G+D Mobile Security

STARCOS 3.7 ID eAT BAC C1, STARCOS 3.7 ID ePass BAC C1

Security Target Lite

Version **1.5**

Author : Giesecke+Devrient Mobile Security GmbH

Status : **Final**

Rating : **Public**

File : GDM_STA37_ID_BAC_C1_ASE

Edition : 12.08.2020

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstraße 159
D-81677 München

Contents

History of this document

1.5	12.08.2020	Uta/stut	Final Version

1 ST Introduction

1.1 ST Reference

Title: Security Target Lite STARCOS 3.7 ID eAT BAC C1, STARCOS 3.7 ID ePass BAC C1

Reference: GDM_STA37_ID_BAC_C1_ASE_Lite

Version 1.5 /Status 12.08.2020

Origin: Giesecke+Devrient Mobile Security GmbH

Author: stut

CC Version: 3.1 (Revision 5)

Assurance Level: EAL4-augmented with assurance component ALC_DVS.2.

TOE: STARCOS 3.7 ID eAT BAC C1, STARCOS 3.7 ID ePass BAC C1

TOE documentation:

- Guidance Documentation STARCOS 3.7 ID – Main Document
- Guidance Documentation for the Initialisation Phase STARCOS 3.7 ID C1
- Guidance Documentation for the Personalisation Phase STARCOS 3.7 ID C1
- Guidance Documentation for the Usage Phase STARCOS 3.7 ID BAC

HW-Part of TOE: IFX_CCI_000005h, H13 (Certificate: BSI-DSZ-CC-1110-V3-2020) [25]. This TOE was evaluated against Common Criteria Version 3.1.

1.2 TOE Overview

This security target defines the security objectives and requirements for the contactless 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’ [5].

STARCOS 3.7 ID eAT BAC C1, STARCOS 3.7 ID ePass BAC C1 is the name of the related Target of Evaluation (TOE). The related products are the STARCOS 3.7 ID eAT BAC C1, STARCOS 3.7 ID ePass BAC C1 cards.

The TOE consists of software in combination with the underlying hardware ('Composite Evaluation'). The TOE software is the STARCOS 3.7 ID operating system and the ePass application of the product. The TOE hardware is the secure IFX_CCI_000005h, H13 certified according to CC EAL6.

The assurance level for the TOE is CC EAL4 augmented.

1.2.1 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides the conformance claims for the Security Target.

Section 3 provides a discussion of the security problems for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the operational environment and the security objective rational to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat.

Section 5 contains the extended component definitions.

Section 6 contains the security functional requirements and assurance requirements derived from the Common Criteria [1], Part 2 [2] and Part 3 [3], which must be satisfied and the security functional requirements rational. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Section 7 contains the TOE Summary Specification.

Section 8 provides information on used acronyms and glossary and the used references.

1.2.2 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to the ‘ICAO Doc 9303’ [5].

The TOE comprises of at least

- 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 of the product and

- the associated guidance documentation.

1.2.3 TOE usage and security features for operational use

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

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

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

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

(3) the printed portrait.

(b) the logical MRTD as data of the MRTD holder stored according to the Logical Data Structure [5] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder

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

(2) the digitized portraits (EF.DG2),

(3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]

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

(5) the Document security object.

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

[1] These additional biometric reference data are optional.

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) [5]. 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 [5]. 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 addresses 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 [5], normative appendix 5.

1.2.4 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [18], the TOE life-cycle is additionally subdivided into 7 steps.)

Phase 1 "Development"

(Step1) 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.

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

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

programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase 2 “Manufacturing”

(Step3) In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

(Step4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book

(Step5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD’s chips with pre-personalization Data.

Application Note 1: Creation of the application implies:

- For the file based operating system of the TOE: the creation of MF and ICAO.DF

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.

Phase 3 “Personalization of the MRTD”

(Step6) The personalization of the MRTD includes (i) the survey of the MRTD holder’s biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing 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 [5] 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.

Application note 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [1] §92) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Basic Authentication Control Key.

Application note 3: This security target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [5]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

Phase 4 “Operational Use”

(Step7) 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.

Application note 4: The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.

Application note 5: The intention of the PP is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the “Operational Use” (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

1.2.5 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.

1.2.6 Configurations of the TOE

The TOE can be used in two different configurations:

1. STARCOS 3.7 ID eAT BAC C1.
2. STARCOS 3.7 ID ePass BAC C1.

In life cycle phase 2 and 3 the specific TOE configuration can be identified by the TOE response to a specific APDU specified in the TOE documentation (see chapter 1.1).

2 Conformance Claims

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 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, July 2017 [3]

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, [4]

has to be taken into account.

2.2 PP Claim

This ST claims strict conformance to the Common Criteria Protection Profile – Machine Readable Travel Document with ”ICAO Application”, Basic Access Control [19].

2.3 Package Claim

This ST is conformant to the assurance package EAL4 augmented with ALC_DVS.2 defined in the CC, part 3 [3].

