Security Target Lite STARCOS 3.3 Passport Edition Version 2.0a

Version 1.0 / Status 19.08.2008

Author G&D/CSOP43
Status Released

F&E

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

Contents

1 Introduction 6
1.1 ST Identification 6
1.2 ST Overview 6
1.3 CC Conformance 7
1.4 Change History 7
1.5 Tables 7
1.6 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 11
2.3.1 Phase 1 “Development” 11
2.3.2 Phase 2 “Manufacturing” 12
2.3.3 Phase 3 “Personalization of the MRTD” 12
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 15
3.2.1 A.Pers_Agent Personalization of the MRTD’s chip 15
3.2.2 A.Insp_Sys Inspection Systems for global interoperability 15
3.2.3 A.Signature_PKI PKI for Passive Authentication 15
3.2.4 A.Auth_PKI PKI for Inspection Systems 16
3.3 Threats 16
3.3.1 T.Chip_ID Identification of MRTD’s chip 16
3.3.2 T.Skimming Skimming the logical MRTD 16
3.3.3 T.Read_Sensitive_Data Read the sensitive biometric reference data 17
3.3.4 T.Forgery Forgery of data on MRTD’s chip 17
3.3.5 T.Counterfeit MRTD’s chip 17
3.3.6 T.Abuse-Func Abuse of Functionality 17
3.3.7 T.Information_Leakage Information Leakage from MRTD’s chip 18
3.3.8 T.Phys-Tamper Physical Tampering 18
3.3.9 T.Malfunction Malfunction due to Environmental Stress 18
3.4 Organisational Security Policies 19
3.4.1 P.Manufact Manufacturing of the MRTD’s chip 19
3.4.2 P.Personalization Personalization of the MRTD by issuing State or Organization only 19
3.4.3 P.Personal_Data Personal data protection policy 19
3.4.4 P.Sensitive_Data Privacy of sensitive biometric reference data 19
3.5 Security Objectives 20
3.5.1 Security Objectives for the TOE 20
3.5.2 Security Objectives for the Development and Manufacturing Environment 22
3.5.3 Security Objectives for the Operational Environment 23
4 Extended Components Definition 25
4.1 Definition of the Family FAU_SAS 25
4.1.1 FAU_SAS Audit data storage 25
4.1.2 FAU_SAS.1 Audit storage 25
4.2 Definition of the Family FCS_RND 25
4.2.1 FCS_RND Generation of random numbers 26
4.3 Definition of the Family FIA_API 26

4.3.1 FIA_API Authentication Prove of Identity ... 26
4.4 Definition of the Family FMT_LIM ... 27
4.4.1 FMT_LIM Limited capabilities and availability ... 27
4.5 Definition of the Family FPT_EMSEC ... 28
4.5.1 FPT_EMSEC.1 TOE Emanation ... 29
5 Security Requirements ... 30
5.1 Security Functional Requirements for the TOE ... 32
5.1.1 Class FAU Security Audit ... 32
5.1.2 Class Cryptographic Support (FCS) ... 32
5.1.3 Class FIA Identification and Authentication ... 36
5.1.4 Class FDP User Data Protection ... 40
5.1.5 Class FMT Security Management ... 43
5.1.6 Class FPT Protection of the Security Functions ... 49
5.2 Security Assurance Requirements for the TOE ... 52
5.2.1 TOE Security Assurance Requirements ... 52
5.3 Security Requirements for the IT environment ... 52
5.3.1 Passive Authentication ... 52
5.3.2 Extended Access Control PKI ... 53
5.3.3 Basic Terminal ... 54
5.3.4 General Inspection System ... 58
5.3.5 Extended Inspection System ... 61
5.3.6 Personalization Terminals ... 62
6 TOE Summary Specification ... 64
6.1 TOE Security Functions ... 64
6.1.1 SF.ACCESS (Access Control) ... 64
6.1.2 SF.ADMIN (Administration of the TOE) ... 65
6.1.3 SF.AUTH (Authentication of the authorized TOE user) ... 66
6.1.4 SF.CRYPTO (Cryptographic Support) ... 67
6.1.5 SF.PROTECTION (Protection of TSC) ... 67
6.1.6 SF.IC (Security Functions of the IC) ... 68
6.2 Assurance Measures ... 68
7 PP Claims ... 70
7.1 PP Reference ... 70
7.2 PP Additions ... 70
8 Rationale ... 71
8.1 Security Objectives Rationale ... 71
8.2 Security Requirements Rationale ... 75
8.2.1 Security Functional Requirements Rationale ... 75
8.2.2 Dependency Rationale ... 83
8.2.3 Security Assurance Requirements Rationale ... 93
8.2.4 Security Requirements – Mutual Support and Internal Consistency ... 94
8.2.5 Rationale for Strength of Function High ... 95
8.3 Rationale for TOE Summary Specification ... 95
8.3.1 Rationale for TOE Security Functions ... 95
8.3.2 Rationale for Assurance Measures ... 109
8.4 Rationale for PP Claims ... 109
8.5 Statement of compatibility ... 110
8.5.1 Classification of Platform TSFs ... 110
8.5.2 Matching statement ... 111
9 Appendix ... 117
9.1 Glossary and Acronyms ... 117
9.2 Acronyms ... 122

9.3 References 123

1 Introduction

1.1 ST Identification

Title: Security Target Lite STARCOS 3.3 Passport Edition Version 2.0a
Reference: GDM_STA33_MRTD_ ASE_00
Version Number/Date: Version 1.0 / Status 19.08.2008
Origin: Giesecke & Devrient GmbH
Author: Jan Eichholz
Compliant to: Common Criteria Protection Profile — Machine Readable Travel Document with ICAO Application, Extended Access Control (PP-MRTD EAC), Version 1.2, 19.11.2007, BSI-PP-0026 [21a]
TOE name: Security Target Lite STARCOS 3.3 Passport Edition Version 2.0a
TOE version: 2.0a
TOE documentation:
- Administrator Guidance [27]
- User Guidance [28]
- STARCOS33PETABLES [29]

HW-Part of TOE: NXP P5CD080V0B (BSI-DSZ-CC-0410-2007) [24]

1.2 ST Overview

The aim of this document is to describe the Security Target for STARCOS 3.3 Passport Edition Version 2.0a for Passport Booklet IC.

The related product is the STARCOS 3.3 Passport Edition Version 2.0a 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 3.3 Passport Edition Version 2.0a fulfils the requirements specified in [5].

STARCOS 3.3 Passport Edition Version 2.0a is a fully interoperable ISO 7816 compliant multi-application Smart Card OS, including a cryptographic library enabling the user to apply TDES and ECDH (compliant to ISO 15946).
Additionally to BSI-PP-0026 [21a] the STARCOS 3.3 Passport Edition Version 2.0a supports the Active Authentication mechanism [7].

The software part of the TOE is implemented on the IC NXP P5CD080V0B 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 V2.3 (ISO 15408) (see [1], [2], [3])

as follows:
- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2 and ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

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

1.4 Change History

Version	Date	Changes	Remarks
1.0	19.08.08	Final Version	eij

1.5 Tables

Table 1 Overview on authentication SFR 37
Table 2 Assurance Requirements: EAL (4+) 52
Table 3 SOF claims for TOE Security Functions 64
Table 4 References of Assurance Measures 69
Table 5 Security Objective Rationale 72
Table 6 Coverage of Security Objective for the TOE by SFR 76
Table 7 Coverage of Security Objectives for the IT environment by SFR 81
Table 8 Dependencies between the SFR for the TOE 87
Table 9 Dependencies between the SFR for the IT environment 92
Table 10 Functional Requirements to Security Function mapping 97
Table 11 Assurance Requirements to Assurance Measures mapping 109
Table 12 Classification of Platform-TSFs 111
Table 13 Mapping of threats 111
Table 14 Mapping of assumptions 112
Table 15 Mapping of objectives 113
Table 16 Mapping of SFRs 115

1.6 Application Notes of the PP

When applicable the application notes of the PP are discussed in notes.

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 and the Extended Access Control according to the ICAO document [7] and the technical report [25].

The TOE comprises of

- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antenna, 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
- the associated guidance documentation Administrator Guidance [27], User Guidance [28], STARCOS33PETABLES [29] and
- the GMA Verifier[1] [30].

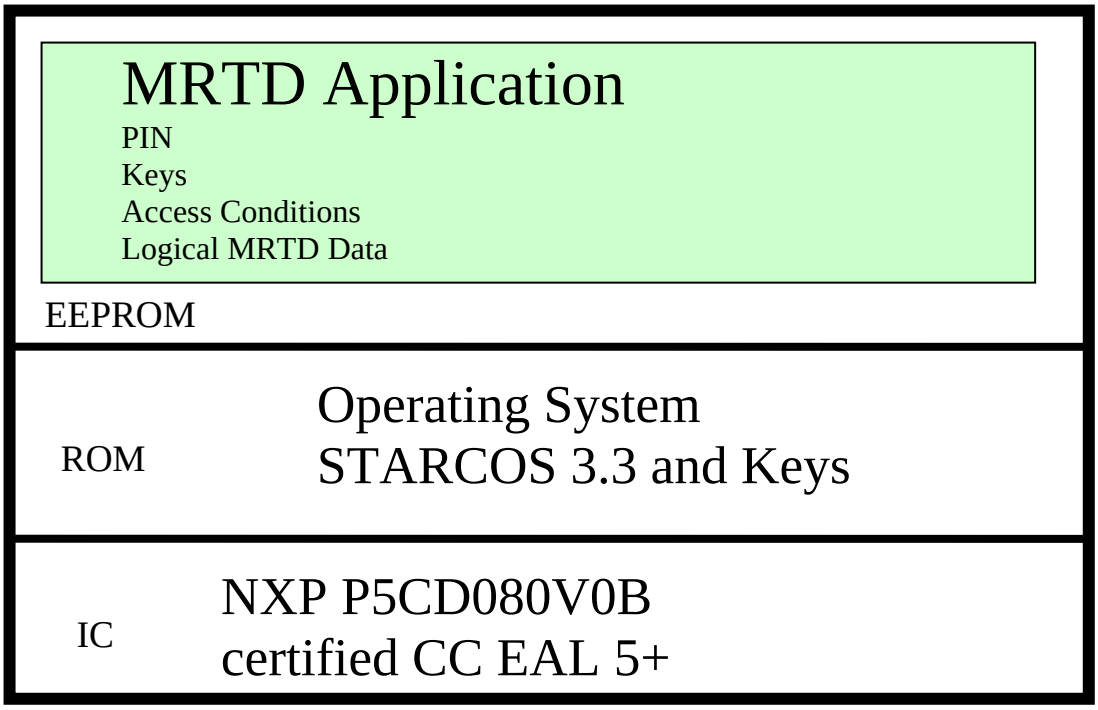


Figure 1 TOE description

[1] The GMA Verifier is not part of the TOE delivery. It is solely used by the MRTD Manufacturer for the correct installation of the TOE and therefore of no use for the Personalisation Agent.

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 trusts a genuine MRTD of an 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, EF.DG1),
(2) the digitized portraits (EF.DG2),
(3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[2]
(4) the other data according to LDS (EF.DG5 to EF.DG16) and
(5) the Document security object.

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

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and 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.

[2] These additional biometric reference data are optional according to [7]. This ST assumes that the issuing State or Organization uses this option and protects these data by means of extended access control.

