MASKTECH

Security Target

COMMON CRITERIA DOCUMENTS | Version 1.2

MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) (BAC)

Machine Readable Travel Document with "ICAO Application",
Basic Access Control

Certification-ID: BSI-DSZ-CC-1148-V3

Public Version

MaskTech International GmbH | Nordostpark 45 | Nuernberg | www.masktech.com | +49 (0)911 95 51 49-0

Contents

1 ST Introduction (ASE_INT.1)

1.1 ST Reference and TOE Reference

Title	Security Target – Machine Readable Travel Document with “ICAO Application”, Basic Access Control, MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) (BAC)
Version	1.2, 2023-08-24
Editors	Christian Wille
Compliant to	Common Criteria Protection Profile - Machine Readable Travel Document with “ICAO Application”, Basic Access Control, version 1.10, BSI-CC-PP-0055
CC Version	3.1 (Revision 5)
Assurance Level	The assurance level for this ST is EAL4 augmented
TOE name	MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) (BAC), operation system for secure passports
TOE Hardware	NXP Semiconductors Germany GmbH P71D352 (N7121), dual interface Smartcard IC (see also section 1.2)
TOE version	MTCOS Pro 2.6 EAC with PACE
Keywords	ICAO, machine readable travel document, basic access control

1.2 TOE Overview

This security target defines the security objectives and requirements for the contactless/contact[1] chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the ’ICAO Doc 9303’ [ICAO_9303].

MTCOS Pro is a fully interoperable multi-application smart card operating system compliant to [ISO_7816]. It provides public and secret key cryptography and supports also other applications like e-purses, health insurance cards and access control.

MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) (BAC) uses two derivatives of P71D352 (N7121) with the sales code:

[1] Both interfaces provide the same functionality and are thus taken as one single product in this ST.

- P71D352D as MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) (BAC) PLUS and
- P71D352P as MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) (BAC) BASIC.

These derivatives differ only whether MIFARE-DESFire and Match-On-Card are part of the platform or not. However, DESFire and Match-On-Card are not part of the TOE and consequently are not security-relevant. Therefore, both derivatives are taken as one configuration.

The operating system software is implemented on the P71D352 (N7121) secure dual-interface controller of NXP Semiconductors Germany GmbH (BSI-DSZ-CC-1136-V3-2022 [NXP_P71_ST]). Chip and cryptographic library are certified according to CC EAL6 augmented compliant to the Protection Profile BSI-CC-PP-0084-2014 [CC_PP-0084]). The TOE consists of software and hardware.

TOE Definition

The Target of Evaluation (TOE) is the contactless/contact integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [ICAO_9303] and providing Basic Access Control according to the 'ICAO 9303' [ICAO_9303].

The TOE comprises of

- the circuitry of the MRTD's chip (the integrated circuit, IC)
- 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 [AGD, MT_Manual]

The TOE is based on [ISO_7816] commands and is intended to be used inside a MRTD as storage of the digital data and supports Basic Access Control and Extended Access Control.

It provides following services for MRTDs:

- Storage of the MRTD data, e.g. data groups and signature
- Organization of the data in a file system as dedicated and elementary files
- Mutual Authenticate and Secure Messaging as specified in [ICAO_9303] for Basic Access Control
- Contactless communication according to [ISO_14443]
- Protection of the privacy of the passport holder with functions like random UID and Basic Access Control

TOE Usage and Security Features for Operational Use

State or organization issues MRTD to be used by the holder for international travel. The traveler presents a MRTD to the Inspection System to prove his or her identity. The MRTD in context of this 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 [ICAO_9303] for contactless or contact based machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of

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)
3. the printed portrait

the logical MRTD as data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contactless/contact integrated circuit. It presents contactless or contact based 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
4. the other data according to LDS (EF.DG5 to EF.DG16)
5. the Document Security Object

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

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO_9303]. These security measures include the binding of the MRTD's chip to the passport book.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO_9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of 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. This Security Target does not address the Active Authentication and the Extended Access Control as optional security mechanisms.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the

inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (Secure Messaging) with this inspection system [ICAO_9303], normative appendix 5.

TOE Life Cycle

The TOE life cycle is described in terms of the four life cycle phases. With respect to [CC_PP-0084], the TOE life cycle is additionally subdivided into 7 steps.

Phase 1: Development (**Step 1**) 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.

(**Step 2**) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the 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 (FLASH) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase 2: Manufacturing (**Step 3**) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and conditionally the parts of the travel document's chip Embedded Software in the non-volatile non-programmable memories (FLASH). NXP Semiconductors Germany GmbH writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the MRTD manufacturer.

Conditionally, NXP Semiconductors Germany GmbH adds the parts of the IC Embedded Software in the non-volatile programmable memories (FLASH) and deactivates the Flash Loader permanently. The IC is securely delivered from NXP Semiconductors Germany GmbH to the MRTD manufacturer.

(**Step 4**) See **Inlay production** below

Note 1: The inlay production including the application of the antenna is not part of the TOE.

(**Step 5**) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD's chips with pre-personalization Data.

Note 2: For file based operating systems, the creation of the application implies the creation of MF and ICAO.DF.

Note 3: The role of the *Manufacturer* performing initialization and pre-personalization in the *Card Issuing* phase is taken over by MaskTech International GmbH, Linxens (Thailand) Co Ltd. (see [SC_Linxens]), Linxens Germany GmbH (see [SC_Linxens_DE]), HID Global Ireland Teoranta (see [SC_HID]), HID Global Malaysia (see [SC_HID_MY]) and NXP Semiconductors Germany GmbH (see [NXP_P71_ST]).

Note 4: In the case of NXP Semiconductors Germany GmbH being the *Manufacturer* performing initialization and pre-personalization, the deactivation of the Flash Loader can also be performed after the initialization/pre-personalization step.

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

(Inlay production) The MRTD manufacturer combines the IC with hardware for the contactless / contact interface in the passport book. The inlay production including the application of the antenna is NOT part of the TOE and takes part after the delivery.

Phase 3: Personalization of the MRTD (**Step 6**) The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrollment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object.

The signing of the Document security object by the Document signer [ICAO_9303] 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.

Phase 4: Operational Use (**Step 7**) The TOE is used as MRTD chip by the traveler 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 can be used according to the security policy of the issuing State but they can never be modified.

Non-TOE Hardware/Software/Firmware Required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

2 Conformance Claims (ASE_CCL.1)

2.1 CC Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 [CC_Part1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 [CC_Part2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1 Revision 5, April 2017 [CC_Part3]

as follows

- Part 2 extended
- Part 3 conformant

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1 Revision 5, April 2017 [CC_PartEM]

has to be taken into account.

2.2 PP Reference

The conformance of this ST to the Common Criteria Protection Profile - Machine Readable Travel Document with “ICAO Application”, Basic Access Control, BSI-CC-PP-0055 [CC_PP-0055] is claimed.

2.3 Package Claim

The assurance level for the TOE is CC EAL4 augmented with ALC_DVS.2 defined in CC part 3 [CC_Part3].

2.4 Conformance Claim Rationale

According section 2.2 this ST claims conformance to [CC_PP-0055]. “Application notes” included in the PP are only resumed, if they are of interest for the reader. In this case they are renamed to “Note” and renumbered consecutively. All other deviations are listed in Table 2.1 below. None of the changes causes a conflict between ST and PP.

Assurance Component	Description
ASE_INT.1 (see sec. 1)	The TOE is described in detail in compliance to the PP. A number of *Manufacturers* for initialization and pre-personalization is included.
ASE_CCL.1 (see sec. 2)	Conformance to CC Parts version 3.1 revision 5 (PP: revision 1 or 2, respectively) is claimed.
ASE_SPD.1 (see sec. 3)	No significant changes.
ASE_OBJ.2 (see sec. 4)	No significant changes.
ASE_ECD.1 (see sec. 5)	The component has not been resumed, but the reference to the according chapter of [CC_PP-0055] is given.
ASE_REQ.2 (see sec. 6)	In order to meet [BSI_AIS31] • FCS_RND.1 has been changed according to [CC_PP-0084] (FCS_RNG.1)

Table 2.1: Conformance claim rationale.

3 Security Problem Definition (ASE_SPD.1)

3.1 Introduction

Assets

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

Logical MRTD Data The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [ICAO_9303]. 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.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the Inspection System for the Chip Authentication and the Active Authentication Public Key (EF.DG15) for Active Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons the 'ICAO Doc 9303' [ICAO_9303] specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16)
- Chip Authentication Public Key in EF.DG14
- Active Authentication Public Key in EF.DG15
- Document Security Object (SOD) in EF.SOD
- Common data in EF.COM

A sensitive asset is the following more general one.