2.4 Conformance Rationale

Since this ST is not claiming conformance to any other protection profile, no rationale is necessary here.

3 Security Problem Definition

3.1 Introduction

3.1.1 Assets

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

Logical MRTD sensitive User 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 [5]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons as the 'ICAO Doc 9303' [5] the TOE described in this protection profile 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.

The TOE prevents read access to sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG4)[2].

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.

[2] Cf. [1] for details how to access these User data under EAC protection.

3.1.2 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.

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 [5].

Terminal
A terminal is any technical system communicating with the TOE through the contactless 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 communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. Optionally, the BIS may support Active Authentication. 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.

Application note 6: This security target does not distinguish between the BIS, GIS and EIS because the Active Authentication and the Extended Access Control is outside the scope.

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 manipulate the logical MRTD without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine travel document, or (iv) to trace a travel document.

Application note 7: 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, (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip), and (v) the Active Authentication Public Key (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 CA 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 [5]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

Application note 8: According to [5] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

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’ [5], 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.

Application note 9: When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

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 **Eeavesdropping 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 Organisational 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 [1], sec. 3.2).

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)[3] 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 [5].

[3] Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by this Security Target.

Application note 10: The organizational security policy P.Personal_Data is drawn from the ICAO ‘ICAO Doc 9303’ [5]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

4 Security Objectives

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

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 [5] 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.

Application note 12: 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.

Application note 12: 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.

The security objective OT.Data_Conf 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' [6] 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 protection profile. 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.

Application note 13: 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 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the MRTD". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless 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 of 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.

Application note 14: This 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.

Application note 15: 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 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 acknowledgement,
  - 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 Signer 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 [5].

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’ [5] 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 or Organization 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 CA 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 [5].

OE.Passive_Auth_Verif Verification by Passive Authentication

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

OE.Prot_Logical_MRTD Protection of data from 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

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	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 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 enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD”, and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD”. Note the manufacturer equips the TOE with the Personalization Agent 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 to **OE.Passive_Auth_Verif** “Verification by Passive Authentication”.

The threat **T.Abuse-Func** “Abuse of Functionality” addresses attacks using the MRTD’s chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality”. 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 enrolment, 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” will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

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

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [16] other components are defined in the protection profile [19].

5.1 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE a family (FAU_SAS) of the class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

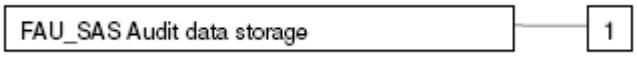
The family ‘Audit data storage (FAU_SAS)’ is specified as follows:

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components

Dependencies: No dependencies

FAU_SAS.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a family (FCS_RND) of the class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

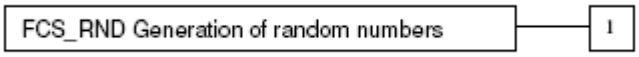
The family ‘Generation of random numbers (FCS_RND)’ is specified as follows:

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers intended to be used for cryptographic purposes.

Component levelling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3 Definition of the Family FMT_LIM

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

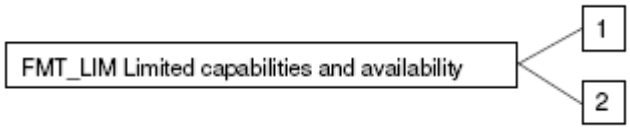
The family ‘Limited capabilities and availability (FMT_LIM)’ is specified as follows:

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

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 [assignment: *limited capability and availability policy*].

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 availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced [assignment: *limited capability and availability policy*].

Application Note 16: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both the requirements shall enforce the related policy.

5.4 Definition of the Family FPT_EMSEC

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

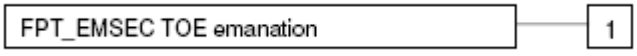
The family 'TOE Emanation (FPT_EMSEC)' is specified as follows:

FPT_EMSEC TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management:	FPT_EMSEC.1 There are no management activities foreseen.
Audit:	FPT_EMSEC.1 There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies

FPT_EMSEC.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: specified limits] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 Security Requirements

The CC allows several operations to be performed on security requirements (on the component level); *refinement*, *selection*, *assignment* and *iteration* are defined in sec. 8.1 of Part 1 [1] of the CC. 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. Refinements of security requirements are denoted in such a way that added words are in **bold text**.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections filled in by the ST author are denoted as double underlined text and a foot note where the selection choices from the PP are listed.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments filled in by the ST author are denoted as double underlined text. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicised like *this*.

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", "Basic Inspection System" 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 section 7 or in the following table. The operations "write", "read", "modify", and "disable read access" are used in accordance with the general linguistic usage. The operations "transmit", "receive", and "authenticate" and "re-authenticate" are originally taken from [2].

Definition of security attributes:

security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation 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 sub-section 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 extended).

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application note 17: 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.1.1/INI_DIS).

6.1.2 Class FCS Cryptographic Support

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

FCS_CKM.1 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

[4] [assignment: *authorised users*]

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

Document Basic Access Key Derivation Algorithm[6] and specified cryptographic key sizes 112 bits[7] that meet the following: [5], normative appendix 5[8].