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 write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism and the Extended Access Control Mechanism. This security target addresses the Chip Authentication described in [25] as an alternative to the Active Authentication stated in [7].

The Basic Access Control is a security feature that shall be mandatory implemented by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [7], Annex E, and [6].

The security target requires the TOE to implement the Chip Authentication defined in [25] and additionally the Active Authentication described in [7]. Both protocols provide evidence of the MRTD's chip authenticity where the Chip Authentication prevents data traces described in [7], Annex G, section G.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates a ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. it could apply the Chip Authentication Private Key corresponding to the Chip Authentication Public Key for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The security target requires the TOE to implement the Extended Access Control as defined in [25]. The Extended Access Control consists of two parts (i) a Terminal Authentication Protocol to authenticate the inspection system as entity authorized by the Issuing State or Organization through the receiving State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. It requires the Chip Authentication of the MRTD's chip to the inspection system and uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. The issuing State or Organization authorizes the receiving State by

means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

2.3 TOE life cycle

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

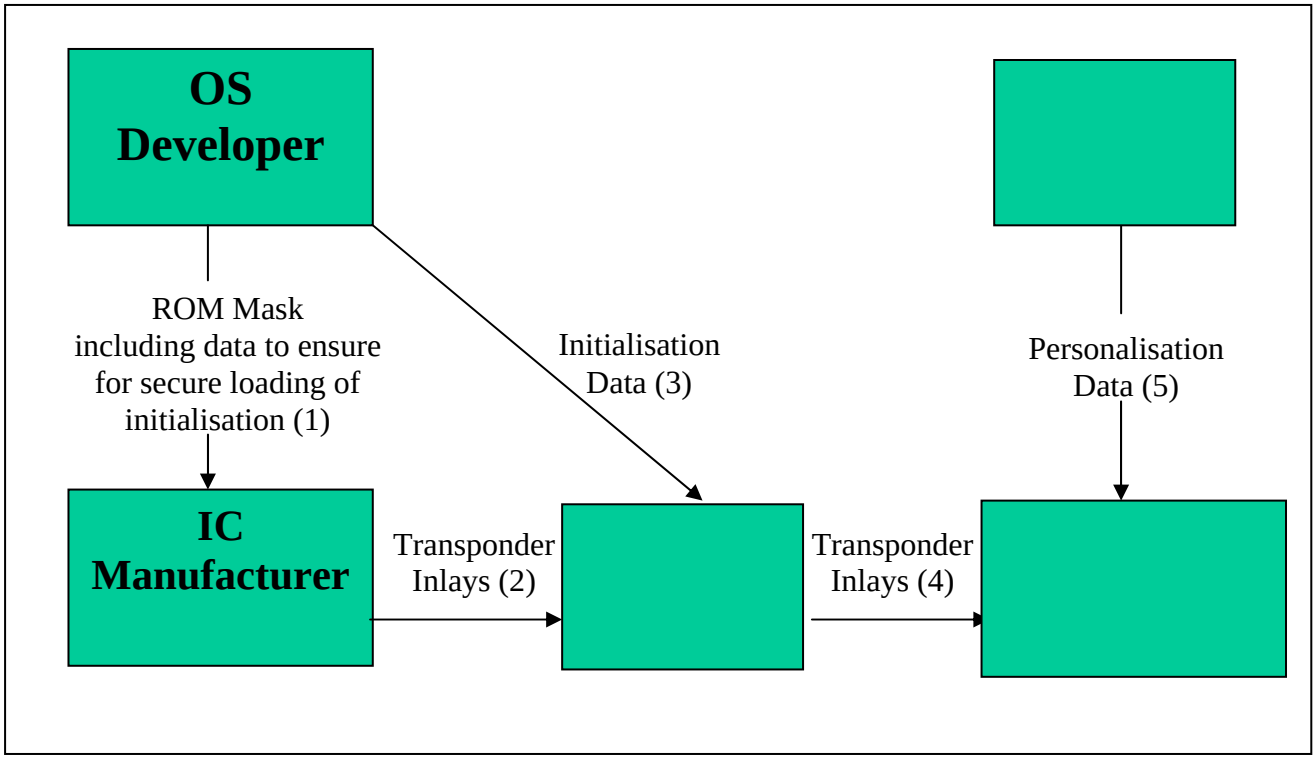


Figure 2 ROM Mask generation and delivery and Initialisation/Personalisation (example)

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.
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.

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 1: The authorized Personalization Agents is not allowed to add and modify data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 "Operational Use".

Note 2: The point of TOE delivery according to CC in this ST and therefore the split up of P.Manufact and P.Personalization is after phase 2. The secure transfer of the TOE between the manufacturer and the personalisation site has to be realised. Note: In many cases security aspects for phase 3 are defined and controlled by the issuing state or organisation.

3 Security Problem Definition

This chapter has been taken from [21a] with minor modifications by adding the Active Authentication mechanism indicated by underlined and bold text..

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 EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [6]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD. The Active Authentication public key is stored in EF.DG 15.

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

n 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 proof his possessing of 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 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, (iv) writing the initial TSF data and and (iv) signing the Document Security Object defined in [6].

3.1.2.3 Country Verifying Certification Authority

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

3.1.2.4 Document Verifier

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

3.1.2.5 Terminal

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

3.1.2.6 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. The **Basic Inspection System** (BIS) (i) contains a terminal for the contactless communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. Optionally, a BIS may supports Active Authentication. The **General Inspection System** (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism. The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

Note 3: The TOE does not allow the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems as described in the BSI-PP-0017 Machine Readable Travel Document with „ICAO Application", Basic Access Control.

3.1.2.7 MRTD Holder

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

3.1.2.8 Traveller

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

3.1.2.9 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 Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, (iv) the Active Authentication Public Key if stored on the MRTD's chip and (v) 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 Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [7]. The Basic Inspection System reads the logical MRTD being under Basic Access Control and performs the Passive Authentication to verify the logical MRTD. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

3.2.3 A.Signature_PKI PKI for Passive Authentication

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical

MRTD. The issuing State or Organization runs a Certification Authority (CA) which (i) securely generates, stores and uses the Country Signing CA Key pair, and (ii) manages the MRTD's Chip Authentication Key Pairs. The CA keeps the Country Signing CA Private Key secret and distributes the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and organizations.

3.2.4 A.Auth_PKI PKI for Inspection Systems

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

3.3 Threats

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

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

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 cannot read optically and does not know in advance the physical MRTD.

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 physical MRTD.

3.3.3 T.Read_Sensitive_Data Read the sensitive biometric reference data

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

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

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 holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the 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 MRTDs to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveller into an other MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD in another contactless chip.

3.3.5 T.Counterfeit MRTD's chip

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

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

The TOE shall avert the threat as specified below.

3.3.6 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.

3.3.7 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).

3.3.8 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.

3.3.9 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 these vulnerabilities an attacker needs information about the functional operation.

3.4 Organisational Security Policies

The TOE shall comply with 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 (EF.DG1), the printed portrait and the digitised portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an inspection system. Additional to the Basic Access Control Authentication defined by ICAO in [7] the MRTD's chip shall protect the confidentiality and integrity of the personal data during transmission to the General Inspection System after Chip authentication.

Note 4: 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.

3.4.4 P.Sensitive_Data Privacy of sensitive biometric reference data

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the MRTD holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the

time the MRTD is presented to the inspection system. The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate.

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 may be written only during and cannot be changed after its personalisation. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

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

3.5.1.3 OT.Data_Conf Confidentiality of personal data

The TOE must ensure the confidentiality of the data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 and the Document Security Object of the logical MRTD by granting read access to terminals successfully authenticated by as (i) Personalization Agent or (ii) Basic Inspection System or (iii) Extended Inspection System. The TOE implements the Basic Access Control as defined by ICAO [7] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

3.5.1.4 OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized inspection systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the

Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

3.5.1.5 OT.Identification Identification and Authentication of the TOE

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

3.5.1.6 OT.Chip_Auth_Proof Proof of MRTD’S chip authenticity

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD’s chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [25] The authenticity prove provided by MRTD’s chip shall be protected against attacks with high attack potential.
The following TOE security objectives address the protection provided by the MRTD’s chip independent on the TOE environment.

3.5.1.7 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.

3.5.1.8 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.

3.5.1.9 OT.Prot_Phys-Tamper Protection against Physical Tampering

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD’s chip Embedded Software. This includes protection against attacks with 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.

3.5.1.10 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.

3.5.1.11 OT.Active_Auth_Proof Proof of MRTD'S chip authenticity

The TOE shall support the Basic Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [7]. The authenticity prove provided by MRTD's chip shall be protected against attacks with high attack potential.

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

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, initialise, pre-personalize genuine MRTD's materials and to personalize authentic MRTDs in order to prevent counterfeit of MRTDs 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 behalf of the issuing State or Organisation (i) establish the correct identity of the holder and create biographical 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 to protect the confidentiality and integrity of these data.

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 CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and organizations maintaining its authenticity and integrity. The Issuing State or organization must (i) generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signing Public Key to receiving States and organizations. The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [6].

3.5.3.1.3 OE.Auth_Key_MRTD MRTD Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

3.5.3.1.4 OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

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

3.5.3.1.5 OE.Active_Auth_Key_MRTD MRTD ActiveAuthentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in

EF.DG15 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

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. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [7]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

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 or Organisation ensures the confidentiality and integrity of the data read from the logical MRTD. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

3.5.3.2.4 OE.Ext_Insp_Systems Authorisation of Extended Inspection Systems

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

4 Extended Components Definition

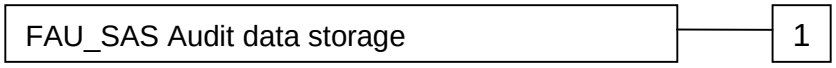
This security target uses components defined as extensions to CC part 2 [2]. Some of these components are defined in [20], other components are defined in [21a].
This chapter has been taken from [21a] with minor modifications.

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.

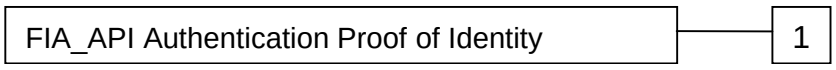
FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].
Dependencies: No dependencies.

4.3 Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. 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.

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.

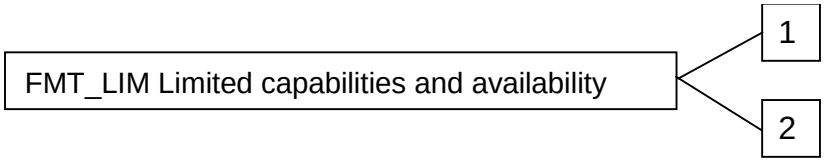
4.4 Definition of the Family FMT_LIM

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 lifecycle.

Management: FMT_LIM.1, FMT_LIM.2
There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2
There are no actions defined to be auditable.

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.

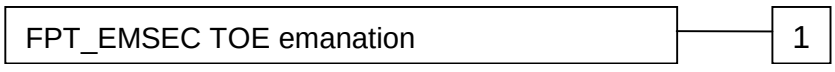
FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].

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[3].

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.

The following table provides an overview of the keys and certificates used:

Name	Data
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying	The Country Verifying Certification Authority Certificate

[3] The assignmemts 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).