Authenticity of the MRTD's chip The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD.

Subjects

This Security Target considers the following subjects:

Manufacturer The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the phase 2 *Manufacturing*. The TOE does not

distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer. During pre-personalization the MRTD manufacturer (so-called Pre-Personalization Agent) prepares the TOE for the personalization, e.g. creation of data files.

Personalization Agent The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of 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 (v) signing the Document Security Object defined in [ICAO_9303].

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

Inspection system (IS) A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The **Basic Inspection System** (BIS) (i) contains a terminal for the contactless or contact based communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

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

Traveler Person presenting the MRTD to the Inspection System and claiming the identity of the MRTD holder.

Attacker A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

Note: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

3.2 Assumptions

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

A.MRTD_Manufact (MRTD manufacturing on steps 4 to 6)

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery (MRTD delivery during steps 4 to 6)

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent (Personalization of the MRTD's chip)

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys (Inspection Systems for global interoperability)

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO_9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

A.BAC-Keys (Cryptographic quality of Basic Access Control Keys)

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [ICAO_9303], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

3.3 Threats

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

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

T.Chip_ID (Identification of MRTD's chip)

Adverse action An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.

Threat agent Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset Anonymity of user.

T.Skimming (Skimming the logical MRTD)

Adverse action An attacker imitates an Inspection System trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.

Threat agent Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset Confidentiality of logical MRTD data.

T.Eavesdropping (Eavesdropping to the communication between TOE and Inspection System)

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

Threat agent Having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset Confidentiality of logical MRTD data.

T.Forgery (Forgery of data on MRTD's chip)

Adverse action An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical

MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

Threat agent Having enhanced basic attack potential, being in possession of one or more legitimate MRTDs.

Asset Authenticity of logical MRTD data.

The TOE shall avert the threats as specified below.

T.Abuse-Func (Abuse of Functionality)

Adverse action An attacker may use functions of the TOE which shall not be used in "Operational Use" phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

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

Threat agent Having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Information_Leakage (Information Leakage from MRTD's chip)

Adverse action 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).

Threat agent Having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality of logical MRTD and TSF data.

T.Phys-Tamper (Physical Tampering)

Adverse action 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) modify User Data or (iv) to modify TSF data.

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

Threat agent Having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Malfunction (Malfunction due to Environmental Stress)

Adverse action An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent Having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

3.4 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2 [CC_Part1]).

P.Manufact (Manufacturing of the MRTD's chip)

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

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

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

P.Personal_Data (Personal data protection policy)

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)[1] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by Inspection Systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO_9303].

Note 5: The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO_9303]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

[1] Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by [CC_PP-0055]

4 Security Objectives (ASE_OBJ.2)

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.

4.1 Security Objectives for the TOE

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

OT.AC_Pers (Access Control for Personalization of logical MRTD)

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO_9303] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Note 6: The OT.AC_Pers implies that

1. the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization
2. the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the “Operational Use” phase is optional.

OT.Data_Int (Integrity of personal data)

The TOE must ensure the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

OT.Data_Conf (Confidentiality of personal data)

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control

based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

Note 7: The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the Inspection System by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. This Security Objective requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [ICAO_9303] that the Inspection System derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this Security Target, but that of BSI-DSZ-CC-1147-V3. Thus the read access must be prevented even in case of a successful BAC Authentication.

OT.Identification (Identification and Authentication of the TOE)

The TOE must provide means to store IC Identification and Pre-Personalization 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*. The storage of the Pre-Personalization Data includes writing of the Personalization Agent Key(s).

In phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

Note 8: The TOE *Security Objective* OT.Identification addresses security features of the TOE to support the Life Cycle security in the Manufacturing and Personalization phases. The IC Identification Data are used for TOE identification in phase 2 and for traceability and/or to secure shipment of the TOE from phase 2 into the phase 3. This Security Objective addresses security features of the TOE to be used by the TOE manufacturing. In the phase 4 the TOE is identified by the Document Number as part of the printed and digital MRZ. This Security Objective forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless/contact interface before successful authentication as Basic Inspection System or as Personalization Agent.

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

OT.Prot_Abuse-Func (Protection against Abuse of Functionality)

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

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

OT.Prot_Inf_Leak (Protection against Information Leakage)

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

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

Note 9: This *Security Objective* pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper (Protection against Physical Tampering)

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

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

with a prior

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

OT.Prot_Malfunction (Protection against Malfunctions)

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

Note 10: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE's internals.

4.2 Security Objectives for the Operational Environment

Issuing State or Organization

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

OE.MRTD_Manufact (Protection of the MRTD Manufacturing)

Appropriate functionality testing of the TOE shall be used in step 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.MRTD_Delivery (Protection of the MRTD delivery)

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- Non-disclosure of any security relevant information
- Identification of the element under delivery
- Meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment)
- Physical protection to prevent external damage
- Secure storage and handling procedures (including rejected TOE's)
- Traceability of TOE during delivery including the following parameters:
  - Origin and shipment details
  - Reception, reception acknowledgment
  - Location material/information

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

OE.Personalization (Personalization of logical MRTD)

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign (Authentication of logical MRTD by Signature)

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute

the Certificate of the Country Signing CA Public Key to receiving States and organizations maintaining its authenticity and integrity. The issuing State or organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment 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 [ICAO_9303].

OE.BAC-Keys (Cryptographic quality of Basic Access Control Keys)

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [ICAO_9303] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

Receiving State or organization

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

OE.Exam_MRTD (Examination of the MRTD passport book)

The Inspection System of the receiving State must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO_9303].

OE.Passive_Auth_Verif (Verification by Passive Authentication)

The border control officer of the receiving State uses the Inspection System to verify the traveler as MRTD holder. The Inspection Systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing CA Public Key and the Document Signer Public Key maintaining their authenticity and availability in all Inspection Systems.

OE.Prot_Logical_MRTD (Protection of data of the logical MRTD)

The Inspection System of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

4.3 Security Objective Rationale

Table 4.1 provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				x									x			
T.Skimming			x										x			
T.Eavesdropping			x													
T.Forgery	x	x					x					x		x	x	
T.Abuse-Func					x						x					
T.Information_Leakage						x										
T.Phys-Tamper							x									
T.Malfunction								x								
P.Manufact				x												
P.Personalization	x			x							x					
P.Personal_Data		x	x													
A.MRTD_Manufact									x							
A.MRTD_Delivery										x						
A.Pers_Agent											x					
A.Insp_Sys														x		x
A.BAC-Keys													x			

Table 4.1: Security Objective Rationale

The OSP **P.Manufact** “Manufacturing of the MRTD’s chip” requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by **OT.Identification**.

The OSP **P.Personalization** “Personalization of the MRTD by issuing State or Organization only” addresses the (i) the enrollment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD”, and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD”. Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** “Identification and Authentication of the TOE”. The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

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

The threat **T.Chip_ID** “Identification of MRTD’s chip” addresses the trace of the MRTD movement by identifying remotely the MRTD’s chip through the contactless communication interface. This threat is countered as described by the security objective **OT.Identification** by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Skimming** “Skimming digital MRZ data or the digital portrait” and **T.Eavesdropping** “Eavesdropping to the communication between TOE and inspection system” address the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD’s chip and a terminal. This threat is countered by the security objective **OT.Data_Conf** “Confidentiality of personal data” through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Forgery** “Forgery of data on MRTD’s chip” addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. **OE.Personalization**). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** “Integrity of personal data” and **OT.Prot_Phys-Tamper** “Protection against Physical Tampering”. The examination of the presented MRTD passport book according to **OE.Exam_MRTD** “Examination of the MRTD passport book” shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** “Authentication of logical MRTD by Signature” and verified by the inspection system according **OE.Passive_Auth_Verif** “Verification by Passive Authentication”.

The threat **T.Abuse-Func** “Abuse of Functionality” addresses attacks of misusing MRTD’s functionality to disable or bypass the TSFs. The security objective for the TOE **OT.Prot_Abuse-Func** “Protection against abuse of functionality” ensures that the usage of functions which may not be used in the “Operational Use” 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. Additionally this objective is supported by the security objective for the TOE environment: **OE.Personalization** “Personalization of logical MRTD” ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

The threats **T.Information_Leakage** “Information Leakage from MRTD’s chip”, **T.Phys-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.MRTD_Manufact** “MRTD manufacturing on step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_Manufact** “Protection of the MRTD Manufacturing” that requires to use security procedures during all manufacturing steps.

The assumption **A.MRTD_Delivery** “MRTD delivery during step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_Delivery** “Protection of the MRTD delivery” that requires to use security procedures during delivery steps of the MRTD.