Application Note 18: 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 [5], 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 [5], 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).

FCS_CKM.4 Cryptographic key destruction - 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.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key value with zero values[9] that meets the following: none[10].

Application Note 19: 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). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA Cryptographic operation – Hash for key derivation

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]

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

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

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

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

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

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SHA The TSF shall perform hashing[11] in accordance with a specified cryptographic algorithm *SHA-1*[12,13] and cryptographic key sizes none[14] that meet the following: *FIPS 180-4*[15,16].

Application Note 20: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive to derive the Basic Access Control Authentication Mechanism (see also FAU_UAU.4) according to [5].

FCS_COP.1/ENC Cryptographic operation – Symmetric 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[17] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[18] and cryptographic key sizes 112 bits[19] that meet the following: FIPS 46-3 [10] and [5]; normative appendix 5, A5.3[20].

Application Note 21: 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

[11] [assignment: *list of cryptographic operations*]
[12] [selection: *SHA-1 or other approved algorithms*]
[13] [assignment: *cryptographic algorithm*]
[14] [assignment: *cryptographic key sizes*]
[15] [assignment: *list of standards*]
[16] [selection: *FIPS 180-2 or other approved standards*]
[17] [assignment: *list of cryptographic operations*]
[18] [assignment: *cryptographic algorithm*]
[19] [assignment: *cryptographic key sizes*]
[20] [assignment: *list of standards*]

FCS_COP.1.1/AUTH The TSF shall perform symmetric authentication – encryption and decryption[21] in accordance with a specified cryptographic algorithm *AES*[22,23] and cryptographic key sizes *128 bits*[24,25] that meet the following: *FIPS 197* [9][26,27].

Application Note 22: 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).

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[28] in accordance with a specified cryptographic algorithm Retail-MAC[29] and cryptographic key sizes 112 bits[30] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[31].

Application Note 26: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 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).

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

[21] [assignment: *list of cryptographic operations*]
[22] [selection: *Triple-DES, AES*]
[23] [assignment: *cryptographic algorithm*]
[24] [selection: *112, 128, 168, 192, 256*]
[25] [assignment: *cryptographic key sizes*]
[26] [selection: *FIPS 46-3 [10], FIPS 197 [9]*]
[27] [assignment: *list of standards*]
[28] [assignment: *list of cryptographic operations*]
[29] [assignment: *cryptographic algorithm*]
[30] [assignment: *cryptographic key sizes*]
[31] [assignment: *list of standards*]

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet

the requirements of RNG class DRG.4:

(DRG.4.1) The internal state of the RNG uses a PTRNG of class PTG.2 as a random source.

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy, even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy for every call.

(DRG.4.5)The internal state of the RNG is seeded by a PTRNG of class PTG.2.

(DRG.4.6) The RNG generates output for which two strings of bit length 128 are mutually different with probability 1 - 2^128.

(DRG.4.7) Statistical test suites cannot practically distinguish the random number from output sequences of an ideal RNG. The random numbers pass test procedure A as defined in AIS20[22]/AIS31[23].[32].

Application Note 24: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

6.1.3 Class FIA Identification and Authentication

Application Note 25: The Table 2 provides an overview of the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to **[5], normative appendix 5, and [21]**
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	AES with 128 bit keys (cf. FCS_COP.1/AUTH)

Table 2 Overview on authentication SFRs

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

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

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

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”[33]

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.

Application Note 26: The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. 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.

Application Note 27: 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. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

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”,

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

2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”[34]

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.

Application note 28: 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).

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 *AES*[35,36].

Application Note 29: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalization Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

Application note 30: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [5]. 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 fulfil 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).

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

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

[36] [selection: *Triple-DES, AES or other approved algorithms*]

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 *AES*[37,38]

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 mechanism(s) *Symmetric Authentication Mechanism with Personalization Agent Key*[39].
2. The TOE accepts the authentication attempt as Basic Inspection System only by means of Basic Access Control Authentication Mechanism with the Document Basic Access Keys[40].

Application Note 31: In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [20] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or other symmetric authentication mechanism based on the two-key Triple-DES. The Personalization Agent is authenticated by using the AES-based Symmetric Authentication Mechanism with the Personalization Agent Key, cf. [20] FIA_UAU.5.2.

Application note 32: The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. 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).

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

Hierarchical to: No other components.

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

[38] [selection: *Triple-DES, AES*]

[39] [selection: *the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]*]

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

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[41].

Application Note 33: The Basic Access Control Mechanism specified in [5] 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.

Application note 34: Note that in case the TOE should also fulfil [20] 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.1)” as specified below (Common Criteria Part 2).

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 an administrator configurable positive integer within range of acceptable values 1 to 10 consecutive[42] unsuccessful authentication attempts occur related to the BAC mechanism[43].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed[44], the TSF shall wait for an administrator configurable time between the receiving the terminal challenge e_{IFD} and sending the TSF response e_{ICC} during the BAC authentication attempts[45].

