MK Lotus GovID IMDa in BAC Configuration

Security Target Lite

MK Lotus GovID IMDa V4.6.8.8 – Basic Access Control

Common Criteria Evaluation Assurance Level 4+

December 12th, 2025

Revision 1.0

Table of Contents

List of Tables

Abbreviations and Notations

Numerical values
Numbers are printed in decimal, hexadecimal or binary notation.
Hexadecimal values are indicated with a ‘h’ suffix as in XXh, where X is a hexadecimal digit from 0 to F.
Decimal values have no suffix.

Example: the decimal value 179 may be noted as the hexadecimal value B3h.

Denoted text
The text added to provide details on how the TOE implementation fulfils some security requirements is written in *italics* and is preceded by the numbered tag “Application Note”.

Key words
The words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY” and “OPTIONAL” are to be interpreted as described in RFC2119 [1].

1. Introduction

1.1. ST Lite overview

This Security Target Lite (ST Lite) 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 Basic Access Control (BAC) security mechanism and Passive Authentication (PA) mechanism, according to ICAO Doc 9303 Part11 [2].

The ePassport product also supports the following advanced security mechanisms:

- Extended Access Control (EAC) v1, which includes Chip Authentication according to ICAO Doc 9303 Part 11 [2], and Terminal Authentication according to BSI TR-03110 [3] and [4],
- Password Authenticated Connection Establishment (PACE) according to ICAO Doc 9303 Part 11 [2],
- Active Authentication mechanism according to ICAO Doc 9303 Part 11 [2].

which are addressed by another ST [5].

1.2. ST Lite reference

Table 1 ST identification

Title	Security Target Lite - MK Lotus GovID IMDa V4.6.8.8 – Basic Access Control
Version	1.0
Date	2025-12-12
Authors	MK Smart

1.3. TOE reference

Table 2 TOE identification

TOE Name	MK Lotus GovID IMDa in BAC Configuration
TOE Version	V4.6.8.8
TOE identifier	Lotus GovID IMDa V4.6.8.8
TOE Identification Data	47h 4Fh 56h 2Dh 4Dh 4Bh 34h 2Eh 36h 2Eh 38h 2Eh 38h
Developer	MK Smart JSC
Evaluation Sponsor	MK Smart JSC
Evaluation Facility	Applus+ Laboratories

The TOE is delivered as a chip ready for loading of applications. It is identified by the following string, representing the Global Reference:

(ASCII codes 47h 4Fh 56h 2Dh 4Dh 4Bh 34h 2Eh 36h 2Eh 38h 2Eh 38h)

The TOE identification data are in the non-volatile memory of the chip. Instructions for reading identification data are provided by the guidance documentation.

1.4. TOE overview

1.4.1. TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [6] and providing the Basic Access Control, Passive Authentication mechanism according to ICAO Doc 9303 Part11 [2].

The TOE comprises of:

- the circuitry of the MRTD's chip (the integrated circuit, IC), see Appendix A
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software, such as RF contactless library or Crypto library from an IC provider.
- the IC Embedded Software,
- the MRTD application with native acceleration APIs, and
- the associated guidance documentation.

1.4.2. TOE major security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains:

(i) visual (eye readable) biographical data and portrait of the holder,

(ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and

(iii) data elements on the MRTD's chip according to LDS for machine reading.

The authentication of the traveler is based on:

(i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and

(ii) optional 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:

(i) 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:

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

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

(c) the printed portrait.

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

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

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

(c) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both

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

(e) the Document Security Object (SOD).

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

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [2], [6] and [7]. 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 Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This Security Target Lite 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.

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 [2], section 9.8.

1.4.3. TOE type

The TOE type is an electronic travel document representing a contactless smart card programmed according to ICAO Doc 9303 [2], [6] and [7], and BSI TR-03110 [3] and [4].

1.4.4. TOE life cycle

The TOE life-cycle is described in terms of the four life-cycle phases (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 (Cryptolibraries) 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 IC Embedded Software and MRTD application are securely delivered to the Inlay&MRTD manufacturer. The IC Embedded Software and MRTD application are loaded to the IC at the Inlay&MRTD manufacturer, the inlay and the guidance documentation is securely delivered to the personalization agent.

Phase 2 “Manufacturing”

(Step3) In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing. The IC manufacturer also performs the IC encapsulation and the delivery process to the the Inlay&MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the Inlay&MRTD manufacturer.

The Inlay&MRTD manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance FLASH).

(Step4 Optional) The Inlay&MRTD manufacturer combines the IC with hardware (e.g. paper, antenna, cover material) for the contactless interface in the passport cover.

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

Application Note 1 Creation of the application implies: the Applet instantiation.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the Inlay&MRTD manufacturer to the Personalization Agent. The Inlay&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.

(Optional step) The personalization agent combines the IC with hardware (e.g. paper, antenna, cover material) for the contactless interface in the passport cover.

The signing of the Document security object by the Document signer [6] and [7] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Application Note 2 The passport book can be made by the Inlay&MRTD manufacturer in phase 2 or the personalization agent in phase 3.