The assumption **A.Pers_Agent** “Personalization of the MRTD’s chip” is covered by the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD” including the enrollment, the protection with digital signature and the storage of the MRTD holder personal data.

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objectives for the TOE environment **OE.Exam_MRTD** “Examination of the MRTD passport book”. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** “Protection of data from the logical MRTD” require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

The assumption **A.BAC-Keys** “Cryptographic quality of Basic Access Control Keys” is directly covered by the security objective for the TOE environment **OE.BAC-Keys** “Cryptographic quality of Basic Access Control Keys” ensuring the sufficient key quality to be provided by the issuing State or Organization.

5 Extended Components Definition (ASE_ECD.1)

This Security Target uses the components defined in chapter 5 of [CC_PP-0055]. The security requirement FCS_RND.1 has been changed according to the security requirement FCS_RNG.1 defined in [CC_PP-0084] to meet [BSI_AIS31]. No other components are used.

6 Security Requirements (ASE_REQ.2)

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 of the CC [CC_Part1]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by showing added/changed words 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 are denoted 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 filled in by the ST author are denoted as double-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 definition of the subjects "Manufacturer", "Personalization Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in chapter 8 or in the following table. The operations "write", "modify", "read" and " disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and "re-authenticate" are originally taken from [CC_Part2]. The operation "load" is synonymous to "import" used in [CC_Part2].

Definition of security attributes

Terminal authentication status

none (any Terminal) default role (i.e. without authorization after start-up)

Basic Inspection System terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.

Personalization Agent Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

6.1 Security Functional Requirements for the TOE

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

6.1.1 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 [CC_Part2] extended).

FAU_SAS.1	Audit storage
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.

Note 11: The Manufacturer role is the default user identity assumed by the TOE in the phase 2 *Manufacturing*. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.1.2 Class Cryptographic Support (FCS)

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2 [CC_Part2]). The iterations are caused by different cryptographic key generation algorithms to be implemented and keys to be generated by the TOE.

FCS_CKM.1	Cryptographic key generation – Generation of Document Basic Access Keys by the TOE
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [ICAO_9303], normative appendix 5.

Note 12: The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [ICAO_9303], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO_9303], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2 [CC_Part2]).

FCS_CKM.4	**Cryptographic key destruction**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion of key value by overwriting with zero or random numbers that meets the following: none.

Note 13: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

6.1.2.1 Cryptographic Operation (FCS_COP.1)

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2 [CC_Part2]). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA	**Cryptographic operation – Hash for Key Derivation by MRTD**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: [FIPS_180-4], **in detail sections 6.1 and 6.2**.

FCS_COP.1/ENC	**Cryptographic operation – Encryption / Decryption Triple DES**
Hierarchical to:	No other components.

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ENC	The TSF shall perform Secure Messaging (BAC) - encryption and decryption in accordance with a specified cryptographic algorithm 3DES in CBC mode and cryptographic key size 112 bit that meet the following: [NIST_SP800-67] and [ISO_10116], sec. 7.

Note 14: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

FCS_COP.1/AUTH	**Cryptographic operation – Authentication**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication - encryption and decryption in accordance with a specified cryptographic algorithm AES **in CBC mode** and cryptographic key sizes 128 bit that meet the following: [ISO_18013-3] Annex B, [ISO_10116], sec. 7, and [FIPS_197].

Note 15: This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

Informative: The usage of Secure Messaging for the personalization in accordance with the cryptographic algorithm AES in CBC mode and cryptographic key size 128 bit is within the scope of certification BSI-DSZ-CC-1147-V3.

FCS_COP.1/MAC	**Cryptographic operation – Retail MAC**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: [NIST_SP800-67] and [ISO_9797-1], MAC Algorithm 3 (Retail-MAC), **in section 7.4**.

Note 16: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

6.1.2.2 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 [CC_Part2]).

FCS_RND.1	**Random number generation (Class PTG.3)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a [hybrid physical] random number generator that implements: (PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output. (PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source. (PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected. (PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon. (PTG.3.5) The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting nontolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time. (PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.
FCS_RND.1.2	The TSF shall provide octets of bits that meet: (PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A none.[1] (PTG.3.8) The internal random numbers shall use PTRNG of class PTG.2 as random source for the postprocessing.

[1] See [KiSch-RNG] Section 2.4.4.

Note 17: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

Note 18: This SFR has been changed according to [CC_PP-0084] (FCS_RNG.1) and justified in [KiSch-RNG] chapter 3 (PTG.3) to meet [BSI_AIS31].

6.1.3 Class FIA Identification and Authentication

Note 19: Table 6.1 provides an overview on the authentication mechanisms used.

Name	**SFR for the TOE**	**Algorithms and key sizes** according to [ICAO_9303] and [BSI_TR-03110]
Basic Access Control Authentication Mechanism	FIA_AFL.1, FIA_UAU.4, FIA_UAU.6	Triple-DES, 112 bit keys; Retail-MAC, 112 bit keys
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	AES, 128 bit keys

Table 6.1: Overview on authentication SFR

The TOE shall meet the requirement “Timing of identification (FIA_UID.1)” as specified below (Common Criteria Part 2 [CC_Part2]).

FIA_UID.1	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow 1. to read the Initialization Data in phase 2 “Manufacturing” 2. to read the random identifier in phase 3 “Personalization of the MRTD” 3. to read the random identifier in phase 4 “Operational Use” 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.

Note 20: The IC manufacturer and the MRTD manufacturer write the initialization data and/or pre-personalization data in the audit records of the IC during the phase 2 “Manufacturing”. The audit records can be written only in the phase 2 “Manufacturing of the TOE”. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer creates the user role Personalization Agent for transition from phase 2 to phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting

the authentication key. After personalization in the phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

Note 21: In the "operational use" phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD's chip use a randomly chosen identifier for the communication channel to allow the terminal to communicate with more then one RFID. This identifier will not violate the OT.Identification.

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2 [CC_Part2]).

FIA_UAU.1	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1	The TSF shall allow 1. to read the Initialization Data in phase 2 "Manufacturing" 2. to read the random identifier in phase 3 "Personalization of the MRTD" 3. to read the random identifier in phase 4 "Operational Use" on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Note 22: The Basic Inspection System and the Personalization Agent authenticate themselves.

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2 [CC_Part2]).

FIA_UAU.4	**Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism 2. Authentication Mechanism based on 3DES, AES

Note 23: The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.

Note 24: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO_9303]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2 [CC_Part2]).

FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide 1. Basic Access Control Authentication Mechanism 2. Symmetric Authentication Mechanism based on 3DES, AES to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: 1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms (a) the Basic Access Control Authentication Mechanism with Personalization Agent Keys (b) the Symmetric Authentication Mechanism with Personalization Agent Key 2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys

Note 25: Because the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control' [CC_PP-0056-V2] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES, but using the Terminal Authentication Protocol using the Personalization Key (cf. [CC_PP-0056-V2] FIA_UAU.5.2).

Note 26: The Basic Access Control Mechanism includes the Secure Messaging for all commands exchanged after successful authentication of the inspection system. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2 [CC_Part2]).

FIA_UAU.6	**Re-authenticating – Re-authenticating of Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

Note 27: The Basic Access Control Mechanism specified in [ICAO_9303] includes the Secure Messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by Secure Messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

Note 28: Note that in case the TOE should also fulfill [CC_PP-0056-V2] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.6)" as specified below (Common Criteria Part 2 [CC_Part2]).

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when 1 unsuccessful authentication attempt occurs related to BAC authentication.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall wait for an administrator configurable time of at least 1 second between the reception of the authentication command and its processing.

Note 29: The TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 consecutive unsuccessful authentication attempts occur related to BAC authentication protocol. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall wait for an administrator configurable time between the receiving the terminal challenge eIFD and sending the TSF response eICC during the BAC authentication attempts. The terminal challenge eIFD and the TSF response eICC are described in [BSI_TR-03110], Appendix C. The refinement by inclusion of the word "consecutive" allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the "consecutive unsuccessful authentication attempts" are count independent on power-on sessions but reset to zero after successful authentication only.

Note 30: The Personalization Agent chooses from a list provided by the Manufacturer the configuration of the authentication failure handling.

6.1.4 Class FDP User Data Protection

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2 [CC_Part2]).

FDP_ACC.1	**Subset access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2 [CC_Part2]).

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1	The TSF shall enforce the Basic Access Control SFP to objects based on the following: 1. Subjects: (a) Personalization Agent (b) Basic Inspection System (c) Terminal 2. Objects: (a) data EF.DG1 to EF.DG16 of the logical MRTD (b) data in EF.COM (c) data in EF.SOD 3. Security attributes: (a) authentication status of terminals.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD 2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following sensitive rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rules: 1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD 2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD 3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.