Name	Data
Certification Authority Certificate (C_{CVCA})	may be a self-signed certificate or a link certificate (cf. [25] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the Issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by Receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the Issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the Receiving State or organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for

Name	Data
	mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.
Active Authentication Public Key Pair	The Active Authentication Key Pair ($SKAA_{ICC}$, $PKAA_{ICC}$) are used for the Active Authentication mechanism according to [7].
Active Authentication Public Key ($PKAA_{ICC}$)	The Active Authentication Public Key ($PKAA_{ICC}$) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Active Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Active Authentication Private Key ($SKAA_{ICC}$)	The Active Authentication Private Key ($SKAA_{ICC}$) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.

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 (Common Criteria Part 2 extended).

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

FAU_SAS.1.1
The TSF shall provide the Manufacturer[4] with the capability to store the IC Identification Data[5] in the audit records.

Dependencies: No dependencies.

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

[4] [assignment: authorised users]

[5] [assignment: list of audit information]

cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

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

Hierarchical to: No other components.

FCS_CKM.1.1/ KDF_MRTD
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[6] and specified cryptographic key sizes 112 bit[7] that meet the following: [7], Annex E.[8]

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

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

Hierarchical to: No other components.

FCS_CKM.1.1/DH_MRTD
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: ECDH compliant to ISO 15946, Document Basic Access Key Derivation and specified cryptographic key sizes 192 bit – 320 bit, 112 bit that meet the following: **[25],** Annex A.1[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.

[6] [assignment: cryptographic key generation algorithm]

7 [assignment: cryptographic key sizes]

8 [assignment: list of standards]

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

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

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

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].

[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]

Dependencies:
[FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC
Hierarchical to: No other components.

FCS_COP.1.1/MAC_MRTD
The TSF shall perform secure messaging – message authentication code[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
FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD

Hierarchical to: No other components.

FCS_COP.1.1/SIG_VER
The TSF shall perform digital signature verification [22] in accordance with a specified cryptographic algorithm ECDSA with SHA-1, SHA-224, SHA-256 and cryptographic key sizes: 192 bit – 320 bit that meet the following: ISO 15946-2, FIPS PUB 180-2.

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/RSA_MRTD Cryptographic operation – Signature creation by MRTD

Hierarchical to: No other components.

FCS_COP.1.1/RSA_MRTD

[18] [assignment: list of cryptographic operations]

[19] [assignment: cryptographic algorithm]

[20] [assignment: cryptographic key sizes]

[21] [assignment: list of standards]

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

The TSF shall perform digital signature creation [23] in accordance with a specified cryptographic algorithm RSA with SHA-1 and cryptographic key sizes: 1024 - 4000 bit that meet the following: scheme 1 of ISO/IEC 9796-2:2002 [19].

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.2.2 Random Number Generation (FCS_RND.1)

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

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

FCS_RND.1.1/ MRTD
The TSF shall provide a mechanism to generate random numbers that meet the requirements for SOF high defined in AIS 20 [5a].

Dependencies: No dependencies.

5.1.3 Class FIA Identification and Authentication

Note 5: The Table 1 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [7], Annex E, and [22]
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys
Basic Access Control Authentication Mechanism	FIA_AFL.1, FIA_UAU.4/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/BT, FIA_UAU.6/BT	Triple-DES, 112 bit keys and Retail-MAC, 112 bit keys
Chip Authentication Protocol	FIA_API.1/MRTD, FIA_UAU.5/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/GIS, FIA_UAU.5/GIS, FIA_UAU.6/GIS	ECDH and Retail-MAC, 112 bit keys
Terminal	FIA_UAU.5/MRTD	FIA_API.1/EIS	RSASSA-PKCS1-

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

Authentication Protocol			v1_5 or EC-DSA with SHA
Active Authentication Mechanism	FIA_API.1/AA	FIA_UAU.4/BT	RSA with 1024 - 4000 bits. Algorithm according to [7], Annex D

Table 1 Overview on authentication SFR

Note the Chip Authentication Protocol include the asymmetric key agreement and the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

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

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

FIA_UID.1.1

The TSF shall allow

(1) to establish the communication channel,
(2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[24]

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

FIA_UID.1.2
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

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

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.

FIA_UAU.1.1
The TSF shall allow

1. to establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
3. to identify themselves by selection of the authentication key [25]

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

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

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. Terminal Authentication Protocol,
3. Authentication Mechanism based on Triple-DES [26].

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/MRTD Multiple authentication mechanisms
Hierarchical to: No other components.

FIA_UAU.5.1/MRTD
The TSF shall provide
1. Basic Access Control Authentication Mechanism,
2. Terminal Authentication Protocol,
3. Secure messaging in MAC-ENC mode,
4. Symmetric Authentication Mechanism based on Triple-DES [27]

to support user authentication.

FIA_UAU.5.2/MRTD
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 Personalization Agent Keys,
(b) the Symmetric Authentication Mechanism with Personalization Agent Key,
(c) the Terminal Authentication Protocol with Personalization Agent Keys.

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

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

2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
3. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging with the key agreed upon with the authenticated terminal by means of the Basic Access Control Authentication Mechanism.
4. After run of the Chip Authentication Mechanism the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism.[28].

Dependencies: No dependencies.

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

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

Hierarchical to: No other components.

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

1. Each command sent to the TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS.
2. Each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS. [29]

Dependencies: No dependencies.

Authentication failure handling (FIA_AFL.1)

Hierarchical to: No other components.

FIA_AFL.1.1
The TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 unsuccessful authentication attempts occur related to a BAC authentication protocol.

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

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

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall wait for an administrator configurable time greater 1 second between receiving the terminal challenge e_{IFD} and sending the TSF response e_{ICC} during the BAC authentication attempts.

Dependencies: FIA_UAU.1 Timing of authentication

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

FIA_API.1/CAP Authentication Proof of Identity - MRTD

Hierarchical to: No other components.

FIA_API.1.1/CAP
The TSF shall provide a Chip Authentication Protocol according to [25] [30] to prove the identity of the TOE[31].

Dependencies: No dependencies.

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

FIA_API.1/AA Authentication Proof of Identity - MRTD

Hierarchical to: No other components.

FIA_API.1.1/AA
The TSF shall provide a Active Authentication Mechanism according to [7] [32] to prove the identity of the TOE[33].

Dependencies: No dependencies.

5.1.4 Class FDP User Data Protection

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

5.1.4.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

[30] [assignment: *authentication mechanism*]

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

[32] [assignment: *authentication mechanism*]

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

FDP_ACC.1.1
The TSF shall enforce the Access Control SFP[34] on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD[35].

Dependencies: FDP_ACF.1 Security attribute based access control

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

5.1.4.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attributes based access control

Hierarchical to: No other components.

FDP_ACF.1.1
The TSF shall enforce the Access Control SFP[36] to objects based on the following:

1. Subjects:
   a. Personalization Agent,
   b. Basic Inspection System,
   c. Extended Inspection System
   d. Terminal,
2. Objects:
   a. data EF.DG1 to EF.DG16 of the logical MRTD,
   b. data in EF.COM,
   c. data in EF.SOD,
3. Security attributes:
   a. authentication status of terminals,
   b. Terminal Authorization [37].

FDP_ACF.1.2

[34] [assignment: access control SFP]

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

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

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

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

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
3. the successfully authenticated Extended Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
4. the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG3 according to the Terminal Authorization,
5. the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG4 according to the Terminal Authorization [38].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[39].

FDP_ACF.1.4

1. The TSF shall explicitly deny access of subjects to objects based on the rule: A terminal authenticated as CVCA is not allowed to read to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,
5. the Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD [40].

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

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

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

FDP_UCT.1.1/ MRTD

The TSF shall enforce the Access Control SFP[41] to be able to transmit and receive[42] objects in a manner protected from unauthorised disclosure **after Chip Authentication**..

---

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

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

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

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 Access Control SFP[43] to be able to transmit and receive[44] user data in a manner protected from modification, deletion, insertion and replay[45] errors **after Chip Authentication**.

FDP_UIT.1.2/ MRTD
The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[46] has occurred **after Chip Authentication**.

Dependencies:

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

5.1.5 Class FMT Security Management

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

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

FMT_SMF.1.1
The TSF shall be capable of performing the following security management functions:
1. Initialization,
2. Personalization
3. Configuration[47].

Dependencies: No Dependencies

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

[42] [selection: transmit, receive]

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

[44] [selection: transmit, receive]

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

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

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

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

FMT_SMR.1 Security roles
Hierarchical to: No other components.

FMT_SMR.1.1
The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifier Certification Authority,
4. Document Verifier,
5. Basic Inspection System,
6. domestic Extended Inspection System
7. foreign Extended Inspection System [48].

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

Hierarchical to:
FIA_UID.1 Timing of identification.

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[49].

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).

[48] [assignment: *the authorised identified roles*]

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

FMT_LIM.2 Limited availability
Hierarchical to: No other components.

FMT_LIM.2.1
The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow
1. User Data to be disclosed or manipulated
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[50].

Dependencies: FMT_LIM.1 Limited capabilities.

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" a 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[51] the Initialization Data and Pre-personalization Data[52] to the Manufacturer[53].

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[54] the Initialization Data[55] to the Personalization Agent[56].

Dependencies:

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

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

[52] [assignment: list of TSF data]

[53] [assignment: the authorised identified roles]

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

[55] [assignment: list of TSF data]

[56] [assignment: the authorised identified roles]

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/CVCA_INI
The TSF shall restrict the ability to write [57] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifier Certification Authority Certificate,
3. initial Current Date [58]

to the Personalization Agent.

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/CVCA_UPD
The TSF shall restrict the ability to update [59] the

1. Country Verifier Certification Authority Public Key,
2. Country Verifier Certification Authority Certificate [60]

to Country Verifier Certification Authority [61].

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

FMT_MTD.1/DATE Management of TSF data – Current date

Hierarchical to: No other components.

FMT_MTD.1.1/DATE

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

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

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

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

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

The TSF shall restrict the ability to modify [62] the Current date [63] to

1. Country Verifier Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System [64].

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
The TSF shall restrict the ability to write[65] the Document Basic Access Keys[66] to the Personalization Agent[67].
Dependencies:
ADV_SPM.1 Informal TOE security policy model
FMT_MTD.1 Management of TSF data

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

Hierarchical to: No other components.

FMT_MTD.1.1/CAPK
The TSF shall restrict the ability to create and load [68] the Chip Authentication Private Key [69] to the Manufacturer and the Personalisation Agent.

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

FMT_MTD.1/AAPK Management of TSF data – Active Authentication Private Key

Hierarchical to: No other components.

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

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

[64] [assignment: *the authorised identified roles*]

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

[66] [assignment: list of TSF data]

[67] [assignment: the authorised identified roles]

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

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

FMT_MTD.1.1/AAPK
The TSF shall restrict the ability to create and load [70] the Active Authentication Private Key [71] to the Manufacturer and the Personalisation Agent.

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 [72] the

1. Document Basic Access Keys,
2. Chip Authentication Private Key,
3. Personalization Agent Keys [73]
4. Active Authentication Private Key

to none [74].

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

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

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

Dependencies:
ADV_SPM.1 Informal TOE security policy model

FMT_MTD.1 Management of TSF data

Refinement: The certificate chain is valid if and only if

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

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

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

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

[74] [assignment: *the authorised identified roles*]

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

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

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

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

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

5.1.6 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information flow for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFR “Non-bypassability of the TSP (FPT_RVM.1)” and “TSF domain separation (FPT_SEP.1)” together with “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below (Common Criteria Part 2 extended):

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[75] and logical MRTD data.