Application Note 3 The TSF data (data created by and for the TOE, that might affect the operation of the TOE) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Basic Authentication Control Key.

Application Note 4 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 [6] *and* [7]*. This approach allows but does not enforce the separation of these roles.*

Phase 4 “Operational Use”

(Step7) The TOE is used as a MRTD's 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 5 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 6 This ST considers 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 2 or later. 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 outlines the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

The TOE delivery occurs at the end of phase 2 (after pre-personalization).

Table 3 Developer Roles and Actors involved in TOE Life Cycle

Roles	Actors	Phase/Step(s)	Site Identification
IC developer	Infineon	1/1: Development of IC and IC dedicated software	**Infineon Neubiberg R&D** Am Campeon 1-12 85579 Neubiberg Germany
Software developer	MK Smart JSC	1/2: Development and testing of IC Embedded Software (OS) and MRTD application	**MKSmart Factory** Lot 40, Quang Minh Industrial Zone, Me Linh District, Hanoi City, Vietnam.
IC manufacturer	Infineon Technologies AG	2/3: IC manufacturing	**Infineon Singapore Production** Global foundries fab 7, Singapore
		2/3: IC encapsulation	**Infineon Wuxi Production** No.8 Xing Chuang san lu, Singapore Industrial Park, Wuxi, Jiangsu Province, P.R.China **Infineon Regensburg Production** Wernerwerkstr.2 93049 Regensburg Germany
Inlay&MRTD manufacturer	MK Smart JSC	2/4: Embedding of IC with hardware (Optional, see the Application Note 2) 2/5: Loading of OS, MRTD application into chip, and pre-personalization	**MKSmart Factory** Lot 40, Quang Minh Industrial Zone, Me Linh District, Hanoi City, Vietnam.

Note: The IC encapsulation can be conducted by the IC manufacturer at different production sites. The Inlay&MRTD manufacturer will receive the IC module from either Infineon Wuxi Production or Infineon Regensburg Production.

1.4.5. Non-TOE hardware/software/firmware

The TOE is defined to comprise the chip and the complete operating system and application. The inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, in which the antenna is made of pure copper with 0.1mm wire diameter, nevertheless these parts are not inevitable for the secure operation of the TOE.

2. TOE Description

2.1. Physical scope of the TOE

The TOE is comprised of the following parts:

- dual-interface chip IFX_CCI_000039h with firmware 80.306.16.0, including HSL v3.52.9708, UMSLC lib v01.30.0564, NRG SW 05.03.4097, SCL v2.15.000 and ACL v3.35.001, (cf. Appendix A for more details);
- smart card operating system (MK Lotus GovID IMDa in BAC Configuration, v**4.6.8.8**) with its Runtime Environment;
- an International Civil Aviation Organization (ICAO) application (ePassport Applet Information v1.8) compliant with ICAO Doc 9303 [2], [6] and [7];
- guidance documentation in PDF or excel format, example scripts and certificates about the preparation and use of the ICAO application, composed by:

Document/File	Version	Date	Hash value (SHA256)
ICAO Applet Personalization Guide – Additional Information [8]	1.3	2025-08-21	B244C0F4D31D4F4F635785AAEE2861EB5C79630B12E9C8F8DA02EED167D03D96
ePassport Applet Information [9]	1.8	2025-08-08	A64FC1394E2A5237B57E81007375288CA4F85139FE6B357CD2D06AC3076807DE
Operational User Guidance [10]	1.8	2025-12-04	D515ABC2CEFB35AAD6C55D09E90BC40ABD0B86CFDA380F0975D0D5691CD84A5E
Preparative Procedures [11]	1.9	2025-12-04	DF80A6796B40E94DCD77E87D20E6D46C9F08B75D4AEDD4DC9950412035D5C86A
scripts_v1.4_20250724.zip	1.4	2025-07-24	39F4EAA5BC85B4F6D39067AA1E08BAD17595AA4807B36F6B7E6F4374C69F5F15

The example scripts and certificates are delivered in conjunction with the guidance documents to the Personalization Agent for testing purpose. The delivery method for documentation, script files and certificate files are a PGP encrypted and signed format from MK Smart secure lab through email or FTP.

The ICAO application and the OS are loaded on the Infineon chip by Inlay&MRTD manufacturer and delivered to the personalization agent through courier. The chip is delivered in form of IC module or passport book depending on whether the Phase2-Step4 is performed by the Inlay&MRTD manufacturer (see details in section 1.4.4 TOE life cycle).

The ePassport product supports both BAC and PACE operation modes, in which BAC mode as described in the current ST is using as the fallback mechanism and PACE mode as described in another ST is the default operation mode.

2.2. Logical scope of the TOE

The operating system manages all the resources of the integrated circuit that equips the ePassport ICAO document, providing secure access to data and functions.
In more detail, in each life cycle phase/step, access to data and functions is restricted by means of cryptographic mechanisms as follows:

- In phase 3, Personalization, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on SCP03 protocol from the GlobalPlatform card specification [12].
- In phase 4, Operational use, the user must prove his entitlement to access less sensitive data, i.e. DG1, DG2, and DG5 to DG16, by means of the BAC mechanism compliant to ICAO Doc 9303-11 [2].