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

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

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

[44] [assignment: *met or surpassed*]

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

Application note 35: These assignments are assigned to ensure especially the strength of authentication function as terminal part of the Basic Access Control Authentication Protocol to resist enhanced basic attack potential.

The terminal challenge e_{IFD} and the TSF response e_{ICC} are described in [21], 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.

6.1.4 Class FDP User Data Protection

Subset access control (FDP_ACC.1)

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

FDP_ACC.1 Subset access control – Basic 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[46] 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[47].

Security attribute based access control (FDP_ACF.1)

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

FDP_ACF.1 Security attribute based access control – Basic 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[48] to objects based on the following:

1. Subjects:
   a. Personalization Agent,

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

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

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

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[49]

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[50]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[51].

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

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.[52]

Application Note 36: The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this protection profile (cf. [20] for details).

Inter-TSF-Transfer

Application Note 37: 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

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

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

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

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

successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

FDP_UCT.1 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[53] to be able to transmit and receive[54] user data in a manner protected from unauthorized disclosure.

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[55] to be able to transmit and receive[56] user data in a manner protected from modification, deletion, insertion and replay[57] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[58] has occurred.

6.1.5 Class FMT Security Management

Application note 38: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements on 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).

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

[53] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[54] [selection: *transmit, receive*]
[55] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[56] [selection: *transmit, receive*]
[57] [selection: *modification, deletion, insertion, replay*]
[58] [selection: *modification, deletion, insertion, replay*]

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Initialization,
2. Pre-Personalization,
3. Personalization[59]

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

FMT_SMR.1 Security roles

Hierarchical to: No other components.

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.[60]

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

Application note 39: 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 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 do not allow

1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[61]

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

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

[61] [assignment: *limited capability and availability policy*]

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with ‘Limited capabilities (FMT_LIM.1)’ the following policy is enforced:
Deploying test features after TOE delivery do not allow

1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[62]

Application note 40: 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.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application note 41: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

FMT_MTD.1/INI_ENA Management of TSF data – Writing 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[63] the Initialization Data and Pre-personalization Data[64] to the Manufacturer[65].

[62] [assignment: *limited capability and availability policy*]

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

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

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

Application note 42: The Pre-personalization Data includes but is 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 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[66] the Initialization Data[67] to the Personalization Agent[68].

Application note 43: 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 Pre-personalization Data by 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 shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

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

Hierarchical to: No other components.

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[69] the Document Basic Access Keys[70] to the Personalization Agent[71].

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

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

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

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

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

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

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

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[72] the Document Basic Access Keys and Personalization Agent Keys[73] to none[74].

Application Note 44: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

6.1.6 Class FPT Protection of the 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 SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

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

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1 The TOE shall not emit information about IC power consumption and command execution time[75] in excess of non useful information[76] enabling access to Personalization Agent Key(s)[77] and logical MRTD data[78].

FPT_EMSEC.1.2 The TSF shall ensure any unauthorized users[79] are unable to use the following interface smart card circuit contacts[80] to gain access to Personalization Agent Key(s)[81] and logical MRTD data[82].

Application note 51: 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

[72] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[73] [assignment: *list of TSF data*]
[74] [assignment: *the authorised identified roles*]
[75] [assignment: *types of emissions*]
[76] [assignment: *specified limits*]
[77] [assignment: *type of users*]
[78] [assignment: *list of types of user data*]
[79] [assignment: *type of users*]
[80] [assignment: *type of connection*]
[81] [assignment: *type of users*]
[82] [assignment: *list of types of user data*]

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).

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[83]

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the condition Reset of the TOE*[84,85] to demonstrate the correct operation of the TSF[86].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[87].

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

[84] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*]

[85] [assignment: *conditions under which self test should occur*]

[86] [selection: [assignment: *parts of TSF*], *the TSF*]

[87] [selection: [assignment: *parts of TSF*], *TSF data*]

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

Application note 46: The MRTD's chip uses state of the art smart card technology and runs some self tests at the request of the authorized user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 is executed during initial start-up by the "authorized user" Manufacturer in the Phase 2 "Manufacturing". Other self tests are executed automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 "Operational Use", e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks.

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[88] to the TSF[89] by responding automatically such that the SFRs are always enforced.

Application note 47: 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.

Application note 48: The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

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 4 (EAL4)

and augmented by the following components:

ALC_DVS.2.

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

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

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-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					
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 3 Coverage of Security Objectives for the TOE by SFR

The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD. 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 SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated (for reasons of interoperability with [20]) by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

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.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The 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 SRF FIA_UAU.4 and FIA_UAU.5 using 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 requires 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.

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 (cf. the SFR FDP_UCT.1 and FDP_UIT.1 for key generation), 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.

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 (cf. Application note 30). 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 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.

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

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMSEC.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

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

The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, 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 analysed, and non-dissolved dependencies are appropriately explained.