FPT_EMSEC.1.2

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

The TSF shall ensure any users[76] are unable to use the following interface smart card circuit contacts[77] to gain access to Personalization Agent Authentication Key and Chip Authentication Private Key [78] and logical MRTD data and Active Authentication Private Key.

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[79].

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.

[76] [assignment: type of users]

[77] [assignment: type of connection]

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

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

Dependencies:
FPT_AMT.1 Abstract machine testing.

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[80] to the TSF[81] 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.

[80] [assignment: physical tampering scenarios]

[81] [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, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

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, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 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.3 AVA_SOF.1 AVA_VLA.4

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 (EF.DG1 to EF.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 (EF.DG1 to EF.DG16) and the Document Security Object[82].

FDP_DAU.1.2/ DS
The **Document Signer** shall provide Inspection Systems of Receiving States or Organization[83] with the ability to verify evidence of the validity of the indicated information.

Dependencies: No dependencies

5.3.2 Extended Access Control PKI

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

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

Hierarchical to: No other components.

FCS_CKM.1.1/PKI
The PKI shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: ECDSA and specified cryptographic key sizes 192 bit – 320 that meet the following: [25], Annex A [84].

Dependencies:
[FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]

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

[83] [assignment: list of subjects]

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

FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/CERT_SIGN Cryptographic operation – Certificate Signing

Hierarchical to: No other components.

FCS_COP.1.1/CERT_SIGN
The PKI shall perform digital signature creation [85] in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 192 bit – 320 bit that meet the following: TR-03111 Ver. 1.0 [25].

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.3.3 Basic Terminal

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

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

FCS_CKM.1/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[86] and specified cryptographic key sizes 112 bit[87] that meet the following: [7], Annex E[88].

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

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

[86] [assignment: cryptographic key generation algorithm]

87 [assignment: cryptographic key sizes]

[88] [assignment: list of standards]

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[89] in accordance with a specified cryptographic algorithms SHA-1[90] and cryptographic key sizes none[91] that meet the following: FIPS 180- 2[92].

Dependencies:
[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal
Hierarchical to: No other components.

FCS_COP.1.1/ ENC_BT

[89] [assignment: list of cryptographic operations]

[90] [assignment: cryptographic algorithm]

[91] [assignment: cryptographic key sizes]

[92] [assignment: list of standards]

The **Basic Terminal** shall perform secure messaging – encryption and decryption[93] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[94] and cryptographic key sizes 112 bit[95] that meet the following: FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)[96].

Dependencies:
[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

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[97] in accordance with a specified cryptographic algorithm Retail-MAC[98] and cryptographic key sizes 112 bit[99] that meet the following: FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)[100].

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/RSA_BT Cryptographic operation – RSA
Hierarchical to: No other components.

FCS_COP.1.1/RSA_BT
The **Basic Terminal** shall perform digital signature verification[101] in accordance with a specified cryptographic algorithm RSA with SHA-1[102] and cryptographic key sizes 1024-4000 bit[103] that meet the following: scheme 1 of ISO/IEC 9796-2:2002[104][19].

[93] [assignment: list of cryptographic operations]

[94] [assignment: cryptographic algorithm]

[95] [assignment: cryptographic key sizes]

[96] [assignment: list of standards]

[97] [assignment: list of cryptographic operations]

[98] [assignment: cryptographic algorithm]

[99] [assignment: cryptographic key sizes]

[100] [assignment: list of standards]

[101] [assignment: list of cryptographic operations]

[102] [assignment: cryptographic algorithm]

[103] [assignment: cryptographic key sizes]

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 meet the requirements for SOF high defined in AIS 20 [5a].

Dependencies: No dependencies.

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 and Active Authentication Mechanism[105].

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[106].
Dependencies: No dependencies.

[104] [assignment: list of standards]

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

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

5.3.4 General Inspection System

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

The General Inspection System verifies the authenticity of the MRTD's by the Chip Authentication Mechanism during inspection and establishes new secure messaging with keys. The reference data for the Chip Authentication Mechanism is the Chip Authentication Public Key read form the logical MRTD data group EF.DG14 and verified by Passive Authentication (cf. to FDP_DAU.1/DS). Note, that the Chip Authentication Mechanism requires the General Inspection System to verify at least one message authentication code of a response sent by the MRTD to check the authenticity of the chip.

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

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

Hierarchical to: No other components.

FCS_CKM.1.1/DH_GIS
The **General Inspection System** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: ECDH, Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes: 192 bit – 320 bit, 112 bit resp that meet the following: **[25]**, Annex A.1 [107].

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

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

Hierarchical to: No other components.

FCS_COP.1.1/SHA_GIS
The **General Inspection System** shall perform hashing [108] in accordance with a specified cryptographic algorithm **SHA-1 and SHA-256** and cryptographic key sizes none [109] that meet the following: FIPS 180-2 [110].

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or

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

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

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

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

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

The General Inspection System shall meet the requirement "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

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

Hierarchical to: No other components.

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

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication Protocol[111].

Dependencies: No dependencies.

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

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

Hierarchical to: No other components.

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

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication[112]

to support user authentication.

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

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

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

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

3. After run of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.[113]

Dependencies: No dependencies.

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

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

Hierarchical to: No other components.

FIA_UAU.6.1/GIS

The **General Inspection System** shall re-authenticate the user under the conditions

1. Each response sent to the General Inspection System after successful authentication of the MRTD with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall have a correct MAC created by means of secure messaging keys agreed upon by the Basic Access Control Authentication Mechanism.
2. Each response sent to the General Inspection System after successful run of the Chip Authentication Protocol shall have a correct MAC created by means of secure messaging keys generated by Chip Authentication Protocol. [114]

Dependencies: No dependencies.

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

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

Hierarchical to: No other components.

FDP_UCT.1.1/GIS

The **General Inspection System** shall enforce the Access Control SFP [115] to be able to transmit and receive[116] objects in a manner protected from unauthorised disclosure **after Chip Authentication**.

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

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

---

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

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

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

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

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

Hierarchical to: No other components.

FDP_UIT.1.1/GIS
The **General Inspection System** shall enforce the Access Control SFP [117] to be able to transmit and receive [118] user data in a manner protected from modification, deletion, insertion and replay [119] errors **after Chip Authentication**.

FDP_UIT.1.2/GIS
The **General Inspection System** shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [120] has occurred **after Chip Authentication**.
Dependencies:
[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

5.3.5 Extended Inspection System

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

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

Hierarchical to: No other components.

FCS_COP.1.1/SIG_SIGN_EIS
The **Extended Inspection System** shall perform signature creation [121] in accordance with a specified cryptographic algorithm: ECDSA and cryptographic key sizes: 192 bit – 320 bit that meet the following: ISO 15946-2.

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/SHA_EIS Cryptographic operation – Hash for Key Derivation by EIS

Hierarchical to: No other components.

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

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

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

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

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

FCS_COP.1.1/SHA_EIS
The **Extended Inspection System** shall perform hashing [122] in accordance with a specified cryptographic algorithm **SHA-1 and SHA-256** and cryptographic key sizes none [123] that meet the following: FIPS 180-2 [124].

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

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

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

Hierarchical to: No other components.

FIA_API.1.1/EIS
The **Extended Inspection System** shall provide a Terminal Authentication Protocol according to [25] [125] to prove the identity of the Extended Inspection system [126].

Dependencies: No dependencies.

5.3.6 Personalization Terminals

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

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

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

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

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

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

[125] [assignment: *authentication mechanism*]

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

and (ii) the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

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

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

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

Hierarchical to: No other components.

FIA_API.1.1/SYM_PT

The **Personalization Terminal** shall provide an Authentication Mechanism based on Triple-DES [127] to prove the identity of the Personalization Agent [128].

Dependencies: No dependencies.

[127] [assignment: *authentication mechanism*]

[128] [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 noncryptographic 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.
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 perform 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) The TSF enforces the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
   - Allowing only the successfully authenticated Personalization Agent to write and to read the data of the data groups EF.COM, EF.SOD and EF.DG1 to EF.DG16 of the logical MRTD,
   - Allowing the successfully authenticated Basic Inspection System to read only data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.
   - Allowing the successfully authenticated Extended Inspection System to read only data in EF.COM, EF.SOD and EF.DG1 to EF.DG16 of the logical MRTD.
2) The TSF shall explicitly deny access of subjects to objects based on the rule: Terminals authenticated as CVCA or DV are not allowed to read data in EF.DG3 and EF.DG4.
3) Not allowing anybody to modify any of the data groups EF.DG1 to EF.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 it is not specified in this chapter otherwise.
5) Nobody is allowed to read the Document Basic Access Keys, the Chip Authentication Private Key, the Active Authentication Private Key and the 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) Ability before user identification and authentication:
   - to read the Initialization Data in Phase 2 “Manufacturing”,
   - to read the ATR (different for and after Initialisation)
   - to establish the communication channel, and
   - to identify themselves by selection of the authentication key.
3) Initialization, personalisation and configuration of the TOE are only allowed for the Manufacturer and the Personalisation Agent.
4) Ability to write the Initialization Data and Pre-personalization Data is restricted to the Manufacturer.
5) Ability to disable read access for users to the Initialization Data is restricted to the Personalization Agent.
6) The ability to write the CVCA Public Key, the initial CVCA certificate and the initial Current Date is restricted to the Personalization Agent.
7) The ability to update the CVCA Public Key and the CVCA certificate is restricted to the CVCA.
8) The Current Date can only be modified by the CVCA, DV or domestic Extended Inspection System.
9) Ability to write the Document Basic Access Keys is restricted to the Personalization Agent.
10) The creation and loading of the Chip Authentication Private Key is restricted to the Manufacturer and the Personalisation Agent**.**
11) Test Features of the TOE are not available for the user in Phase 4 “Operational Use”. If Test Features are performed by the TOE then 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.

12) Maintenance of the security roles: Manufacturer, Personalization Agent, Country Verifier Certification Authority, Document Verifier, Basic Inspection System, domestic Extended Inspection System, foreign Extended Inspection System.
13) Only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control.
14) Ability to write the data of the data groups EF.DG1 to EF.DG16 of the logical MRTD.
15) The creation and loading of the Active Authentication Private Key is restricted to the Manufacturer and the Personalisation Agent**.**

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

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
   - Terminal Authentication Protocol
   - Secure messaging in MAC-ENC mode
   - Symmetric Authentication Mechanism based on Triple-DES
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) After successful authentication as Basic Inspection System and until completion of the Chip Authentication mechanism only commands with correct message authentication code with key agreed upon with the authenticated terminal by means of the Basic Access Control Authentication Mechanism are accepted.
6) After run of the Chip Authentication Mechanism only commands with correct message authentication code with key agreed with the terminal by means of the Chip Authentication Mechanism are accepted.
7) Terminal authentication attempts are only accepted if the terminal uses secure messaging established by the Chip Authentication Mechanism.
8) Chip Authentication Protocol according to [25] to prove the identity of the TOE.
9) Re-Authentication:
   (a) Each command sent to the TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS.
   (b) Each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.
10) The TSF wait for an administrator configurable time between receiving the terminal challenge and sending the TSF response, if the defined number of unsuccessful authentication attempts has been met or surpassed.

11) The TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 unsuccessful authentication attempts occurs related to a BAC authentication protocol.
12) Ability to read the data of the groups EF.SOD, EF.COM and EF.DG1 to EF.DG16 of the logical MRTD, depending on the identity of the terminal.
13) Active Authentication Mechanism according to [7].