Note 31: The inspection system needs special authentication and authorization for read access to DG3 and DG4 defined in [CC_PP-0056-V2].

6.1.4.1 Inter-TSF-Transfer

Note 32: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2 [CC_Part2]).

FDP_UCT.1	Basic data exchange confidentiality – MRTD
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1	The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure.

The TOE shall meet the requirement “Data exchange integrity (FDP_UIT.1)” as specified below (Common Criteria Part 2 [CC_Part2]).

FDP_UIT.1	Data exchange integrity – MRTD
Hierarchical to:	No other components.
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]
FDP_UIT.1.1	The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred

6.1.5 Class FMT Security Management

Note 33: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

The TOE shall meet the requirement “Specification of Management Functions (FMT_SMF.1)” as specified below (Common Criteria Part 2 [CC_Part2]).

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

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization 2. Pre-personalization 3. Personalization

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below (Common Criteria Part 2 [CC_Part2]).

FMT_SMR.1	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles: 1. Manufacturer 2. Personalization Agent 3. Basic Inspection System
FMT_SMR.1.2	The TSF shall be able to associate users with roles

Note 34: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1” as specified below (Common Criteria Part 2 [CC_Part2] extended).

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: 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 4. Substantial information about construction of TSF to be gathered which may enable other attacks

The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below (Common Criteria Part 2 [CC_Part2] extended).

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their capabilities 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 4. Substantial information about construction of TSF to be gathered which may enable other attacks

Note 35: The formulation of “Deploying Test Features ...” in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term “software” in item 3 of FMT_LIM.1.1and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

The TOE shall meet the requirement “Management of TSF data (FMT_MTD.1)” as specified below (Common Criteria Part 2 [CC_Part2]). 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.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer

Note 36: The Pre-personalization Data include but are not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

FMT_MTD.1/INI_DIS	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent

Note 37: According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE restricts the ability to write the Initialization Data and the Prepersonalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the phase 2. The IC Manufacturer writes the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the phase 2 and 3 “personalization” but is not needed and may be misused in the phase 4 “Operational Use”. Therefore the external read access will be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

FMT_MTD.1/KEY_WRITE	Management of TSF data – Key Write
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent

FMT_MTD.1/KEY_READ	Management of TSF data – Key Read
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none

Note 38: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access keys.

6.1.6 Class FPT Protection of Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF

testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFR "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 [CC_Part2] extended).

FPT_EMSEC.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall not emit information retrievable by side channel attacks in excess of non-useful information enabling access to Personalization Agent Key(s) and transport keys.
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts **and contactless I/O** to gain access to Personalization Agent Key(s) and transport keys.

Note 39: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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 [CC_Part2]).

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

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to out-of-range operating conditions where therefore a malfunction could occur 2. failure detected by TSF according to FPT_TST.1

The TOE shall meet the requirement “TSF testing (FPT_TST.1)” as specified below (Common Criteria Part 2 [CC_Part2]).

FPT_TST.1	**TSF testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up and at the condition “request of random numbers“ to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

The TOE shall meet the requirement “Resistance to physical attack (FPT_PHP.3)” as specified below (Common Criteria Part 2 [CC_Part2]).

FPT_PHP.3	Resistance to physical attack
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

Note 40: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

6.2 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 EAL4

and augmented by taking the following components:

- ALC_DVS.2

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The table 6.2 provides an overview for security functional requirements coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					
FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_RND.1	x	x	x					
FIA_UID.1			x	x				
FIA_AFL.1			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4	x	x	x					
FIA_UAU.5	x	x	x					
FIA_UAU.6	x	x	x					
FDP_ACC.1	x	x	x					
FDP_ACF.1	x	x	x					
FDP_UCT.1	x	x	x					

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FDP_UIT.1	x	x	x					
FMT_SMF.1	x	x	x					
FMT_SMR.1	x	x	x					
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA				x				
FMT_MTD.1/INI_DIS				x				
FMT_MTD.1/KEY_WRITE	x	x	x					
FMT_MTD.1/KEY_READ	x	x	x					
FPT_EMSEC.1	x				x			
FPT_TST.1					x		x	
FPT_FLS.1	x				x		x	
FPT_PHP.3	x				x	x		

Table 6.2: Coverage of Security Objectives for the TOE by SFR

OT.AC_Pers The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with [CC_PP-0056-V2] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication

reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

OT.Data_Int 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 of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_ COP.1/AUTH.

The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 require the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

OT.Data_Conf The security objective **OT.Data_Conf** "Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests Secure Messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC for key generation(cf. the SFR FDP_UCT.1 and FDP_UIT.1), and FCS_COP.1/ENC and FCS_COP.1/ MAC for the

ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

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

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

Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

OT.Prot_Abuse-Func The security objective **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality" is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

OT.Prot_Inf_Leak 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 SFRs 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

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

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

6.3.2 Dependency Rationale

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

Table 6.3 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptogr. key distribution or FCS_COP.1 Cryptogr. operation],	Fulfilled by FCS_COP.1/ENC, and FCS_COP.1/MAC,
	FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation]	Fulfilled by FCS_CKM.1
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation],	justification 1 for non-satisfied dependencies
	FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation],	Fulfilled by FCS_CKM.1,
	FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation],	justification 2 for non-satisfied dependencies

SFR	Dependencies	Support of the Dependencies
	FCS_CKM.4 Cryptogr. key destruction	justification 2 for non-satisfied dependencies
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation], FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.1, Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FCS_UID.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 3 for non-satisfied dependencies
FDP_UCT.1	[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 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[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 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/ KEY_WRITE	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ KEY_READ	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 6.3: Dependencies between the SFR for the TOE

Justification for non-satisfied dependencies between the SFR for TOE

No. 1 The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1 nor an import (FDP_ITC.1/2) is necessary.

No. 2 The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE life cycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

No. 3 The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

No. 4 The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS respectively GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

6.3.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.

The component ALC_DVS.2 has no dependencies.

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together 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 6.3.2 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 analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the additional assurance in section 6.3.3 Security Assurance Requirements Rationale components 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 6.3.2 Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 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.

7 TOE Summary Specification (ASE_TSS.1)

This chapter describes the TOE security functions and the assurance measures covering the requirements of the previous chapter.

7.1 TOE Security Functions

This chapter gives the overview description of the different TOE Security Functions composing the TSF.

7.1.1 TOE Security Functions from Hardware (IC) and Cryptographic Library

7.1.1.1 F.IC_CL: Security Functions of the Hardware (IC) and Cryptographic Library

This security function covers the security functions of the hardware and the cryptographic library. The Security Target of the hardware [NXP_P71_ST] defines the following security functionalities, which are grouped in TSF portions:

TSF portion	Title	Description
TSF.Service	Service functionality beside cryptographic operations	This portion of the TSF comprises • random number generation, • reconfiguration of the TOE features, • self-test functionality, • a secure channel for using the Flash Loader and • provides mechanisms to store initialization, pre-personalization, and/or other data on the TOE.

TSF portion	Title	Description
TSF.Protection	General security measures to protect the TSF	This portion of the TSF • comprises physical and logical protection to avoid information leakage, • detect fault injection, • defines resets in case an error or attack was detected and • guarantees that memories used by the cryptographic libraries are cleared before other applications can access these memories.
TSF.Control	Operating conditions, memory and hardware access control	This portion of the TSF • controls the operating conditions and • manages the access rights to memories and peripherals for the different TOE modes.
TSF.Crypto	Crypto Service	This portion of the TSF • provides cryptographic functionality such as TDES and AES in different modes depending on the availability of the N7121 Crypto Library and • covers asymmetric cryptography (RSA and ECC over GF(p)) and hashing.

Table 7.1: Security functionality provided by the hardware and cryptographic library.

7.1.2 TOE Security Functions from Embedded Software (ES) – Operating system

7.1.2.1 F.Access_Control

This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. This function consists of following elements:

1. Access to objects is controlled based on subjects, objects (any file) and security attributes.
2. No access control policy allows reading of any key.
3. Any access not explicitly allowed is denied.
4. Access control in phase 2 – initialization/pre-personalization – enforces initialization and pre-personalization policy: configuration and initialization of the TOE, configuring of Access Control policy and doing key management only by the manufacturer (Initialization/Pre-personalization Agent) or on behalf of him (see F.Management).