The Table 4 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 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/ENC, and FCS_COP.1/MAC, 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 Cryptographic 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 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	justification 1 for non-satisfied dependencies 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 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1 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 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	justification 2 for non-satisfied dependencies 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 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1 Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
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, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1

FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 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 4 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.1.1/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 nor to import a key during the addressed TOE lifecycle 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.

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. There is no need for 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 positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The selection of 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 MRTD's material.

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements

Dependencies ALC_DVS.2:

no dependencies.

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 form a mutually supportive and internally consistent whole.

The analysis of the TOE 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 analysed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) 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.

6.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the Infineon microcontroller derivative IFX_CCI_000005h, H13 [25]. This statement is compliant to the requirements of [4a].

6.4.1 Classification of Platform TSFs

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

TOE Security Functionality	Relevant	Not relevant
SF_DPM: Device Phase Management	x	
SF_PS: Protection against Snooping	x	
SF_PMA: Protection against Modifying Attacks	x	
SF_PLA: Protection against Logical Attacks	x	
SF_CS: Cryptographic Support	x	

Table 5 Classification of Platform-TSFs

All listed TSFs of the Platform-ST are relevant for the Composite-ST.

6.4.2 Matching statement

The TOE relies on fulfillment of the following implicit assumptions on the IC:

- Certified Infineon microcontroller derivative IFX_CCI_000005h, H13; the optional ACL , SCL, NRG and CIPURSE™libraries are not used by the composite TOE.
- Hybrid Random Number Generation with PTG.2 classification according to [23].
- Cryptographic support based symmetric algorithm and 112 bits (2-key Triple-DES) and 128 bits (AES) symmetric cryptographic key length.
- the hardware support library (HSL) in the versions 03.11.8339

The rationale of the Platform-ST has been used to identify the relevant SFRs, TOE objectives, threats and OSPs. All SFRs, objectives for the TOEs, but also all objectives for the TOE-environment, all threats and OSPs of the Platform-ST have been used for the following analysis.

6.4.2.1 TOE Security Environment

6.4.2.1.1 Threats and OSPs

(see chapters 3.3 Threats and 3.4 Organisational Security Policies)

The OSPs of the Composite-ST are not applicable to the IC and are therefore not mapped to the OSPs of the Platform-ST.

The augmented organizational security policy P.Add-Functions of the Platform-ST deals with additional specific security functionality of the cryptographic libraries and could therefore be mapped to OT.Prot_Inf_Leak and OT.Prot_Phys-Tamper of the Composite-ST.

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

- T.Phys-Tamper
- T.Malfunction
- T.Abuse-Func
- T.Information_Leakage
- T.Forgery

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

- T.Leak-Inherent
- T.Phys_Probing
- T.Malfunction
- T.Phys_Manipulation
- T.Leak-Forced
- T.Abuse-Func
- T.RND
- T.Mem-Access

The following table shows the mapping of the threats.

Platform-ST		T.Leak-Inherent	T.Phys_Probing	T.Phys_Manipulation	T.Malfunction	T.Leak-Forced	T.Abuse-Func	T.RND	T.Mem-Access
Composite-ST	T.Phys_Tamper	x	x	x	x	x		x	
	T.Malfunction				x				
	T.Abuse-Func						x		x
	T.Information_Leakage	x	x	x	x	x	x		
	T.Forgery			x	x				

Table 6 Mapping of threats

T.Phys-Tamper matches to T.Leak-Inherent, T.Phys_Probing, T.Phys-Manipulation, T.Malfunction, T.Leak-Forced and T.RND as physical TOE

interfaces like emanations, probing, environmental stress and tampering are used to exploit vulnerabilities.

T.Abuse-Func matches to T.Mem-Access as security violations either accidentally or deliberately could access restricted data (which may include code) or privilege levels.

T.Information_Leakage matches to T.Leak-Inherent, T.Phys_Probing, T.Phys-Manipulation, T.Malfunction, T.Leak-Forced and T.Abuse-Func as physical TOE interfaces like emanations, probing, environmental stress and tampering could be used to exploit exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data.

T.Forgery matches to T.Phys_Manipulation and T.Malfunction because if an attacker fraudulently alters the User Data or/and TSF-data stored on the MRTD or/and exchanged between the TOE and the inspection system then the listed threats of the Platform-ST could be relevant.

6.4.2.1.2 Assumptions

The assumptions from this ST (see chapter 3.2 Assumptions) make no assumptions on the platform.

The assumptions from the Platform-ST [25] are as follows:

Assumption	Classification of assumptions	Mapping to Security Objectives of this Composite-ST
A.Process-Sec-IC	not relevant	n/a
A.Resp-Appl	relevant	OT.Data_Int, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper
A.Key-Function	relevant	OT.Prot_Inf_Leak

Table 7 Mapping of assumptions

There is no conflict between security environments of this Composite-ST and the Platform-ST [25].

6.4.2.2 Security objectives

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

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

The following platform objectives could be mapped to composite objectives:

- O.RND
- O.Phys-Probing

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

These Platform-ST objectives can be mapped to the Composite-ST objectives as shown in the following table.