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

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) ECDH (compliant to ISO 15946) key import with key sizes of 192 bit - 320 bit and the import of Document Basic Access Key Derivation with key sizes of 112 bit, that meet [25], Annex A.1**.**
3) Hashing in accordance with SHA-1 that meet the following: FIPS 180-2.
4) 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.
5) Secure messaging – message authentication with Retail MAC and key sizes of 112 bit that meet: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).
6) Digital signature verification in accordance to ECDSA with SHA-1, SHA-224, SHA-256 and key sizes 192 bit - 320 bit that meet ISO 15946-2, FIPS PUB 180-2.
7) Random number generation according AIS20 [5a] for key generation and authentication process.
8) Destroying cryptographic keys by physical deletion by overwriting the memory data with zeros or random data.
9) RSA for signature creation according scheme 1 of ISO/IEC 9796-2:2002 [19]

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. After a successfully performed Chip Authentication 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 after Chip Authentication has been performed successfully.
2) Ensuring that transmitted and received objects are protected from unauthorised disclosure through secure messaging after Chip Authentication has been performed successfully.

3) Determination on receipt of user data if modification, deletion, insertion and replay have occurred through secure messaging after Chip Authentication has been performed successfully**.**
4) Hiding information about IC power consumption and command execution time.
5) The TOE ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
6) Maintaining a security domain for the TSF execution that protects it from interference and tampering by untrusted subjects.
7) Enforcing separation between the security domains of subjects in the TSC.
8) Running 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.
9) Providing authorised users with the capability to verify the integrity of TSF data and stored TSF executable code.

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_STA33_MRTD_ACM_00.
AM_ADO	The delivery, installation, generation and start-up of the TOE are described in GDM_STA33_MRTD _ADO_00.
AM_ADV	The representing of the TSF is described in GDM_STA33_MRTD _ADV_SPM_00 for security policy modelling, in GDM_STA33_MRTD _ADV_FSP_00 for functional specification, in GDM_STA33_MRTD _ADV_HLD_00 for high level design, in GDM_STA33_MRTD _ADV_LLD_00 for low level design, in GDM_STA33_MRTD _ADV_IMP_00 for implementation representation and in

Assurance Measures	Description
	GDM_STA33_MRTD _ADV_RCR_00 for representation correspondence.
AM_AGD	The guidance documentation is described in GDM_STA33_MRTD _AGD_USR_00 for the user and in GDM_STA33_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_STA33_MRTD _ALC_00
AM_ATE	The testing of the TOE is described in GDM_STA33_MRTD _ATE_00.
AM_AVA	The vulnerability assessment for the TOE is described in GDM_STA33_MRTD _AVA_MSU_00 for the misuse, in GDM_STA33_MRTD _AVA_SOF_00 for the strength of TOE security functions and in GDM_STA33_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_STA33_MRTD _AVA_VLA_00 may become GDM_STA33_MRTD _AVA_VLA_02).

7 PP Claims

7.1 PP Reference

The conformance of this ST to the Common Criteria Protection Machine Readable Travel Document with “ICAO Application, Extended Access Control (PP-MRTD EAC), Version 1.2, 19.11.2007, BSI-PP-0026, [21a] is claimed.

7.2 PP Additions

Active Authentication based on ICAO PKI v1.1 [7] has been added. The added and modified SFRs are listed in chapter 8.4

8 Rationale

The chapters 8.1 and 8.2 (except 8.2.5) have been taken from [21a] with minor modification to support the Active Authentication Mechanism 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.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.Active_Auth_proof	OD.Assurance	OD.Material	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System	OE.Active_Auth_Key_MRTD
T.Chip-ID			x [129]		x															x		
T.Skimming			x																			
T.Read_Sensitive_Data				x													x				x	
T.Forgery	x	x							x						x			x	x			
T.Counterfeit						x					x		x			x		x				x
T.Abuse-Func							x															
T.Information_Leakage								x														
T.Phys-tamper									x													
T.Malfunction										x												
P.Manufact												x	x									
P.Personalization	x											x		x								
P.Personal_Data		x	x																	x		
P.Sensitive_Data				x													x				x	
A.Pers_Agent														x								
A.Insp_Sys																		x		x		
A.Signature_PKI															x			x				
A.Auth_PKI																	x				x	

[129] In [21a] T.Chip-ID is covered in this table by OT.Sens_Data_Conf. However, the threat is countered by OT.Data_Conf as stated in chapter 7.1 of [21a].

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. **OD.Material** "Control over MRTD material" ensures that materials, equipment and tools used to produce genuine and authentic MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs.

The OSP **P.Personalization** "Personalization of the MRTD by issuing State or Organization only" addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD", and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD". Note, the manufacturer equips the TOE with the Personalization Agent Authentication key(s) according to **OD.Assurance** "Assurance Security Measures in Development and Manufacturing Environment". The security objective OT.AC_Pers limits the management of TSF data and the enabling and disabling of the TSF Basic Access Control to the Personalization Agent.

The OSP **P.Personal_Data** "Personal data protection policy" requires that the logical MRTD can be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an inspection system. This OSP is covered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the secure messaging based on session keys agreed in this protocol. The security objective **OT.Data_Conf** requires the TOE to implement the Basic Access Control as defined by ICAO [7] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" requires the inspection system to protect their communication with the TOE before secure messaging is successfully established based on the Chi Authentication Protocol. After successful Chip Authentication the security objective **OT.Data_Conf** "Confidentiality of personal data" ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System.

The OSP **P.Sensitive_Data** "Privacy of sensitive biometric reference data" is fulfilled and the threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the TOE-objective **OT.Sens_Data_Conf** "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorised inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorisation bases on Document Verifier certificates issued by the issuing state or organisation as required by **OE.Authoriz_Sens_Data** "Authorisation for use of sensitive biometric reference data". The Document Verifier of the receiving state has to authorize Extended Inspection Systems by creating appropriate Inspection System

certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** "Authorisation of Extended Inspection Systems".

The threat **T.Chip_ID** "Identification of MRTD's chip" addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the secure messaging based on session keys agreed in this protocol. The security objective **OT.Identification** "Identification and Authentication of the TOE" by limiting the TOE chip identification to the Basic Inspection System. The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" requires the inspection system to protect to their communication (as Basic Inspection System) with the TOE before secure messaging based on the Chip Authentication Protocol is successfully established. After successful Chip Authentication the security objective OT.Data_Conf "Confidentiality of personal data" ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System.

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

The threat **T.Forgery** "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRTD passport book according to **OE.Exam_MRTD** "Examination of the MRTD passport book" shall ensure that passport book does not contain 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.Counterfeit** "MRTD's chip" addresses the attack of unauthorised copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of MRTD's chip authentication" using a authentication key pair to be generated by the issuing state or organisation. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_MRTD** "MRTD Authentication Key". According to **OE.Exam_MRTD** "Examination of the MRTD passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip. MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs targeted on by **OD.Material**. Additionally, this attack is thwarted through the chip by an identification and authenticity proof required by **OT.Active_Auth_Proof**

"Proof of MRTD's chip authentication" using an authentication key pair to be generated by the issuing state or organisation. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Active_Auth_Key_MRTD** "MRTD Authentication Key".

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

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

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

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the MRTD passport book" which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

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

The assumption **A.Auth_PKI** "PKI for Inspection Systems" is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** "Authorisation for use of sensitive biometric reference data" requires the CVCA to limit the read access to sensitive biometric by issuing Document Verifier certificates for authorised receiving

States or Organisations only. The Document Verifier of the receiving state is required by **OE.Ext_Insp_Systems** "Authorisation of Extended Inspection Systems" to authorise Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure.

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.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.Active_Auth_Proof
FAU_SAS.1					x						
FCS_CKM.1/KDF_MRTD	x	x	x	x		x					
FCS_CKM.1/DH_MRTD	x	x		x		x					
FCS_CKM.4/MRTD	x	x	x	x							
FCS_COP.1/SHA_MRTD	x	x	x	x		x					
FCS_COP.1/TDES_MRTD	x	x	x								
FCS_COP.1/MAC_MRTD	x	x	x	x		x					
FCS_COP.1/SIG_VER	x			x							
FCS_COP.1/RSA_MRTD	x	x	x	x							x
FCS_RND.1/MRTD	x			x							
FIA_UID.1	x	x	x	x	x						
FIA_UAU.1	x	x	x	x	x						
FIA_UAU.4/MRTD	x	x	x	x							
FIA_UAU.5/MRTD	x	x	x	x							
FIA_UAU.6/MRTD	x	x	x	x							
FIA_AFL.1			x								
FIA_API.1/CAP						x					
FIA_API.1/AA											x
FDP_ACC.1	x	x	x	x							
FDP_ACF.1	x	x	x	x							
FDP_UCT.1/MRTD			x	x							
FDP_UIT.1/MRTD		x		x							
FMT_SMF.1	x	x	x								
FMT_SMR.1	x	x	x								

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.Active_Auth_Proof
FMT_LIM.1							x				
FMT_LIM.2							x				
FMT_MTD.1/INI_ENA					x						
FMT_MTD.1/INI_DIS					x						
FMT_MTD.1/CVCA_INI				x							
FMT_MTD.1/CVCA_UPD				x							
FMT_MTD.1/DATE				x							
FMT_MTD.1/KEY_WRITE	x		x								
FMT_MTD.1/CAPK		x	x	x		x					
FMT_MTD.1/AAPK		x	x	x							x
FMT_MTD.1/KEY_READ	x	x	x	x		x					x
FMT_MTD.3				x							
FPT_EMSEC.1	x							x			
FPT_TST.1								x		x	
FPT_RVM.1							x				
FPT_FLS.1								x		x	
FPT_PHP.3								x	x		
FPT_SEP.1							x			x	

Table 6 Coverage of Security Objective for the TOE by SFR

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

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

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

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

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

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

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

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data in EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: only the successful authenticated Personalization Agent, Basic Inspection Systems (Note the General Inspection Systems use the role Basic Inspection System.) and Extended Inspection Systems are allowed to read the data of the logical MRTD. The SFR FMT_SMR.1 lists

the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys). The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

The SFR FIA_AFL.1 strengthens the authentication function as terminal part of the Basic Access Control Authentication Protocol or other authentication functions if necessary. The SFR FIA_UAU.4/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5/MRTD enforces the TOE (i) to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and (ii) to accept chip authentication only after successful authentication as Basic Inspection System. Moreover, the SFR FIA_UAU.6/MRTD requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

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

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

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

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

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

The security objective **OT.Identification** "Identification and Authentication of the TOE" address the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

The TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data. The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their use in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application note 32 of [21a]).

The security objective **OT.Chip_Auth_Proof** "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol provided by FIA_API.1/CAP proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/DH_MRTD is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol [25] requires additional TSF according to FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode secure messaging).

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

The security objective **OT.Prot_Inf_Leak** "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the MRTD's chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption clock, or I/O lines, which is addressed by the SFR FPT_EMSEC.1,

- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or

- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

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

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

The security objective **OT.Active_Auth_Proof** “Proof of MRTD’s chip authenticity” is ensured by the Active Authentication Protocol provided by FIA_API.1/AA proving the identity of the TOE. The Active Authentication Protocol defined by FIA_API.1/AA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ. The Active Authentication Protocol [7] requires additional TSF according to FCS_COP.1/RSA_MRTD.

