of the TOE is managed by TSF.ADMIN (Administration of the TOE).

FMT_MOF.1.1 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.
SF.ADMIN.3 enables and disables the TSF Basic Access Control only through the Personalization Agent. With enabled Basic Access Control secure messaging is enabled which enables to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred and therefore meets the above stated TOE SFR.

FMT_SMF.1.1 requires that the TSF shall be capable of performing the following security management functions:
1. Initialization,
2. Personalization
3. Configuration.

SF.ADMIN.4 assigns the security management functions: initialization, personalisation and configuration to the Manufacturer and Personalisation Agent and therefore meets the above stated TOE SFR.

FMT_SMR.1.1 requires that the TSF shall maintain the roles
1. Manufacturer,
2. Personalization Agent,
3. Primary Inspection System,
4. Basic Inspection System.
SF.ADMIN.9 maintains the security roles: Manufacturer, Personalization Agent, Primary Inspection System, Basic Inspection System and therefore meets the above stated TOE SFR.

FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles.
SF.ADMIN.9 maintains the security roles: Manufacturer, Personalization Agent, Primary Inspection System, Basic Inspection System and therefore meets the above stated TOE SFR.

FMT_LIM.1.1 requires that the TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.
SF.ADMIN.8 deploys Test Features after TOE Delivery that does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks and therefore meets the above stated TOE SFR.

FMT_LIM.2.1 requires that 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 User Data to be disclosed or manipulated TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.
SF.ADMIN.8 deploys Test Features after TOE Delivery that does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/ INI_ENA requires that the TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.
SF.ADMIN.5 has the ability to write the Initialization Data and Pre-personalization Data restricted to the Manufacturer and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/ INI_DIS requires that the TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.
SF.ADMIN.6 has the ability to disable read access for users to the Initialization Data restricted to the Personalization Agent and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/ KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

SF.ACCESS.5 has the ability to write the Initialization Data and Pre-personalization Data restricted to the Manufacturer and SF.ADMIN.7 has the ability to write the Document Basic Access Keys and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/ KEY_READ requires that the TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none.
SF.ACCESS.6 has the ability to disable read access for users to the Initialization Data restricted to the Personalization Agent and therefore meets the above stated TOE SFR.

8.3.1.1.7 **FPT_EMSEC.1.1** , **FPT_FLS.1.1** e.g.

SF.PROTECTION (Protection of TSC) protects the TSF functionality, TSF data and user data. and TSF.IC (Security Functions of the IC) covers the Security Functions of the IC.

FPT_EMSEC.1.1 requires that the TOE shall not emit information about IC power consumption and command execution time in excess of non useful information enabling access to Personalization Agent Authentication Key and logical MRTD data.
SF.PROTECTION.4 hides information about IC power consumption and command execution time, to ensure that the IC contacts VCC, GND and IO can not be used to gain access to Personalization Agent Authentication Key and logical MRTD data and therefore meets the above stated TOE SFR.

FPT_EMSEC.1.2 requires that the TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Authentication Key and logical MRTD data.
SF.PROTECTION.4 hides information about IC power consumption and command execution time, to ensure that the IC contacts VCC, GND and IO can not be used to gain access to Personalization Agent Authentication Key and logical MRTD data and therefore meets the above stated TOE SFR.

FPT_FLS.1.1 requires that 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.
SF.IC provides resistance to physical tampering of the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analysing and physical tampering and therefore meets the above stated TOE SFR.

FPT_TST.1.1 requires that the TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the condition Reset of the TOE to demonstrate the correct operation of the TSF.
SF.PROTECTION.5 demonstrates the correct operation of the TSF and therefore meets the above stated TOE SFR.

FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data.
SF.PROTECTION.5 demonstrates the correct operation of the TSF and therefore meets the above stated TOE SFR.

FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.
SF.PROTECTION.5 demonstrates the correct operation of the TSF and therefore meets the above stated TOE SFR.

FPT_PHP.3.1 requires that the TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the TSP is not violated.
SF.IC provides detection of physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation and therefore meets the above stated TOE SFR.

FPT_RVM.1.1 requires that the TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
SF.PROTECTION.6 provides the invocation of TSP enforcement functions. After succeeding each function within the TSC is allowed to proceed and therefore meets the above stated TOE SFR.

FPT_SEP.1.1 requires that the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

SF.PROTECTION.7 maintains a security domain for the TSF execution that protects it from interference and tampering by untrusted subjects and therefore meets the above stated TOE SFR.

FPT_SEP.1.2 requires that the TSF shall enforce separation between the security domains of subjects in the TSC.
SF.PROTECTION.8 enforces separation between the security domains of subjects in the TSC and therefore meets the above stated TOE SFR.