Platform-ST		O.RND	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Abuse-Func	O.Leak-Forced	O.Leak-Inherent	O.Identification
Composite-ST	OT.Prot_Abuse-Func					x			
	OT.Prot_Inf_Leak						x	x	
	OT.Prot_Phys-Tamper	x	x	x	x				
	OT.Identification								x
	OT.Prot_Malfunction			x					

Table 8 Mapping of objectives

O.Cap_Avail_Loader, O.Authentication, O.Ctrl_Auth_Loader and O.Prot_TSF_Confidentiality : The Flash Loader is used to load the encrypted initialization image into the flash memory of the chips during Initialization (after Phase 4) and Composite Product Integration (in Phase 5). The usage of the Loader is addressed in TOE documentation [28] and by OE.Lim_Block_Loader. In User configuration (Phases 5-6), the Loader capability is not accessible by the Security IC Embedded Software and the Secure Flash Loader is not available.

OT.Prot_Phy-Tamper requires require detection of and resistance to physical tampering, which matches to O.RND as well as O.Phys-Probing, O.Phys-Manipulation and O.Malfunction.

The following Platform-ST objectives are not relevant for or cannot be mapped to objectives of the Composite-ST:

- O.Add-Functions cannot be mapped
- O.MEM_ACCESS is not relevant because the Composite-TOE does not use area based memory access control.

All Security Objectives for the Environment (see chapter 4.2 and [19]) are not linked to the platform and are therefore not applicable to this mapping. These objectives are:

- 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

There is no conflict between security objectives of this Composite-ST and the Platform-ST [25].

6.4.2.3 Security requirements

6.4.2.3.1 Security Functional Requirements

This Composite-ST has the following platform-related SFRs:

- FCS_COP.1.1/ENC
- FCS_COP.1.1/AUTH
- FCS_COP.1.1/MAC
- FCS_RND.1
- FPT_PHP.3
- FPT_EMSEC.1
- FPT_FLS.1
- FPT_TST.1
- FMT_LIM.1
- FMT_LIM.2
- FAU_SAS.1

The following Platform-SFRs could be mapped to Composite-SFRs:

- FCS_RNG.1
- FCS_COP.1/TDES (by SCP)
- FCS_COP.1/AES (by SCP)
- FRU_FLT.2
- FPT_PHP.3
- FPT_FLS.1
- FPT_TST.2
- FMT_LIM.1/Loader
- FMT_LIM.2/Loader

- FAU_SAS.1

They will be mapped as seen in the following table.

Platform-ST		FCS_RNG.1	FCS_COP.1/TDES (by SCP)	FCS_COP.1/AES (by SCP)	FRU_FLT.2	FPT_FLS.1	FPT_PHP.3	FMT_LIM.1/Loader	FMT_LIM.2/Loader	FAU_SAS.1	FPT_TST.2
Composite-ST	FCS_COP.1.1/ENC		x								
	FCS_COP.1.1/AUTH			x							
	FCS_COP.1.1/MAC		x								
	FCS_RND.1	x									
	FPT_PHP.3				x	x	x				
	FPT_EMSEC.1						x				
	FPT_FLS.1					x					
	FPT_TST.1										x
	FMT_LIM.1							x			
	FMT_LIM.2								x		
	FAU_SAS.1									x	

Table 9 Mapping of SFRs

FCS_COP.1.1/ENC and FCS_COP.1.1/MAC of the Composite-ST match FCS_COP.1/TDES (by SCP) of the Platform-ST when the DES coprocessor is used by the TOE.

FCS_COP.1.1/AUTH of the Composite-ST matches FCS_COP.1/AES (by SCP) of the Platform ST when the AES coprocessor is used by the TOE.

FCS_RND.1 of the Composite-ST matches to the equivalent SFR of the Platform-ST FCS_RNG.1.

FPT_PHP.3 of the Composite-ST matches the robustness requirements of FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the Platform-ST.

FPT_EMSEC.1 of the Composite-ST matches the emission requirement FPT_TST.2 of the Platform-ST.

FCS_FLS.1 of the Composite-ST matches to the equivalent SFR of the Platform-ST FPT_FLS.1.

FPT_TST.1 of the Composite-ST matches to FPT_TST.2 of the Platform-ST.

FMT_LIM.1 and FMT_LIM.2 of the Composite-ST match to the equivalent SFR of the Platform-ST (FMT_LIM.1/Loader and FMT_LIM.2/Loader).

FAU_SAS.1 of the Composite-ST matches to the equivalent SFR of the Platform-ST.