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

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

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

	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System	OE.Active_Auth_Key_MRTD
Document Signer									
FDP_DAU.1/DS		x	x		x	x			x
Document Verification PKI									
FCS_CKM.1/PKI				x					
FCS_COP.1/CERT_SIGN				x					

	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System	OE.Active_Auth_Key_MRTD
Basic Inspection System									
FCS_CKM.1/KDF_BT	x				x		x		
FCS_CKM.4/BT					x		x		
FCS_COP.1/SHA_BT	x				x		x		
FCS_COP.1/ENC_BT	x				x		x		
FCS_COP.1/MAC_BT	x				x		x		
FCS_RND.1/BT	x				x		x		
FIA_UAU.4/BT	x				x		x		
FIA_UAU.6/BT	x				x		x		
General Inspection System									
FCS_CKM.1/DH_GIS	x				x				
FCS_COP.1/SHA_GIS	x				x				
FIA_UAU.4/GIS					x				
FIA_UAU.5/GIS					x		x		
FIA_UAU.6/GIS					x		x		
FDP_UCT.1/GIS	x				x		x		
FDP_UIT.1/GIS	x				x		x		
Extended Inspection System									
FCS_COP.1/SIG_SIGN_EIS	x							x	
FCS_COP.1/SHA_EIS	x							x	
FIA_API.1/EIS	x							x	
Personalization Agent									
FIA_API.1/SYM_PT	x								

Table 7 Coverage of Security Objectives for the IT environment by SFR

The **OE.Personalization** "Personalization of logical MRTD" requires the Personalization Terminal to authenticate themselves to the MRTD's chip to get the write authorization.

If the Basic Access Control Authentication Mechanism with the Personalization Agent

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

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

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

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

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

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

The **OE.Exam_MRTD** "Examination of the MRTD passport book" requires the Basic Inspection System for global interoperability to implement the terminal part of the Basic Access Control [7] as required by FCS_CKM.1/KDF_BT, FCS_CKM.4/BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT, FCS_RND.1/BT, FIA_UAU.4/BT and FIA_UAU.6/BT. The verification of the authenticity of the MRTD's chip by General Inspection Systems and Extended Inspection Systems (including the functionality of the GIS) is covered by

the FCS_CKM.1/DH_GIS, FCS_COP.1/SHA_GIS, FIA_UAU.4/GIS, FIA_UAU.5/GIS and FIA_UAU.6/GIS providing the Chip Authentication Protocol and checking continuously the messages received from the MRTD's chip. The authenticity of the Chip Authentication Public Key (EF.DG14) is ensured by FDP_DAU.1/DS.

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

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

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

The **OE.Active_Auth_Key_MRTD** "MRTD Authentication Key" is covered by FDP_DAU.1/DS which requires the Document Signer to provide a capability to generate evidence for the validity of active authentication public key in DG 15. There is no need for the PP to provide any specific requirement for the method of generation, distribution and handling of the Active Authentication Private Key by the IT environment.

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.

SFR	Dependencies	Support of the Dependencies
FCS_CKM. 1/KDF_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, FCS COP.1/TDES MRTD, FCS_COP. 1/MAC_MRTD justification 1 for non-satisfied dependencies
FCS_CKM.1/DH_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 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 2 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
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 4 for non-satisfied dependencies

SFR	Dependencies	Support of the 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 4 for non-satisfied dependencies
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, justification 5 for non-satisfied dependencies
FCS_RND.1/MRTD	No dependencies	n.a.
FCS_COP.1/RSA_MRTD	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_CKM.4, see justification A for non-satisfied dependencies
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UAU.1 Timing of authentication	Fulfilled
FIA_UAU.4/MRTD	No dependencies	n.a.
FIA_UAU.5/MRTD	No dependencies	n.a.
FIA_UAU.6/MRTD	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled
FIA_API.1/CAP	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1

SFR	Dependencies	Support of the Dependencies
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.1, justification 6 for non-satisfied dependencies
FDP_UCT.1/MRTD	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1, justification 7 for non-satisfied dependencies
FDP_UIT.1/MRTD	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_ TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1, justification 7 for non-satisfied dependencies
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled
FMT_LIM.1	FMT_LIM.2	Fulfilled
FMT_LIM.2	FMT_LIM.1	Fulfilled
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled

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

Table 8 Dependencies between the SFR for the TOE

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

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

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

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

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

No. 5: The SFR FCS_COP.1/SIG_VER uses the initial public key Country Verifying

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

No. 6: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.2) is necessary here.

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

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

No.A: The SFR FCS_COP.1/RSA_MRTD does not calculate any shared secrets, nor does it import user data. Therefore there is not need for any special security attributes.

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

SFR	Dependencies	Support of the Dependencies
FDP_DAU.1	No dependencies	n.a.
FCS_CKM.1/PKI	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 9 for non-satisfied dependencies

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

SFR	Dependencies	Support of the 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 12 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 12 for non-satisfied dependencies
FCS_COP.1/RSA_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, see justification B for non-satisfied dependencies
FCS_RND.1/BT	No dependencies	n.a.
FIA_UAU.4/BT	No dependencies	n.a.
FIA_UAU.6/BT	No dependencies	n.a.
FCS_CKM.1/DH_GIS	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_COP.1/MAC_BT, FCS_CKM.4/BT, justification 13 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/SHA_GIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	FCS_COP.1/MAC_BT, FCS_CKM.4/BT, justification 13 for non-satisfied dependencies
FIA_UAU.4/GIS	No dependencies	n.a.
FIA_UAU.5/GIS	No dependencies	n.a.
FIA_UAU.6/GIS	No dependencies	n.a.
FDP_UCT.1/GIS	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_ TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	justification 14 for non-satisfied dependencies
FDP_UIT.1/GIS	[FTP_ITC.1 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]	justification 14 for non-satisfied dependencies
FCS_COP.1/SIG_SIGN_EIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 15 for nonsatisfied dependencies

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/SHA_EIS	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes	justification 15 for nonsatisfied dependencies
FIA_API.1/EIS	No dependencies	n.a.
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. 9: The TOE does not have specific functional security requirements to the IT environment establishing Document Verification PKI which have to be described by the listed dependency here.

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

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

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

No. 13: The SFR FCS_CKM.1/DH_GIS and FCS_COP.1/SHA_GIS are used for generation of secure messaging session keys (cf. FCS_COP.1/SHA_GIS, application note 66 of [21a]) by means of the Chip Authentication Protocol. These session keys are destroyed by the same function as for the Basic Terminal (cf. FCS_CKM.4/BT). There is no need for import or management of security attributes of these session keys.

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

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

No.B: The SFR FCS_COP.1/RSA_BT does not calculate any shared secrets, nor does it import user data. Therefore there is not need for any special security attributes.

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

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

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

The component ADV_IMP.2 has the following dependencies:

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

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

The component ALC_DVS.2 has no dependencies.

The component AVA_MSU.3 has the following dependencies:
- ADO_IGS.1 Installation, generation, and start-up procedures
- ADV_FSP.1 Informal functional specification
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

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

The component AVA_VLA.4 has the following dependencies:
- ADV_FSP.1 Informal functional specification
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

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

8.2.4 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.

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/DH_MRTD				2)		
FCS_CKM.1.1/KDF_MRTD				1)		
FCS_CKM.4.1/ MRTD				8)		
FCS_COP.1.1/ SHA_MRTD				3)		
FCS_COP.1.1/ TDES_MRTD				4)		4)
FCS_COP.1.1/MAC_MRTD				5)		
FCS_RND.1.1/ MRTD				7)		3)
FCS_COP.1.1/SIG_VER				6)		
FCS_COP.1.1/RSA_MRTD				9)		
FIA_AFL.1.1			11)			
FIA_AFL.1.2			10)			
FIA_API.1.1/CAP			8)			
FIA_API.1.1/AA			13)			
.		2)				

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
FIA_UID.1.1						
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/MRTD			1)			
FIA_UAU.5.2/MRTD			3), 4), 5), 6), 7)			
FIA_UAU.6.1/MRTD			9)			
FDP_ACC.1.1	1), 2), 3)					
FDP_ACF.1.1	1), 2)					
FDP_ACF.1.2	1)	14)	12)			
FDP_ACF.1.3	1), 2)					
FDP_ACF.1.4	2)					
FDP_UCT.1.1/ MRTD					2)	
FDP_UIT.1.1/ MRTD					1)	
FDP_UIT.1.2/ MRTD					3)	
FMT_SMF.1.1		3)				
FMT_SMR.1.1		12)				
FMT_SMR.1.2		12)				
FMT_LIM.1.1		11)				
FMT_LIM.2.1		11)				
FMT_MTD.1.1/ INI_ENA		4)				
FMT_MTD.1.1/ INI_DIS		5)				
FMT_MTD.1.1/ KEY_WRITE		9)				
FMT_MTD.1.1/ KEY_READ	5)					
FMT_MTD.1.1/CVCA_INI		6)				
FMT_MTD.1.1/CVCA_UPD		7)				
FMT_MTD.1.1/DATE		8)				
FMT_MTD.1.1/CAPK		10)				
FMT_MTD.1.1/AAPK		15)				
FMT_MTD.3.1		13)				
FPT_EMSEC.1.1					4)	
FPT_EMSEC.1.2					4)	
FPT_FLS.1.1						2)

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_TST.1.1					8)	
FPT_TST.1.2					9)	
FPT_TST.1.3					9)	
FPT_PHP.3.1						1)
FPT_RVM.1.1					5)	
FPT_SEP.1.1					6)	
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, FCS_COP, FCS_RND

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

FCS_CKM.1.1/DH_MRTD requires that cryptographic keys are generated in accordance with a specified cryptographic key generation algorithm: ECDH compliant to ISO 15946, Document Basic Access Key Derivation and specified cryptographic key sizes: 192 bit – 320 bit, 112 bit that meet the following: [25], Annex A.1.

SF.CRYPTO.2 states that ECDH (ISO 15946) key generation and Document Basic Access Key Derivation is in accordance with the above stated standards and therefore meets the above stated TOE SFR.

FCS_CKM.1.1/ KDF_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.CRYPTO.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.8 states that cryptographic keys are destroyed by physical deletion by overwriting the memory data with zeros or random data and therefore meets the above stated TOE SFR.

FCS_COP.1.1/SIG_VER requires that the TSF shall perform digital signature verification in accordance with specified cryptographic algorithms.

SF.CRYPTO.6 states that Digital signature verification is in accordance to ECDSA with SHA-1, SHA-224, SHA-256 and key sizes 192 bit - 320 bit that meet ISO 15946-2, FIPS PUB 180-2.

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.3 states that hashing by the TOE is performed in accordance with SHA-1 that meets 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.4 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.5 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.7 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.

FCS_COP.1.1/RSA_MRTD requires that the TSF shall provide a signature creation according to scheme 1 of IOS/IEC 9796-2:2002 [19].

SF.CRYPTO.9 states, that the TOE provides RSA signature creation according to scheme 1 of ISO/IEC 9796-2:2002 [19] and therefore meets the above stated SFR.

8.3.1.1.3 FIA_AFL, FIA_API, FIA_UID, FIA_UAU

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_AFL.1.1 requires that the TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 unsuccessful authentication attempts occur related to a BAC authentication protocol.

SF.AUTH.11 states that the TOE shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 unsuccessful authentication attempts occurs related to a BAC authentication protocol and therefore meets the above stated TOE SFR.