8.3.2 Rationale for Assurance Measures

The following table demonstrates the coverage of the Assurance Requirements by the Assurance measures by indicating the correspondence with crosses.

Assurance Requirements / Assurance Measures	**AM_ACM**	**AM_ADO**	**AM_ADV**	**AM_AGD**	**AM_ALC**	**AM_ATE**	**AM_AVA**
ACM	**X**						
ADO		**X**					
ADV			**X**				
AGD				**X**			
ALC					**X**		
ATE						**X**	
AVA							**X**

Table 11 Assurance Requirements to Assurance Measures mapping

8.4 Rationale for PP Claims

Since the ST security objectives and requirements are identical to those of the claimed PP [21a], this part of the ST is omitted.

9 Appendix

9.1 Glossary and Acronyms

Term	Definition
Active Authentication	Security mechanism defined in [7] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [7] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [8]
biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [8]
Country Signing CA Certificate C_{CSCA})	Self-signed certificate of the Country Signing CA Public Key (K_{PuCSCA}) issued by CSCA stored in the inspection system.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [7]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}). [7]
Eavesdropper	A threat agent with low attack potential reading the communication between the

Term	Definition
	MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [9]
Extended Access Control	Security mechanism identified in [7] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [8]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [9]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [8]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [9]
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the nonvolatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity. [9]
Inspection system IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.

Term	Definition
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit. *Integrity* Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [6]
Issuing State	The Country issuing the MRTD. [6]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology. [6] The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [6] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder (1) the digital Machine Readable Zone Data (digital MRZ data, DG1), (2) the digitized portraits (DG2), (3) the biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both and (4) the other data according to LDS (DG5 to DG16).
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [6]
Machine readable visa (MRV)	A visa or, where appropriate, an entry clearance (herein after collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visapage in a passport. [6]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [6]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [8]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes

Term	Definition
	- the file structure implementing the LDS [6], - the definition of the User Data, but does not include the User Data itself (i.e. content of DG1 to DG14 and DG 16) and - the TSF Data including the definition the authentication data but except the authentication data itself (i.e. Active Authentication Key pair and Document Basic Access Key).
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [10], p. 14.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. [8]
Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent. It may be (i) a symmetric cryptographic Personalization Agent Authentication Secret Key or (ii) pair of asymmetric keys, i.e. the Personalization Agent Authentication Private Key and the Personalization Agent Authentication Public Key.
Personalization Agent Authentication Private Key	Asymmetric cryptographic key used by the Personalization Agent to prove their identity and get access to the logical MRTD, TSF data for TSF required by the SFR FIA_API.1/MAM_PT
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and

Term	Definition
	(4) other data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
***Primary Inspection System* (PIS)**	A inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
Receiving State	The Country to which the MRTD holder is applying for entry. [6]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [8]
secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel. [9]
traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
unpersonalized MRTD	MRTD material prepared to produce an personalized MRTD containing an initialised and pre-personalized MRTD's chip.
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. [9]
verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

9.2 Acronyms

Acronym	Term
BIS	Basic Inspection System
CC	Common Criteria
OSP	Organisational security policy
PIS	Primary Inspection System
PT	Personalization Terminal
SAR	Security assurance requirements
SFP	Security Function Policy
SFR	Security functional requirement
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSP	TOE Security Policy
TSF	TOE security functions

9.3 References

Common Criteria	
[1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1, August 1999
[2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1, August 1999
[3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1, August 1999
[4]	Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999
[5]	Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik
[5a]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2.12.199
ICAO	
[6]	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
[7]	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
[8]	ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003
[9]	BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS,

	TECHNICAL REPORT Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 1.9, ICAO TAG MRTD/NTWG, 19 May 2003
[10]	INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)
[11]	Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version – 0.42 - Draft, August, 2004, Dr. Kügler, BSI
Cryptography	
[12]	Geeignete Kryptoalgorithmen In Erfüllung der Anforderungen nach §17 (1) SigG vom 22. Mai 2001 in Verbindung mit Anlage 1, I 2, SigV vom 22. November 2001, Bundesanzeiger Nr. 30, S.2537-2538, 13.02.04.
[13]	ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999
[14]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
[15]	Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[16]	Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[17]	Certicom Research: SEC 1: Elliptic Curve Cryptography, September 20, 2000, Version 1.0
[18]	AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©,September 20, 1998
[19]	ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002
Protection Profiles	
[20]	PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001
[21]	Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002
[21a]	Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control, Version 1.0, 18.08.2005, BSI-PP-0017, Bundesamt für Sicherheit in der Informationstechnik
Sonstige	
[22]	Dennis Kügler: „Advanced Security Mechanisms for Machine Readable Travel Documents”, Version 0.7, BSI, presented 1.12.2004
[23]	ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004
[24]	Certification Report Philips P5CT072, to be specified, after completion of HW evaluation

-End of Document-