5. Access control in phase 3 – personalization – enforces personalization policy: writing of user data, keys (Basic Access Control) and reading of initialization data only by the Personalization Agent identified with its authentication key (see F.Management).
6. Access control in phase 4 – operational use – enforces operational use policy: reading of user data by BIS authenticated at least by Secure Messaging with BAC.

7.1.2.2 F.Identification_Authentication

This function provides identification/authentication of the user roles

- Manufacturer (Initialization/Pre-personalization Agent),
- Personalization Agent and
- Basic Inspection System

by the methods:

1. **Personalization** phase:
   - Symmetric authentication [FIPS_197, NIST_SP800-38B] with following properties:
     - It uses a challenge from the TOE.
     - The cryptographic method for confidentiality is AES-128/CBC provided by F.Crypto.
     - The cryptographic method for authenticity is CMAC provided by F.Crypto.
     - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
     - After three consecutive failed authentication attempts the authentication method is blocked and the key is no longer usable (retry counter with a value of 3).
     - A usage counter of 50.000 prevents the unlimited usage of the key. The counter cannot be reset. After the limit is reached, the key is irreversibly blocked.
     - On success the session keys are created and stored for Secure Messaging.
     - Keys and data in transient memory are overwritten after usage.
   - Secure Messaging with following properties:
     - The cryptographic method for confidentiality is AES-128/CBC provided by F.Crypto.
     - The cryptographic method for authenticity is CMAC provided by F.Crypto.
     - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
     - The initialization vector is an encrypted Send Sequence Counter (SSC) for encryption and MAC.
     - A session key is used.
     - The Secure Messaging session is limited by a Secure Messaging counter of 500.000; the decrease of the counter is depending on the length of the command and response APDUs. If a new Secure Messaging session is started, the counter is reset to 500.000.
     - Upon any command that is not protected correctly with the session keys these are overwritten according to [FIPS_140-3] (or better) and a new authentication is required.

  - Keys and data in transient memory are overwritten after usage.

2. **Operational use** phase:
   - Symmetric BAC authentication method [ICAO_9303] with following properties:
     - The authentication is as specified by ICAO.
     - It uses a challenge from the MRTD.
     - The method can be configured by the administrator to delay the processing of the authentication command after a failed authentication.
     - The cryptographic method for confidentiality is Triple-DES/CBC provided by F.Crypto.
     - The cryptographic method for authenticity is DES/Retail MAC provided by F.Crypto.
     - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
     - On success the session keys are created and stored for Secure Messaging.
   - Secure Messaging with following properties:
     - The Secure Messaging is as specified by ICAO.
     - The cryptographic method for confidentiality is Triple-DES/CBC provided by F.Crypto.
     - The cryptographic method for authenticity is DES/Retail MAC provided by F.Crypto.
     - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
     - The initialization vector is an encrypted Send Sequence Counter (SSC).
     - In phases 3 and 4 a session key is used.
     - The Secure Messaging session is limited by a Secure Messaging counter of 500.000; the decrease of the counter is depending on the length of the command and response APDUs. If a new Secure Messaging session is started, the counter is reset to 500.000.
     - On any command that is not protected correctly with the session keys these are overwritten according to [FIPS_140-3] (or better) and a new BAC authentication is required.
     - Keys in transient memory are overwritten after usage.

7.1.2.3 F.Management

In phase 2 the Manufacturer (Initialization/Pre-personalization Agent) performs the initialization and configures the file layout including security attributes. In any case the layout determines that the parameters given in F.Access_Control for phases 3 and 4 are enforced. The agent can also do key management and other administrative tasks.

In phase 3 the Personalization Agent performs the following steps:

- Formatting of all data to be stored in the TOE according to ICAO requirements which are outside the scope of the TOE. The data to be formatted includes the index file, data groups, Passive Authentication data, BAC key derived from the Machine Readable Zone data and parameters.
- Writing of all the required data to the appropriate files as specified in [ICAO_9303].

- Changing the TOE into the end-usage mode for phase 4 where reading of the initialization data is prevented.

7.1.2.4 F.Crypto

This function provides the implementation to

- DES (supplied by F.IC_CL)
- 3DES/CBC (supplied by F.IC_CL)
- DES/Retail MAC (supported by F.IC_CL)
- AES (supplied by F.IC_CL) used in phase 3
- CMAC used in phase 3

This function implements the hash algorithms according to [FIPS_180-4]

- SHA-1 (supplied by F.IC_CL)

7.1.2.5 F.Verification

TOE internal functions ensures correct operation.

7.2 Assurance Measures

The assurance measures fulfilling the requirements of EAL4 augmented with ALC_DVS.2 is given in table 7.2.

Measure	Measure
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures, automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample

Measure	Measure
AVA_VAN.3	Focused vulnerability analysis

Table 7.2: Assurance Measures

7.3 TOE Summary Specification Rationale

Table 7.3 shows the coverage of the SFRs by TSFs.

SFR	TSFs
FAU_SAS.1	F.IC_CL
FCS_CKM.1	F.IC_CL
FCS_CKM.4	F.Identification_Authentication
FCS_COP.1/SHA	F.IC_CL, F.Crypto
FCS_COP.1/ENC	F.IC_CL, F.Crypto
FCS_COP.1/AUTH	F.IC_CL, F.Crypto
FCS_COP.1/MAC	F.IC_CL, F.Crypto
FCS_RND.1	F.IC_CL
FIA_UID.1	F.Access_Control
FIA_UAU.1	F.Access_Control
FIA_UAU.4	F.Identification_Authentication
FIA_UAU.5	F.Access_Control, F.Identification_Authentication
FIA_UAU.6	F.Identification_Authentication
FIA_AFL.1	F.Access_Control, F.Identification_Authentication
FDP_ACC.1	F.Access_Control
FDP_ACF.1	F.Access_Control
FDP_UCT.1	F.Identification_Authentication
FDP_UIT.1	F.Identification_Authentication
FMT_SMF.1	F.Management
FMT_SMR.1	F.Identification_Authentication
FMT_LIM.1	F.IC_CL
FMT_LIM.2	F.IC_CL
FMT_MTD.1/INI_ENA	F.IC_CL, F.Access_Control
FMT_MTD.1/INI_DIS	F.Access_Control, F.Management
FMT_MTD.1/KEY_WRITE	F.Access_Control
FMT_MTD.1/KEY_READ	F.Access_Control
FPT_EMSEC.1	F.IC_CL
FPT_FLS.1	F.IC_CL
FPT_TST.1	F.IC_CL, F.Verification
FPT_PHP.3	F.IC_CL

Table 7.3: Coverage of SFRs for the TOE by TSFs.

The SFR **FAU_SAS.1** requires the storage of the chip identification data which is addressed in **F.IC_CL (TSF.Service)**.

The SFR **FCS_CKM.1** requires the BAC key derivation algorithm, which is supplied by the BAC authentication mechanism of **F.Identification_Authentication**.

The SFR **FCS_CKM.4** requires the destroying of cryptographic keys. This is done in **F.Identification_Authentication** ("Overwrites keys in transient memory after usage").

The SFR **FCS_COP.1/SHA** requires SHA-1. **F.IC_CL (TSF.Crypto)** and **F.Crypto** provide this hash algorithm.

The SFR **FCS_COP.1/ENC** requires Triple-DES in CBC mode and cryptographic key size 112 bit to perform Secure Messaging - encryption and decryption. This is provided by **F.IC_CL (TSF.Crypto)** and **F.Crypto**.

The SFR **FCS_COP.1/AUTH** requires AES in CBC mode and cryptographic key size 128 bit to perform Secure Messaging - encryption and decryption. This is provided by **F.IC_CL (TSF.Crypto)** and **F.Crypto**.

The SFR **FCS_COP.1/MAC** requires Triple-DES in Retail MAC mode and cryptographic key size 112 bit to perform Secure Messaging - Message Authentication Code. This is provided by **F.Crypto**.

The SFR **FCS_RND.1** requires the generation of random numbers which is provided by **F.IC_CL (TSF.Service)**. The provided random number generator produces cryptographically strong random numbers which are used at the appropriate places as written in the addition there.

The SFR **FIA_UID.1** requires timing of identification. It is handled by **F.Access_Control** which enforces identification of a role before access is granted ("...only executed after this TSF allowed access"). Also all policies prevent reading sensitive or user dependent data without user identification.

The SFR **FIA_UAU.1** requires timing of authentication. It is handled by **F.Access_Control** which enforces authentication of a role before access is granted ("...only executed after this TSF allowed access"). Also all policies prevent reading sensitive or user dependent data without user authentication.

The SFR **FIA_UAU.4** requires prevention of authentication data reuse. This is in particular fulfilled by using changing initialization vectors in Secure Messaging. Secure Messaging is provided by **F.Identification_Authentication**.