FIA_AFL.1.2 requires that the TSF shall wait for an administrator configurable time between receiving the terminal challenge e_{IFD} and sending the TSF response e_{ICC} during the BAC authentication attempts when the defined number of unsuccessful authentication attempts has been met or surpassed

SF.AUTH.10 states that the TOE waits for an administrator configurable time between receiving the terminal challenge and sending the TSF response, if the defined number of unsuccessful authentication attempts has been met or surpassed and therefore meets the above stated TOE SFR.

FIA_API.1.1/CAP requires that the TSF shall provide a Chip Authentication Protocol according to [25] to prove the identity of the TOE

SF.AUTH.8 states that the TOE has implemented the Chip Authentication Protocol according to [25] to prove the identity of the TOE and therefore meets the above stated TOE SFR.
.

FIA_UID.1.1 requires that the TSF shall allow

(3) to establish the communication channel,
(4) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[130]
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",
- to read the ATR (different for and after Initialisation)
- to establish the communication channel, and
- to identify themselves by selection of the authentication key.

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.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 6 otherwise and therefore meets the above stated TOE SFR.

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

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 (different for and after Initialisation)
- to establish the communication channel, and

to identify themselves by selection of the authentication key 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.ACCESS.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. Terminal Authentication Protocol,
3. Authentication Mechanism based on Triple-DES.

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

SF.AUTH.2 realises the prevention of reuse of authentication data and therefore meets the above stated TOE SFR.

FIA_UAU.5.1/MRTD requires that the TSF shall provide
1. Basic Access Control Authentication Mechanism,
2. Terminal Authentication Protocol,
3. Secure messaging in MAC-ENC mode,
4. Symmetric Authentication Mechanism based on Triple-DES [131]

to support user authentication.

SF.AUTH.1 realises user authentication provided through:
- Basic Access Control Authentication Mechanism
- Terminal Authentication Protocol
- Secure messaging in MAC-ENC mode
- Symmetric Authentication Mechanism based on Triple-DES

and therefore meets the above stated TOE SFR.

FIA_UAU.5.2/MRTD 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 Personalization Agent Keys,
   b) the Symmetric Authentication Mechanism with Personalization Agent Key,
   c) the Terminal Authentication Protocol with Personalization Agent Keys.
2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
3. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging with the key agreed upon with the authenticated terminal by means of the Basic Access Control Authentication Mechanism.
4. After run of the Chip Authentication Mechanism the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism.[132].

SF.AUTH.3 - 7 realises user authentication for the Personalisation Agent:
(a) for the Basic Access Control Authentication Mechanism with
the Personalization Agent Keys,

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

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

(b) for the Symmetric Authentication Mechanism with the Personalization Agent Key

(c) for the Terminal Authentication Protocol with the Personalization Agent Keys 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

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

SF.AUTH.9 enables the authentication of a user under the above stated and therefore meets the above stated TOE SFR.

8.3.1.1.4 FDP_ACC, FDP_ACF

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

SF.ACCESS.1, 2 and 3:

- allows only the successfully authenticated Personalization Agent to write the data of the data groups COM, SOD and DG1 to DG16 of the logical MRTD,
- allows only the the successfully authenticated Basic Inspection System to read only data in COM, SOD, DG1, DG2 and DG5 to DG16 of the logical MRTD.
- allows only the the successfully authenticated Extended Inspection System to read only data in COM, SOD and DG1 to DG16 of the logical MRTD.

The TSF shall explicitly deny access of subjects to objects based on the rule: Terminals authenticated as CVCA or DV are not allowed to read data in DG3 and DG4 and therefore meets the above stated TOE SFR.

FDP_ACF.1.1 requires that the TSF shall enforce the Access Control SFP to objects based on the following:

1. Subjects:
   a. Personalization Agent,
   b. Basic Inspection System,
   c. Extended Inspection System
   d. Terminal,
2. Objects:

a. data EF.DG1 to EF.DG16 of the logical MRTD,

b. data in EF.COM,

c. data in EF.SOD,

3. Security attributes:

a. authentication status of terminals,

b. Terminal Authorization

SF.ACCESS.1 and 2:

- allows only the successfully authenticated Personalization Agent to write the data of the data groups COM, SOD and DG1 to DG16 of the logical MRTD,
- allows only the the successfully authenticated Basic Inspection System to read only data in COM, SOD, DG1, DG2 and DG5 to DG16 of the logical MRTD.
- allows only the the successfully authenticated Extended Inspection System to read only data in COM, SOD and DG1 to DG16 of the logical MRTD.

The TSF shall explicitly deny access of subjects to objects based on the rule: Terminals authenticated as CVCA or DV are not allowed to read data in DG3 and DG4 and therefore meets the above stated TOE SFR.

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

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

SF.ACCESS.1

- Allows only the successfully authenticated Personalization Agent to write and to read the data of the data groups COM, SOD and DG1 to DG16 of the logical MRTD,
- Allows the successfully authenticated Basic Inspection System to read only data in COM, SOD, DG1, DG2 and DG5 to DG16 of the logical MRTD.
- Allows the successfully authenticated Extended Inspection System to read only data in COM, SOD and DG1 to DG16 of the logical MRTD.

SF.ADMIN.14 realises the ability to write the data of the data groups DG1 to DG16 of the logical MRTD.

SF.AUTH.12 realises the ability to read the data of the groups SOD, COM and DG1 to DG16 of the logical MRTD and therefore meets the above stated TOE SFR.

FDP_ACF.1.3 requires that the TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

SF.ACCESS.1 and 2

- Allows only the successfully authenticated Personalization Agent to write and to read the data of the data groups COM, SOD and DG1 to DG16 of the logical MRTD,
- Allows the successfully authenticated Basic Inspection System to read only data in COM, SOD, DG1, DG2 and DG5 to DG16 of the logical MRTD.
- Allows the successfully authenticated Extended Inspection System to read only data in COM, SOD and DG1 to DG16 of the logical MRTD.
- denies access of subjects to objects based on the rule: Terminals authenticated as CVCA or DV are not allowed to read data in DG3 and DG4

and therefore meets the above stated TOE SFR.

FDP_ACF.1.4 requires that the TSF shall explicitly deny access of subjects to objects based on the rules:

1. The TSF shall explicitly deny access of subjects to objects based on the rule: A terminal authenticated as CVCA is not allowed to read to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,
5. the Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.

SF.ACCESS.2 is not allowing access of subjects to objects based on the rule: Terminals authenticated as CVCA or DV are not allowed to read data in DG3 and DG4 and therefore meets the above stated TOE SFR.

8.3.1.1.5 FDP_UCT, FDP_UIT

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 Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorised disclosure after Chip Authentication.

SF.PROTECTION.2 ensures that transmitted and received objects are protected from unauthorised disclosure after Chip Authentication and therefore meets the above stated TOE SFR.

FDP_UIT.1.1/ MRTD requires that the TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication.

SF.PROTECTION.1 ensures that transmitted and received user data is protected from

modification, deletion, and insertion and replay errors after Chip Authentication 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 after Chip Authentication and replay has occurred.

SF.PROTECTION.3 determines on receipt of user data if modification, deletion, insertion and replay has occurred after Chip Authentication and therefore meets the above stated TOE SFR.

8.3.1.1.6 FMT_SMF, FMT_SMR, FMT_LIM, FMT_MTD

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

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.3 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. Country Verifier Certification Authority,
4. Document Verifier,
5. Basic Inspection System,
6. domestic Extended Inspection System
7. foreign Extended Inspection System

SF.ADMIN.12 maintains the security roles: Manufacturer, Personalization Agent, Country Verifier Certification Authority, Document Verifier, Basic Inspection System, domestic Extended Inspection System, foreign Extended 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.12 maintains the security roles: Manufacturer, Personalization Agent, Country Verifier Certification Authority, Document Verifier, Basic Inspection System, domestic Extended Inspection System, foreign Extended 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.11 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.11 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.4 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.5 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.ADMIN.9 restricts the ability to write the Document Basic Access Keys to the Personalization Agent 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, Personalization Agent Keys, Chip Authentication Private Key and the Active Authentication Private Key to none.

SF.ACCESS.5 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/CVCA_INI requires that the TSF shall restrict the ability to write the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifier Certification Authority Certificate,
3. initial Current Date

to the Personalization Agent.

SF.ADMIN.6 restricts the ability to write the CVCA Public Key, the initial CVCA certificate and the initial Current Date is restricted to the Personalization Agent and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/CVCA_UPD requires that the TSF restricts the ability to update the

1. Country Verifier Certification Authority Public Key,
2. Country Verifier Certification Authority Certificate

to Country Verifier Certification Authority.

SF.ADMIN.7 restricts the ability to update the CVCA Public Key and the CVCA certificate is restricted to the CVCA and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/DATE requires that the TSF restricts the ability to modify the Current date to

1. Country Verifier Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System.

SF.ADMIN.8 restricts the modification of the Current Date to the CVCA, DV or domestic Extended Inspection System and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/CAPK requires that the TSF restricts the ability to create and load the Chip Authentication Private Key to the Manufacturer and the Personalisation Agent.

SF.ADMIN.10 restricts the creation and loading of the Chip Authentication Private Key to the Manufacturer and the Personalisation Agent and therefore meets the above stated TOE SFR.

FMT_MTD.1.1/AAPK requires that the TSF restricts the ability to create and load the Active Authentication Private Key to the Manufacturer and the Personalisation Agent.

SF.ADMIN.15 restricts the creation and loading of the Active Authentication Private Key to the Manufacturer and the Personalisation Agent and therefore meets the above stated TOE SFR.

FMT_MTD.3.1 requires that the TSF ensures that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control.

SF.ADMIN.13 requires that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control and therefore meets the above stated TOE SFR.

8.3.1.1.7 FPT_EMSEC, FPT_FLS, FPT_TST, FPT_PHP, FPT_RVM, FPT_SEP

SF.PROTECTION (Protection of TSC) protects the TSF functionality, TSF data and user data and SF.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.2 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.8 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.9 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.9 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.1 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.5 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.6 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.7 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

This security target is conformant to the claimed PP [21a]. Additionally, the Active Authentication Mehcnism is included in the TOE. This implies the below desribed augmentations:

Addition of new TOE Objectives:

- OT.Active_Auth_Proof

Addition of new IT Environment Objectives:

- OE.Active_Auth_Key_MRTD

Addition of new SFR's for the TOE:

- FCS_COP.1/RSA_MRTD
- FIA_API.1/AA
- FMT_MTD.1/AAPK

Extension of existing SFR's for the TOE:

- FMT_MTD.1/KEY_READ: to include the Active Authentication private key
- FPT_EMSEC.1.2: to include the Active Authentication private key

Addition of new IT environment SFRs:

- FCS_COP.1.1/RSA_BT

Extension of IT environment SFRs:

- FIA_UAU.4/BT: include the Active Authentication mechanism

8.5 Statement of compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the NXP Chip P5CD080 [HW ST P5CD].

8.5.1 Classification of Platform TSFs

A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for the Composite-ST.