The following Platform-SFRs are not mapped to Composite-SFRs:

- FDP_ACC.1, because the composite TOE is always in system mode and therefore no MMU is necessary and because the composite TOE does not use the platform TOE special function registers.
- FDP_ACF.1, because the composite TOE does not use the platform TOE special function registers and the MMU.
- FMT_MSA.1, because the composite TOE is always in system mode and therefore no MMU and special function registers is necessary.
- FMT_MSA.3, because the composite TOE is always in system mode and therefore no MMU is necessary.
- FMT_SMF.1, because the TOE does not change the CPU mode.
- FDP_ITT.1, because it deals with the internal data processing policy of the platform TOE that does not by itself impact the composite TOE.
- FPT_ITT.1, because it deals with the basic internal data protection of the platform TOE that does not by itself impact the composite TOE.
- FDP_IFC.1, because it deals with the data processing policy of the platform TOE that does not by itself impact the composite TOE.
- FDP_SDI.1 and FDP_SDI.2 are not applicable to the composite TOE. Protection against malfunctions is covered by the SFRs FPT_TST.1 and FPT_FLS.1 of the composite TOE.
- FMT_LIM.1 and FMT_LIM.2 as internal test features of the IFX platform are not accessible by the Composite TOE.
- FDP_UCT.1, FDP_UIT.1, FIA_API.1, FTP_ITC.1, FDP_ACC.1/Loader and FDP_ACF.1/Loader because the Flash Loader is used to load the encrypted initialization image into the flash memory of the chips during Initialization (after Step 4) and Composite Product Integration (in Step 5). The usage of the Loader is addressed in [28]. In Operational Use (Phase 4), the Loader capability is not accessible by the Security IC Embedded Software and the Secure Flash Loader is not available.

6.4.2.3.2 Assurance requirements

The Composite-ST requires EAL 4 according to Common Criteria V3.1R5 augmented by ALC_DVS.2.

The Platform-ST requires EAL 6 according to Common Criteria V3.1 R5 augmented by: ALC_FLR.1.

As EAL 6 covers all assurance requirements of EAL 4 all non-augmented parts of the Composite-ST will match to the Platform-ST assurance requirements.

6.4.3 Overall no contradictions found

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

7 TOE summary specification

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

7.1 TOE Security Functions

7.1.1 SF_AccessControl

The TOE provides access control mechanisms that allow to maintain different users and to associate users with roles (Manufacturer, Personalization Agent, Basic Inspection System).

The TOE restricts the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer. Manufacturer is the only role with the capability to store the IC Identification Data in the audit records. Users of role Manufacturer are assumed default users by the TOE during the Phase 2.

The TOE enforces access control on terminals by requiring authentication prior to gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.

Personalization Agent is the only role with the ability:

- to disable read access for users to the Initialization Data,
- to write the Document Basic Access Keys,
- to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD after successful authentication.

The 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 after successful authentication,
- is not allowed to read data in EF.DG3 and EF.DG4 of the logical MRTD.

No terminal is allowed

- to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
- to read any of the EF.DG1 to EF.DG16 of the logical MRTD.

The access control mechanisms ensure that nobody is allowed to read the Document Basic Access Keys and the Personalization Agent Keys.

Test features of the TOE are not available for the user in Phase 4. Deploying test features after TOE delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated,

software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks.

All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

7.1.2 SF_Authentication

After activation or reset of the TOE no user is authenticated.

TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication.

The TOE supports user authentication by the following means:

- Basic Access Control Authentication Mechanism,
- Symmetric Authentication Mechanism based on AES.

The Basic Inspection System authenticates to the TOE by means of Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

The Personalization Agent authenticates himself to the TOE by use of the Personalization Agent Keys with the Symmetric Authentication Mechanism.

The TOE prevents reuse of authentication data related to the Basic Access Control Authentication Mechanism and the Symmetric Authentication Mechanism.

After successful authentication of the terminal with Basic Access Control Authentication Mechanism the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

Protection of user data transmitted from the TOE to the terminal is achieved by means of secure messaging with encryption and message authentication codes once successful authentication of terminal with the Basic Access Control Authentication Mechanism has been completed. After authentication, user data in transit is protected from unauthorized disclosure, modification, deletion, insertion and replay errors.

7.1.3 SF_AssetProtection

The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets of the TOE as well as temporarily stored hash values for data to be signed.

The TOE hides information about IC power consumption and command execution time ensuring that neither the Personalization Agent Keys nor the logical MRTD data nor any other confidential information can be derived from this information.

The TOE ensures any unauthorized users are unable to use the smart card circuit contacts to gain access to Personalization Agent Keys and logical MRTD data.

7.1.4 SF_TSFProtection

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.

The TOE is resistant to physical tampering on the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF the TOE preserves a secure state.

The TOE runs a suite of self-tests during initial start-up, periodically during normal operation, at the reset, verifying correct operation of the TSF.

7.1.5 SF_KeyManagement

The TOE generates 2-key Triple DES keys in accordance with the Document Basic Access Key Derivation Algorithm that uses SHA-1 hash function as specified in [5].

The TOE supports overwriting the cryptographic keys with zero values as follows:

- the BAC Session Keys after detection of an error in a received command by verification of the MAC, and after successful run of the Chip Authentication Protocol,
- any session keys before starting the communication with the terminal in a new power-on-session.

7.2 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 6.3.

The following table lists the Assurance measures and references the corresponding documents describing the measures.

Assurance Measures	Description
AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design,

	in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the operational user guidance documentation and in the documentation for preparative procedures.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in the life cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

Table 10 References of Assurance measures

7.3 Fulfilment of the SFRs

The following table shows the mapping of the SFRs to security functions of the TOE.