The SFR **FIA_UAU.5** requires Basic Access Control authentication mechanism and symmetric authentication mechanism based on Triple-DES. In addition SFR **FIA_UAU.5** also requires the authentication of any user's claimed identity. **F.Identification_Authentication** and **F.Access_Control** fulfill these requirements.

The SFR **FIA_UAU.6** requires re-authentication for each command after successful authentication. This is done by **F.Identification_Authentication** providing Secure Messaging.

The SFR **FIA_AFL.1** requires the detection of an unsuccessful authentication attempt and the waiting for a specified time between the reception of an authentication command and its processing. **F.Identification_Authentication** detects unsuccessful authentication attempts and can be used "to delay the processing of the authentication command after a failed authentication command".

The SFR **FDP_ACC.1** requires the enforcement of the access control policy on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16. This is done by F.Access_Control (based on the objects: “a. data EF.DG1 to EF.DG16 ...”).

The SFR **FDP_ACF.1** requires the enforcement of the access control policy which is done by **F.Access_Control** (“Access to objects is controlled based on subjects, objects (any files) and security attributes”).

The SFR **FDP_UCT.1** requires the transmitting and receiving data protected from unauthorized disclosure after Basic Access Control. This is done by using an encrypted communication channel, which is based on Secure Messaging provided by **F.Identification_Authentication**.

The SFR **FDP_UIT.1** requires the transmitting and receiving data protected from modification, deletion, insertion and replay after Basic Access Control. This is done by using an protected communication channel. This channel is based on Secure Messaging provided by **F.Identification_Authentication**. A send sequence counter makes each command unique while the authenticity method makes it possible to detect modifications.

The SFR **FMT_SMF.1** requires security management functions for initialization, personalization and configuration. This is done by **F.Management**: The Manufacturer (Initialization/Pre-personalization Agent) performs the Initialization and configures the file layout in phase 2, the Personalization Agent performs the personalization in phase 3.

The SFR **FMT_SMR.1** requires the maintenance of roles. The roles are managed by **F.Identification_Authentication**.

The SFR **FMT_LIM.1** requires limited capabilities of test functions which is provided by **F.IC_CL (TSF.Control)** which controls what commands can be executed thereby preventing external usable test functions to do harm. The IC Dedicated Test Software only is available in the test mode.

The SFR **FMT_LIM.2** requires limited availabilities of test functions which is provided by **F.IC_CL (TSF.Control)** which controls what commands can be executed thereby preventing external usable test functions to do harm and the access to memory and special function registers. The IC Dedicated Test Software only is available in the test mode.

The SFR **FMT_MTD.1/INI_ENA** requires writing of Initialization data and Pre-personalization data to the manufacturer. Writing of Pre-personalization and Installation data only by the manufacturer is enforced by **F.Access_Control**, which limits these operations to phase 2. In addition **F.IC_CL (TSF.Control)** stores this data in the User Read Only Area which cannot be changed afterwards.

The SFR **FMT_MTD.1/INI_DIS** requires only the Personalization agent to be able to disable reading of the Initialization data. This is provided by **F.Management** (Personalization agent: “Changing the TOE into the end-usage mode for phase 4 where reading of the Initialization data is prevented”) and **F.Access_Control**.

The SFR **FMT_MTD.1/KEY_WRITE** requires the Personalization agent to be able to write the Document Basic Access Keys. This is provided by **F.Access_Control** allowing the personalization agent in phase 3 to write all necessary data.

The SFR **FMT_MTD.1/KEY_READ** requires the Document Basic Access Keys and the Personalization Agent Keys to never be readable. This is enforced by **F.Access_Control**, which does not allow reading of any key to any role.

The SFR **FPT_EMSEC.1** requires limiting of emanations. This is provided by **F.IC_CL (TSF.Control)**.

The SFR **FPT_FLS.1** requires failure detection and preservation of a secure state. This is provided by **F.IC_CL (TSF.Protection, TSF.Control)**. The security functions audit continually and react to environmental and other problems by bringing the IC into a secure state.

The SFR **FPT_TST.1** requires testing for (a) correct operation, (b) integrity of data and (c) integrity of executable code. **F.Verification** does this testing. **F.IC_CL (TSF.Protection)** controls all NVM and FLASH content for integrity.

The SFR **FPT_PHP.3** requires resistance to physical manipulation and probing. This is provided by **F.IC_CL (TSF.Protection)** which is provided by the hardware to resist attacks.

7.4 Statement of Compatibility

This is a statement of compatibility between this composite Security Target and the Security Target of P71D352 (N7121) [NXP_P71_ST].

7.4.1 Relevance of Hardware TSFs

All security functions of the hardware and cryptographic library that are used by the TOE (see Table 7.1) are relevant for the composite Security Target.

7.4.2 Compatibility: TOE Security Environment

7.4.2.1 Security Objectives

Table 7.4 gives a mapping of the hardware security objectives to those of the composite ST. .

HW objective	Matches TOE objective	Remarks
O.Leak-Inherent (protection against inherent information leakage)	OT.Prot_Inf_Leak	
O.Phys-Probing (protection against physical probing)	OT.Prot_Inf_Leak OT.Prot_Phys-Tamper	
O.Malfunction (protection against malfunctions)	OT.Prot_Inf_Leak OT.Prot_Malfunction	
O.Phys-Manipulation (protection against physical manipulation)	OT.Prot_Inf_Leak OT.Prot_Phys-Tamper	
O.Leak-Forced (protection against forced information leakage)	OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper	

HW objective	Matches TOE objective	Remarks
O.Abuse-Func (protection against abuse of functionality)	OT.Prot_Abuse-Func OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper	
O.Identification (TOE identification)	OT.Identification	
O.RND (random numbers)	OT.Data_Int OT.Data_Conf OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper	
O.Cap_Avail_Loader (capability and availability of the loader)	–	not applicable (the loader is deactivated before delivery)
O.Ctrl_Auth_Loader (optional) (access control and authenticity for the loader)	–	not applicable (the loader is deactivated before delivery)
O.TDES (cryptographic service Triple-DES)	OT.Data_Int OT.Data_Conf	
O.AES (cryptographic service AES)	OT.Data_Int	
O.SHA (cryptographic service hash function)	OT.Data_Int OT.Data_Conf	
O.NVM-Integrity (integrity support of data stored to NVM)	–	no conflict
O.Access-Control (access control to memories and special function registers)	–	no conflict
O.Self-Test (self-test)	OT.Prot_Inf_Leak OT.Prot_Malfunction	
O.PUF (optional) (sealing/unsealing user data)	–	no conflict
O.Secure-User-Mode-Box (optional) (secure user mode box firewall)	–	no conflict
O.RSA (RSA functionality (optional))	–	no conflict
O.ECC (elliptic-curve cryptography over GF(p) (optional))	–	no conflict
OE.Resp-Appl (treatment of user data)	–	no conflict
OE.Process-Sec-IC (protection during composite product manufacturing)	–	no conflict

HW objective	Matches TOE objective	Remarks
OE.Lim_Block_Loader (limitation of capability and blocking the loader)	–	not applicable (the loader is deactivated before delivery)
OE.Loader_Usage (optional) (secure communication and usage of the Loader)	–	not applicable (the loader is deactivated before delivery)
OE.Check-Init (check of initialization data by the security IC embedded software)	–	no conflict

Table 7.4: Mapping of hardware to TOE security objectives including those of the environment.

7.4.2.2 Security Requirements

Table 7.5 addresses the platform security requirements and their relevance for the TOE. Neither the SFRs that can be mapped to the platform SFRs nor those that are application specific (and thus not listed in the table) show any conflicts with the platform SFRs.