TOE Security Functions	**Relevant**	**Not relevant**
F.RNG: Random Number Generator	x	
F.HW_DES: Triple-DES Co-processor	x	
F.HW_AES: AES Co-processor		x
F.OPC: Control of Operating Conditions	x	
F: PHY: Protection against Physical Manipulation	x	
F.LOG: Logical Protection	x	
F.COMP: Protection of Mode Control	x	
F.MEM_ACC: Memory Access Control		x
F.SFR_ACC: Special Function Register Access Control		x

Table 12 Classification of Platform-TSFs

F.MEM_ACC and F.SFR_ACC are not relevant of the Composite-ST because the combination of F.SFR_ACC and F.COMP ensures that the other CPU modes are not available for the Smartcard Embedded Software, but reserved for specific purposes fulfilled by the IC Dedicated Software.

8.5.2 Matching statement

The TOE needs the following implicit assumptions of the IC (see 2.1)

- Certified NXP Microcontroller P5CD080

8.5.2.1 TOE Security Environment

8.5.2.1.1 Threats

(See chapter 3.3)

The following threats of this Composite-ST are directly related to IC functionality:

- T.Information_Leakage
- T.Phys-Tamper

These threats will be mapped to the following Platform-ST threats and OSPs:

- T.Leak-Inherent
- T.Phys_Probing
- T.Phys_Manipulation
- T.Malfunction
- T.Abuse_Func
- T.Leak-Forced
- P.Add-Components (Additional Specific Security Components)
- P.Process-TOE (Protection during TOE Development and Production)

The table below shows the mapping of the threats.

		P.Add-Components	P.Process-TOE	T.Leak-Inherent	T.Phys_Probing	T.Phys_Manipulation	T.Malfunction	T.Abuse_Func	T.Leak-Forced
Composite-ST	T.Phys-Tamper	X	X		X	X	X	X	
	T.Information_Leakage	X	X	X					X

Table 13 Mapping of threats

The threats from chapter 3.3 not mentioned here are not related to the Platform-ST. T.Phys-Tamper matches to T.Phys_Probing, T.Phys_Manipulation, T.Malfunction, T.Abuse_Func as all these threats are directed against the SCP in a direct or indirect physical way.

Additionaly P.Add_components and P.Process-TOE as a specific security components policy matches with T.Phys-Tamper and T.Information_Leakage because it prevents modification of configuration data during TOE Development and Production and after TOE delivery. Information_Leakage matches to T.Leak-Inherent and T.Leak-Forced and also P.Add_components and P.Process-TOE because all threats and OSP are dealing also with leakage threats.

8.5.2.1.2 Assumptions

(See chapter 3.2)
The assumptions A.Pers_Agent, A.Insp_Sys, A.Signature_PKI and A.Auth_PKI do not contain any assumption for the platform.
The assumption from the Platform-ST:

Assumptions of Platform-ST	**Classification of significant assumptions**	**Mapping to Security Objectives of this Composite-ST**
A.Process-Card	IrPA (irrelevant platform assumption)	n/a
A.Plat-Appl	IrPA	n/a
A.Resp-Appl	CfPA (automatically fulfilled platform assumption)	OT.Prot_Inf_Leak,
A.Check-Init	CfPA	OT.Identification
A.Key-Function	CfPA	OT.Prot_Inf_Leak,

Table 14 Mapping of assumptions

There is no significant platform assumption (SgPA) of the Platform-ST fore this Composite-ST. There is **no conflict** between **security environments** of this Composite-ST and the Platform-ST.

8.5.2.1.3 Organisational Security Policies

(See chapter 3.4)
This composite ST has organisational security policies, which are directly related to the Platform-ST:

- P.Manufact

These organisational security policies can be mapped directly to the following Plattform-ST organisational security policy:

- P.Process-TOE

Other organisational security policies of this Composite-ST in chapter 3.4 are not applicable for the mapping to the Platform-ST. These organisational security policies are:

- P.Personalization
- P.Personal_Data
- P.Sensitive_Data

There is **no conflict** between **organisational security policies** of this Composite-ST and the Platform-ST.

8.5.2.1.4 Security Objctives

(See chapter 3.5)

This Composite-ST has security objectives which are directly related to the Platform-ST:

- OT.Identification
- OT.Prot_Inf_Leak
- OT.Prot_Phys-Tamper
- OT.Prot_Malfunction

These objectives can be mapped to the following Platform-ST objectives:

- O.Leak-Inherent
- O.Phys-Probing
- O.Malfunction
- O.Phys-Manipulation
- O.Leak-Forced
- O.Abuse-Func

		O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.Identification
Composite-ST	Obejctives for TOE_IC							
	OT.Identification							X
	OT.Prot_Inf_Leak	X	X		X	X	X	
	OT.Prot_Phys-Tamper	X	X		X	X	X	
	OT.Prot_Malfunction			X				

Table 15 Mapping of objectives

OT.Identification matches directly O.Identification.
OT.Prot_Inf_Leak and OT.Prot_Phys_Tamper are matching O.Leak-Inherent, O.Phys-Probing, O.Phys-Manipulation, O.Leak-Forced and O.Abuse-Func because they provide protection against disclosure of primary assets including confidential data (User Data or TSF data) stored and/or processed in the Smart Card IC to avoid interpretations of signals extracted from the hardware part of the TOE (Power Supply, Electro Magnetic emissions, e.g.).
OT.Malfunction matches directly O.Malfunction.

Other objectives of this Composite-ST in chapter 3.5.1 are not applicable for the mapping to the Platform-ST. These objectives are:

- OT.AC_Pers
- OT.Data_Int
- OT.Data_Conf
- OT.Sens_Data_Conf
- OT_Chip_Auth_Proof
- OT.Prot_Abuse-Func
- OT.Active_Auth_Proof

The other Objectives (see 3.5.2, 3.5.3 and 3.5.3.2) are all not linked to the platform and are therefore not applicable to this mapping.

There is **no conflict** between **security objectives** of this Composite-ST and the Platform-ST.

8.5.2.1.5 Security requirements

(See chapter 5.1)
This Composite-ST contains the following platform related SFRs:

- FCS_COP.1/TDES_MRTD
- FCS_COP.1/MAC_MRTD
- FCS_RND.1/MRTD
- FMT_LIM.1
- FMT_LIM.2
- FMT_MTD.1/INI_ENA
- FMT_MTD.1/INI_DIS
- FPT_EMSEC.1
- FPT_FLS.1
- FPT_TST.1
- FPT_PHP.3

These SFRs will be matched by the following SFRs of the Platform-ST:

- FPT_FLS.1
- FCS_RND.1
- FRU_FLT.2
- FDP_ITT.1
- FPT_ITT.1
- FPT_PHP.3
- FCS_COP.1 [DES]
- FMT_LIM.1
- FMT_LIM.2
- FPT_SEP.1[CONF]

The matching will be as described in the table below.

		FPT_FLS.1	FCS_RND.1	FCS_COP.1[DES]	FRU_FLT.2	FDP_ITT.1	FPT_ITT.1	FPT_PHP.3	FMT_LIM.1	FMT_LIM.2	FPT_SEP.1[CONF]
Composite-ST											
	FCS_COP.1/TDES_MRTD			X							
	FCS_COP.1/MAC_MRTD			X							
	FCS_RND.1/MRTD		X								
	FMT_LIM.1								X		
	FMT_LIM.2									X	
	FMT_MTD.1/INI_ENA										X
	FMT_MTD.1/INI_DIS										X
	FPT_EMSEC.1					X	X				
	FPT_FLS.1	X			X			X			
	FPT_TST.1				X						
	FPT_PHP.3				X			X			

Table 16 Mapping of SFRs

FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD are matching FCS_COP.1 [DES] as the Platform provides encryption and decryprion for the composite product with the necessary cryptographic key sizes.
FCS_RND.1/MRTD matches FCS_RND.1 as the Platform provides a mechanism to generate random numbers for the composite product.
FMT_LIM.1 and FMT_LIM.1 are matching directly FMT_LIM.1 and FMT_LIM.2 of the platform.
FMT_MTD.1/INI_ENA and FMT_INI_DIS are matching FPT_SEP.1[CONF], since FPT_SEP.1[CONF] offers the possibility to fix special parts of the hardware (including memory space for the memory blocks).
FPT_EMSEC.1 matches to FPT_ITT.1 and FDP_ITT.1 as the Composite-TOE should not emit information about IC power consumption and execution time while the Platform protects user and TSF data by leackage attacks.
FPT_FLS.1 matches to FPT_FLS.1, FRU_FLT.2 and FPT_PHP.3 as the Composite-TOE should preserve a secure state when the Platform operates out of normal operating conditions, while the Platform should ensure the robustness and operate always in a secure state.
FPT_TST.1 matches FRU_FLT.2 as the Platform must ensure that the TOE operates correctly within some limits.
FPT_PHP.3 matches the robustness requirements of FRU_FLT.2 and FPT_PHP.3.
RSA cryptograhic operations are supported by the ST-Platform through the FameXE co-processor through basic arithmetic functions for large integer numbers.

8.5.2.1.6 Assurance requirements

The Composite-ST requires EAL 4 augmented by:
ADV_IMP.2

AVA_VLA.4
The Platform-ST requires EAL 5 augmented by:
ALC_DVS.2
AVA_MSU.3
AVA_VLA.4

As EAL 5 covers all assurance requirements of EAL 4 all non augmented parts of the Composite-ST will match to the Platform-ST assurance requirements. But also the augmented parts of the Composite-ST match to the Platform-ST:
ADV_IMP.2 is part of EAL 5 and AVA_VLA.4 is augmented for the Platform-ST as well.

8.5.2.1.7 Overall no contracdictions found

Overall there is **no conflict** between **security requirements** of this Composite-ST and the Platform-ST[HW ST P5CD].

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 protects their communication by means of secure messaging with Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [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.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (selfsigned certificate).
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [8]
Country Signing CA Certificate C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy

Term	Definition
Authority	of the issuing Country or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD. It is
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [7], Annex E.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key 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 SOD)	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]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [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	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.
Extended Inspection System EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.

Term	Definition
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [8]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in 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.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
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

Term	Definition
	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) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16).
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [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 visa page 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 - 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 DG13 and DG 16) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [10],

Term	Definition
	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.
Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
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.

Term	Definition
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.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be all valid for the Current Date.
travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel. [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
EIS	Extended Inspection System
GMA	Generic MRTD Application
n.a.	Not applicable
OSP	Organisational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE security functions

9.3 References

Common Criteria	
[1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-09-001
[2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-09-002
[3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-09-00
[4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-09-004
[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)
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
[19a]	ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002.
[19b]	ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002
[19c]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[19d]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
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, Extended Access Control (PP-MRTD EAC), Version 1.2, 19.11.2007, BSI-PP-0026, Bundesamt für Sicherheit in der Informationstechnik
Other	
[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 BSI-DSZ-CC-0410-2007 for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B and P5CC080V0B each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification, Bundesamt für Sicherheit in der Informationstechnik (BSI), 05.07.07
[25]	Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.0, TR-03111, Bundesamt für Sicherheit in der Informationstechnik (BSI), 14.02.2007
[26]	Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006
[27]	Administrator Guidance STARCOS 3.3 Passport Edition 2.0a, Version 0.3, 09.05.2008, Giesecke&Devrient
[28]	User guidance STARCOS 3.3 Passport Edition 2.0a, Version 0.4, 07.05.2008, Giesecke&Devrient
[29]	STARCOS 3.3 Passport Edition TABLES, Version 1.0, 19.08.2008, Giesecke&Devrient
[30]	Generic MRTD Application Verifier Tool for STARCOS 3.3 Passport Edition, Version 2.0, 26.06.2008, Giesecke&Devrient

-End of Document-