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement
FAU_SAS.1	x				
FCS_CKM.1					x
FCS_CKM.4					x
FCS_COP.1/SHA		x			x
FCS_COP.1/ENC		x		x	
FCS_COP.1/AUTH		x		x	
FCS_COP.1/MAC		x		x	
FCS_RND.1		x		x	
FIA_UID.1		x			
FIA_UAU.1		x			
FIA_UAU.4		x			
FIA_UAU.5		x			
FIA_UAU.6		x			
FIA_AFL.1		x			
FDP_ACC.1	x				
FDP_ACF.1	x				

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement
FDP_UCT.1		x			
FDP_UIT.1		x			
FMT_SMF.1	x				
FMT_SMR.1	x				
FMT_LIM.1	x		x		
FMT_LIM.2	x		x		
FMT_MTD.1/INI_ENA	x				
FMT_MTD.1/INI_DIS	x				
FMT_MTD.1/KEY_WRITE	x				
FMT_MTD.1/KEY_READ	x				
FPT_EMSEC.1			x		
FPT_TST.1				x	
FPT_FLS.1				x	
FPT_PHP.3				x	

Table 11 Mapping of SFRs to mechanisms of TOE

7.3.1 Justifications for the correspondence between functional requirements and TOE mechanisms

Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 7.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

7.4 Rationale for PP Claims

This security target is conformant to the claimed PP [19].

8 Glossary and Acronyms

8.1 Glossary

Term	Definition
Active Authentication	Security mechanism defined in [5] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of Organization.
Application Note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
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 Control Access (BAC)	Security mechanism defined in [5] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document 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 from the 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. [5]
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 unauthorised copy or reproduction of a genuine security document made by whatever means. [5]
Country Signing CA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority and 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 [5]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It

Term	Definition
	is stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}). [5]
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.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [5]
Extended Access Control	Security mechanism identified in [5] 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 itself 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 portrait. [5]
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 utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all MRTDs. [5]
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. [5]
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

Term	Definition
	document or visa; or (d) no travel document or visa, if required. [5]
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. [5]
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). [5]
Issuing State	The country issuing the MRTD. [5]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [5]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [5] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16) (6) EF.COM and EF.SOD
Logical Travel Document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye

Term	Definition
	readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [5]
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. [5]
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. [5]
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. [5]
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 [5], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14 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 integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO, [6], 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.

Term	Definition
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 “Enrolment” (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 authentication key used (i) by the Personalization Agent to prove his identity and to 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 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. [5]
reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

Term	Definition
secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [5]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Travel document	A passport or other official document of identity issued by a State or Organisation which may be used by the rightful holder for international travel. [5]
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 [1]).
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 [1]).
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. [5]
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.

8.2 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	Organisational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement

Acronym	Term
TOE	Target of Evaluation
TSF	TOE security functionality

9 Bibliography

9.1 Common Criteria

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

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

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, July 2017

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

[4a] Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, December 2015, Version 1.4, CCDB-2015-12-001

9.2 ICAO

[5] ICAO Doc 9303, Specifications for electronically enabled passports with biometric identification capabilities. In Machine Readable Travel Documents – Part 1: Machine Readable Passport, Volume 2, ICAO, 6th edition, 2006

[6] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

9.3 Cryptography

[7] ISO/IEC 9796-2: Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002

[8] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[9] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[10] Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[11] Federal Information Processing Standards Publication FIPS PUB 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[12] National Institute of Standards and Technology: FIPS PUB 180-4: Secure hash standard, August 2015.

[13] NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999

[14] ANSI X9.62-1999, AMERICAN NATIONAL STANDARD, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998

[15] Certicom Research: SEC 1: Elliptic Curve Cryptography, September 20, 2000, Version 1.0

9.4 Protection Profiles

[16] Common Criteria Protection Profile PP conformant to Smartcard IC Platform, BSI-PP-0002-2001, version 1.0, July 2001

[17] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

[18] Common Criteria Protection Profile Security IC Platform, BSI-PP-0035-2007, version 1.0, June 2007

[19] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, version 1.10, 25th March 2009

[20] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-2009, version 1.10, 25th March 2009

9.5 Technical Guidelines and Directives

[21] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), TR-03110, version 1.11, 21.02.2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[22] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 02.12.1999

[23] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31; Bundesamt für Sicherheit in der Informationstechnik, Version 1, 25.09.2001

[24] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 32; Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Bundesamt für Sicherheit in der Informationstechnik,Version 1, 2.7.2001

9.6 Other

[25] Public Security Target BSI-DSZ-CC-1110-V3-2020, “Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, design step H13”(sanitised public document), Infineon Technologies AG, Version 1.8, 22.04.2020

[26] ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2000

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

[28] Guidance Documentation for the Personalisation Phase STARCOS 3.7 ID C1, Version 2.1 / Status 27.07.2020, Giesecke+Devrient Mobile Security GmbH

-End of Document-