HW SFRs	Matches TOE SFR	Remarks
FRU_FLT.2 (limited fault tolerance)	FPT_FLS.1 FPT_TST.1	
FPT_FLS.1 (failure with preservation of secure state)	FPT_FLS.1	
FMT_LIM.1 (limited capabilities)	FMT_LIM.1	
FMT_LIM.2 (limited availability)	FMT_LIM.2	
FAU_SAS.1 (audit storage)	FAU_SAS.1	
FDP_SDC.1 (stored data confidentiality)	–	used implicitly, no conflict
FDP_SDI.2 (stored data integrity monitoring and action)	–	used implicitly, no conflict
FPT_PHP.3 (resistance to physical attack)	FPT_PHP.3	
FDP_ITT.1 (basic internal transfer protection)	FPT_EMSEC.1	
FPT_ITT.1 (basic internal TSF data transfer protection)	FPT_EMSEC.1	

HW SFRs	Matches TOE SFR	Remarks
FDP_IFC.1 (subset information flow control)	FPT_EMSEC.1	
FCS_RNG.1/PTG.2 (random number generation – PTG.2)	FCS_RND.1	
FMT_LIM.1/Loader (limited capabilities – loader)	–	not applicable (loader deactivated before delivery)
FMT_LIM.2/Loader (limited availability – loader)	–	not applicable (loader deactivated before delivery)
FTP_ITC.1/Loader (inter-TSF trusted channel (optional))	–	not applicable (loader deactivated before delivery)
FDP_UCT.1/Loader (basic data exchange confidentiality (optional))	–	not applicable (loader deactivated before delivery)
FDP_UIT.1/Loader (data exchange integrity (optional))	–	not applicable (loader deactivated before delivery)
FDP_ACC.1/Loader (subset access control – loader (optional))	–	not applicable (loader deactivated before delivery)
FDP_ACF.1/Loader (security attribute based access control – loader (optional))	–	not applicable (loader deactivated before delivery)
FCS_COP.1/TDES (cryptographic operation – TDES)	–	used implicitly with crypto library, no conflict
FCS_CKM.4/TDES (cryptographic key destruction – TDES)	–	used implicitly, no conflict
FCS_COP.1/AES (cryptographic operation – AES)	–	used implicitly with crypto library, no conflict
FCS_CKM.4/AES (cryptographic key destruction – AES)	–	used implicitly, no conflict
FCS_COP.1/TDES_LIB (cryptographic operation – TDES – crypto library (optional))	FCS_COP.1/ENC FCS_COP.1/MAC	
FCS_CKM.4/TDES_LIB (cryptographic key destruction – crypto library (optional))	–	used implicitly, no conflict
FCS_COP.1/AES_LIB (cryptographic operation – AES – crypto library (optional))	FCS_COP.1/AUTH	
FCS_CKM.4/AES_LIB (cryptographic key destruction – crypto library (optional))	–	used implicitly, no conflict

HW SFRs	Matches TOE SFR	Remarks
FCS_RNG.1/DRG.4 (random number generation – hybrid deterministic (optional))	–	not used by the TOE, no conflict
FCS_RNG.1/PTG.3 (random number generation – hybrid physical (optional))	FCS_RND.1	
FCS_COP.1/RSA (cryptographic operation – RSA (optional))	–	not used by the TOE, no conflict
FCS_CKM.1/RSA_KeyGen (Cryptographic Key Generation – RSA (optional))	–	not used by the TOE, no conflict
FCS_CKM.4/RSA (cryptographic key destruction – RSA (optional))	–	not used by the TOE, no conflict
FCS_CKM.5/RSA_PubkeyDerivation (Cryptographic key derivation – RSA public key computation (optional))	–	not used by the TOE, no conflict
FCS_COP.1/ECDSA (cryptographic operation – ECDSA (optional))	–	not used by the TOE, no conflict
FCS_COP.1/ECC_DHKE (cryptographic operation – Diffie-Hellman key exchange (optional))	–	not used by the TOE, no conflict
FCS_CKM.1/ECC_KeyGen (Cryptographic Key Generation – ECC (optional))	–	not used by the TOE, no conflict
FCS_CKM.4/ECC (Cryptographic Key Destruction – ECC (optional))	–	not used by the TOE, no conflict
FCS_COP.1/SHA (cryptographic operation – hashing (optional))	FCS_COP.1/SHA	
FCS_COP.1/AES_PUF (cryptographic operation – PUF based AES)	–	not used by the TOE, no conflict
FCS_COP.1/MAC_PUF (cryptographic operation – PUF based MAC)	–	not used by the TOE, no conflict
FCS_CKM.1/PUF (cryptographic key generation – PUF)	–	not used by the TOE, no conflict
FCS_CKM.4/PUF (cryptographic key destruction – PUF)	–	not used by the TOE, no conflict

HW SFRs	Matches TOE SFR	Remarks
FPT_TST.1 (subset TOE testing)	FPT_TST.1	
FMT_SMF.1 (specification of management functions)	–	not used by the TOE, no conflict
FDP_ACC.1/ACP (subset access control – access control policy)	–	used implicitly, no conflict
FDP_ACF.1/ACP (security attribute based access control – access control policy)	–	used implicitly, no conflict
FMT_MSA.1/ACP (management of security attributes – access control policy)	–	used implicitly, no conflict
FMT_MSA.3/ACP (static attribute initialization – access control policy)	–	used implicitly, no conflict

Table 7.5: Mapping of hardware to TOE SFRs.

7.4.2.3 Assurance Requirements

The level of assurance of the

- TOE is EAL4 augmented with ALC_DVS.2
- Hardware is EAL6 augmented with ALC_FLR.1 and ASE_TSS.2

This shows that the assurance requirements of the TOE matches the assurance requirements of the hardware.

7.4.3 Conclusion

Overall no contradictions between the Security Targets of the TOE and the hardware can be found.

8 Glossary and Acronyms

Active Authentication Security mechanism defined in [ICAO_9303] option by which means the MRTD's chip proves and the Inspection System verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of organization.

Application note / Note Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Audit records Write-only-once non-volatile memory area of the MRTD's 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 (BAC) Security mechanism defined in [ICAO_9303] by which means the MRTD's chip proves and the Inspection System protects their communication by means of Secure Messaging with Basic Access Keys (see there).

Basic Inspection System (BIS) An Inspection System which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived form printed MRZ data for reading the logical MRTD.

Biographical data (biodata) The personalized details of the MRTD holder 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. [ICAO_9303]

Biometric reference data Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.

Counterfeit An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_9303]

Country Signing CA Certificate (CCSCA) Self-signed certificate of the Country Signing CA Public Key (K_{PuCSCA}) issued by CSCA stored in the Inspection System.

Document Basic Access Keys Pair of symmetric (two-key) Triple-DES keys used for Secure Messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the Inspection System [ICAO_9303]. 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 (CDS). [ICAO_9303]

Eavesdropper A threat agent with enhanced basic attack potential reading the communication between the MRTD's chip and the Inspection System to gain the data on the MRTD's chip.

Enrollment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]

Extended Access Control Security mechanism identified in [ICAO_9303] by which means the MRTD's chip (i) verifies the authentication of the Inspection Systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the Inspection System by Secure Messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.

Extended Inspection System (EIS) A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.

Forgery Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO_9303]

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. [ICAO_9303]

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.

IC Identification Data The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.

Impostor A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_9303]

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. [ICAO_9303]

Initialization Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.2, TOE life cycle, phase 2, step 3).

Initialization Data Any data defined by the TOE manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).

Inspection The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO_9303]

Inspection system (IS) A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

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). [ICAO_9303]

Issuing State The Country issuing the MRTD. [ICAO_9303]

Logical Data Structure (LDS) The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the MRTD's chip.

Logical MRTD Data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contactless/contact integrated circuit. It presents contactless or contact based readable data including (but not limited to)

1. personal data of the MRTD holder,
2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
3. the digitized portraits (EF.DG2),
4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,
5. the other data according to LDS (EF.DG5 to EF.DG16) and
6. EF.COM and EF.SOD.

Logical travel document Data stored according to the Logical Data Structure as specified by ICAO in the contactless/contact 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. [ICAO_9303]

Machine readable visa (MRV) A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [ICAO_9303]

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. [ICAO_9303]

Machine-verifiable biometrics feature A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_9303]

MRTD application Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes

- the file structure implementing the LDS [ICAO_9303],
- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and
- the TSF Data including the definition the authentication data but except the authentication data itself.

MRTD Basic Access Control Mutual authentication protocol followed by Secure Messaging between the Inspection System and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.

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

MRTD's Chip A contactless or contact based integrated circuit chip complying with ISO/IEC 14443 [ISO_14443] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO_Session12] 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) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.

Passive authentication (i) Verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.

Personalization The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrollment" (cf. sec. 1.2, TOE life cycle, phase 3, step 6).

Personalization Agent The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.

Personalization Agent Authentication Information TSF data used for authentication proof and verification of the Personalization Agent.

Personalization Agent Key Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD 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, FIA_UAU.5 and FIA_UAU.6.

Physical travel document Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to)

1. biographical data,
2. data of the machine-readable zone,
3. photographic image and
4. other data

Pre-personalization Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf. sec. 1.2, TOE life cycle, phase 2, step 5).

Pre-personalization Data Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.

Pre-personalized MRTD's chip MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.

Primary Inspection System (PIS) An inspection system that contains a terminal for the contactless or contact based communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.

Random Identifier Random identifier used to establish a communication to the TOE in phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability.

Receiving State The Country to which the Traveler is applying for entry. [ICAO_9303]

Reference data Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

Secondary image A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO_9303]

Secure Messaging in Encrypted Mode Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO_7816-4].

Skimming Imitation of the Inspection System to read the logical MRTD or parts of it via the contactless or contact based communication channel of the TOE without knowledge of the printed MRZ data.

Travel document A passport or other official document of identity issued by a State or organization which may be used by the rightful holder for international travel. [ICAO_9303]

Traveler 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 [CC_Part1]).

Unpersonalized MRTD The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.

User data Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC_Part1]).

Verification The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO_9303]

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.

Acronyms

Acronym	Term
BIS	Basic Inspection System
CC	Common Criteria
EF	Elementary File
GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number
MF	Master File
n.a.	Not applicable
OSP	Organizational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE security functions

9 Bibliography

[AGD] User Guidance – MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), MaskTech International GmbH, Version 1.2, 2023-08-24.

[BSI_AIS31] Anwendungshinweise und Interpretationen zum Schema – Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, AIS 31, Version 3, 2013-05-15.

[BSI_TR-03110] TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents, BSI, Version 2.20, 2015.

[BSI_TR-03110-1] TR-03110-1, Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015-02-26.

[BSI_TR-03110-3] TR-03110-3, Technical Guideline 03110: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 – Common Specifications, BSI, Version 2.21, 2016-12-21.

[BSI_TR-03116-2] TR-03116-2, Technische Richtlinie – Kryptographische Verfahren für Projekte der Bundesregierung - Teil 2 – Hoheitliche und eID-Dokumente, BSI, Stand 2022, 2021-11-30.

[CC_Part1] CCMB-2017-04-001, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, 2017-04.

[CC_Part2] CCMB-2017-04-002, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, 2017-04.

[CC_Part3] CCMB-2017-04-003, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, 2017-04.

[CC_PartEM] CCMB-2017-04-004, Version 3.1, Revision 5, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC_PP-0055] BSI-CC-PP-0055-2009, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Basic Access Control, BSI, Version 1.10, 2009-03-25.

[CC_PP-0056-V2] BSI-CC-PP-0056-V2-2012-MA-02, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Extended Access Control with PACE, BSI, Version 1.3.2, 2012-12-05.

[CC_PP-0084] BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages, EUROSMART, Version 1.0, 2014-01-13.

[FIPS_140-3] FIPS PUB 140-3, Security Requirements for Cryprographic Modules, National Institute of Standards and Technology, 2019-03.

[FIPS_180-4] FIPS PUB 180-4, Secure Hash Standard (SHS), National Institute of Standards and Technology, 2015-08.

[FIPS_197] FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), National Institute of Standards and Technology, 2001-11.

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, ICAO, 2021.

[ICAO_Session12] Facilitation (FAL) Division, twelfth session, Cairo, ICAO, 10-2004.

[ISO_10116] ISO/IEC 10116-2017, Information technology – Security techniques - Modes of operation for an n-bit block cipher, ISO/IEC, 2017-07.

[ISO_14443] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Multipart Standard, ISO/IEC, 2016-2018.

[ISO_18013-3] ISO/IEC 18013-3:2017, Information technology – Personal identification – ISO-compliant driving license – Part 3: Access control, authentication and integrity validation, ISO/IEC, 2017-04.

[ISO_7816] ISO/IEC 7816, Identification cards – Integrated circuit cards – Multipart Standard, ISO/IEC, 2008.

[ISO_7816-4] ISO/IEC 7816-4:2020, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, ISO/IEC, 2020-05.

[ISO_9797-1] ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO/IEC, 2011.

[KiSch-RNG] Version 2.0, A proposal for: Functionality classes for random number generators, W. Killmann and W. Schindler, 2011-09-18.

[MT_Manual] MTCOS Pro 2.6 on P71D352 (N7121) – Manual, MaskTech GmbH, 2023-08-07. Version 1.0.

[NIST_SP800-38B] NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology, 2016-10.

[NIST_SP800-67] NIST SP 800-67 Rev. 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST, 2017-11.

[NIST_SP800-90A] NIST SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, 2015-06.

[NXP_P71_ST] NXP Semiconductors, Security Target Lite 'NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library', BSI-DSZ-CC-1136-V3-2022, Rev. 2.6, 2022-06-13.

[SC_HID] BSI-DSZ-CC-S-0232-2023, HID Global GmbH, Site Security Target Lite of HID Global Ireland Teoranta in Galway, Ireland, Rev. D, 2023-05-08.

[SC_HID_MY] BSI-DSZ-CC-S-0233-2023, HID Global GmbH, Site Security Target Lite for HID Global Malaysia, PRO-01286 Rev D2, 2020-04-17.

[SC_Linxens] BSI-DSZ-CC-S-0207-2021, Linxens (Thailand) Co Ltd., Site Security Target LITE for Linxens Thailand, Version 2.4, 2021-11-24.

[SC_Linxens_DE] BSI-DSZ-CC-S-0214-2022, Linxens Germany GmbH, Site Security Target Lite for Linxens Germany GmbH, Version 1.0, 2021-01-26.

10 Revision History

Version	Date	Author	Changes
1.0	2023-07-28	Christian Wille	Public version based on v0.5 of the confidential ST of BSI-DSZ-CC-1148-V3-2023
1.1	2023-08-08	Christian Wille	Update bibliography
1.2	2023-08-24	Gudrun Schürer	Amended life cycle, update bibliography

11 Contact

MaskTech GmbH – **Headquarters**

Nordostpark 45	Phone	+49 911 955149 0
D-90411 Nuernberg	Fax	+49 911 955149 7
Germany	Email	info@masktech.de

MaskTech GmbH – **Support**

Bahnhofstr. 13	Phone	+49 911 955149 0
D-87435 Kempten	Fax	+49 831 5121077 5
Germany	Email	support@masktech.de

MaskTech GmbH – **Sales**

Lauenburger Str. 15	Phone	+49 4151 8990858
D-21493 Schwarzenbek	Fax	+49 4151 8995462
Germany	Email	stimm@masktech.de

A Overview Cryptographic Algorithms

The following cryptographic algorithms are used by the TOE to enforce its security policy:

	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments ST-Reference
1	Authenticated Key Agreement / Authentication	BAC, Symmetric Authentication, based on 3DES in CBC mode	[BSI_TR-03110-1] [ICAO_9303] [NIST_SP800-67] (3DES) [ISO_10116] sec. 7 (CBC) also cf. lines 3, 4	112	[BSI_TR-03110-1] [ICAO_9303]	FIA_AFL.1 FIA_UAU.4 FIA_UAU.6
2	Authenticated Key Agreement / Authentication	BAC, Symmetric Authentication, based on AES in CBC mode, conforming to BAP standard (basic access protection, driving license).	[FIPS_197] (AES) [ISO_10116] sec. 7 (CBC) [ISO_18013-3] Annex B [ICAO_9303] also cf. lines 3, 4	128	[ISO_18013-3] Annex B [ICAO_9303]	FCS_COP.1/AUTH
3	Key Derivation	BAC Key Derivation, SHA-1	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303] [FIPS_180-4] sec. 6	-	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303]	FCS_COP.1/SHA
4	Key Derivation	Document Basic Access Key Derivation Algorithm	[BSI_TR-03110-1] [ICAO_9303]	-	[BSI_TR-03110-1] [ICAO_9303]	FCS_CKM.1
5	Confidentiality	3DES in CBC mode for Secure Messaging	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303] [NIST_SP800-67] (3DES) [ISO_10116] sec. 7 (CBC)	112	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303]	FCS_COP.1/ENC FDP_UCT.1
6	Integrity	3DES in Retail MAC mode for Secure Messaging	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303] [NIST_SP800-67] (3DES) [ISO_9797-1] sec. 7.4, MAC Algorithm 3 (Retail-MAC)	112	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303]	FCS_COP.1/MAC FDP_UIT.1
7	Trusted Channel	ICAO BAC Secure Messaging in ENC/MAC mode	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303] sec. 4 also cf. lines 3, 5, 6	-	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303]	FCS_COP.1/SHA FCS_COP.1.1/ENC FCS_COP.1/MAC FDP_UIT.1 FDP_UCT.1
8	Cryptographic Primitive	PTG.3 Random number generator (PTG.2 and cryptographic post-processing)	[BSI_AIS31] [NIST_SP800-90A] sec. 10.2, 10.3.2	-	[BSI_TR-03116-2]	FCS_RND.1
9	Cryptographic Primitive	SHA-1	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303] [FIPS_180-4] sec. 6	-	[BSI_TR-03110-1] [BSI_TR-03110-3] [ICAO_9303]	FCS_COP.1/SHA

Table A.1: Overview Cryptographic Algorithms