After a successful authentication, the communication between the ePassport ICAO document and the terminal is protected by the Secure Messaging mechanism defined in section 6 of the ISO 7816-4 specification [13].

The integrity of the data stored under the LDS can be checked by means of the Passive Authentication mechanism defined in [2]. Passive Authentication and BAC mechanisms are described in more detail in the following subsections.

2.2.1. Passive Authentication

Passive Authentication uses a digital signature to authenticate data stored in the data groups on the MRTD chip. This signature is generated in the personalization phase of the MRTD chip over a Document Security Object containing the hash values of all data groups stored on the chip.

Passive Authentication consists of the following steps [2]:
1. The inspection system reads the Document Security Object (SOD), which contains the Document Signer Certificate (CDS, cf. [6]), from the IC.
2. The inspection system builds and validates a certification path from a Trust Anchor to the Document Signer Certificate used to sign the Document Security Object (SOD) according to [7].
3. The inspection system uses the verified Document Signer Public Key (KPuDS) to verify the signature of the Document Security Object (SOD).
4. The inspection system reads relevant data groups from the IC.
5. The inspection system ensures that the contents of the data groups are authentic and unchanged by hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (SOD).

2.2.2. Basic Access Control

Authentication and Key Establishment is provided by a three-pass challenge-response protocol according to ISO/IEC 11770-2 [14], Key Establishment Mechanism 6 using 3DES FIPS 46-3 [15] as block cipher. A cryptographic checksum according to ISO/IEC 9797-1 [16] MAC Algorithm 3 is calculated over and appended to the ciphertexts. The modes of operation described in ICAO Doc 9303 [2] are used. Exchanged nonces must be of size 8 bytes, exchanged keying material must be of size 16 bytes. The inspection system and the IC must not use distinguishing identifiers as nonces.

The BAC session keys generated during BAC authentication are used to protect the confidentiality and integrity of the transmitted data. The key derivation function specified in ICAO Doc 9303 [2] is used, which requires using the hash function SHA-1 to derive the 112 bit Triple-DES key.

Note: Triple-DES algorithm with 112 bit key size and Retail MAC are already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [17]. And SHA-1 is not an agreed hash function.

Triple-DES used in Retail mode and the hash function SHA-1 are included in the evaluation scope for compatibility with ePassport application standards.

3. Conformance Claims

3.1. Common Criteria Conformance Claim

This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017 [18].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017 [19]; as follows: **Part 2 extended**.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017 [20]; as follows: **Part 3 conformant**.

The following methodology will be used for the evaluation:

- Common Criteria for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, April 2017 [21]

The extended security functional requirements are defined in section 6.

3.2. Protection Profile Conformance Claim

This ST claims **strict** conformance to the following protection profile:

- Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control (BAC PP), BSI-CC-PP-0055 (Version 1.10, 25th March 2009) [22]

3.3. Package Conformance Claim

This Security Target claims conformance to:

- EAL 4 assurance package augmented by ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3 defined in the CC part 3 [20]

3.4. Conformance Claim Rationale

The TOE type of this ST is the contactless-only integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [6] and providing the Basic Access Control according to ICAO Doc 9303 Part11 [2], which is consistent to the TOE type defined in the BAC PP [22].

This ST adopts as a reference the ICAO Doc 9303 Eighth Edition 2021. Due to this update, in this ST any references to the ICAO Doc 9303 2006 specification in the BAC PP [22] have been replaced with references to Doc 9303 2021 [2], [6] and [7].

The security problem definition includes all the assets, the subjects, the assumptions, the threats, and the organizational security policies taken from BAC PP [22].

All the security objectives for the TOE and security objectives for the operational environment are taken from BAC PP [22].

All the extended component definitions are taken from BAC PP [22].

The security functional requirements described in section 7 of this ST include the SFRs of BAC PP [22], with some refinements. The following table shows the refinements made to the security functional requirements:

Security Functional Requirement	Rationale
FIA_UAU.5	**Refinement** This SFR is refined to reflect the symmetric authentication mechanism of the personalization agent by means of SCP03 protocol.

4. Security Problem Definition

4.1. Introduction

4.1.1. Assets

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

Logical MRTD Data

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [6]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. 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' [2] the TOE described in this security target 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)

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.

4.1.2. Subjects

This security target considers the following subjects:

Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the Inlay&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 Inlay&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 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 (iv) signing the Document Security Object defined in [6] and [7].

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. The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

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

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

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

> *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.*

4.2. 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.

4.2.1. 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

4.2.2. 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

4.2.3. T.Eavesdropping

Eavesdropping to the communication between the 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

4.2.4. 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

4.2.5. T.Abuse-Func

Abuse of Functionality

Adverse action: An attacker may use functions of the TOE which shall not be used in the phase “Operational Use” 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.

4.2.6. 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 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

4.2.7. 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

4.2.8. 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.

4.3. Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operation.

4.3.1. P.Manufact

Manufacturing of the MRTD's chip

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

4.3.2. P.Personalization

Personalization of the MRTD by issuing State or Organization only

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

4.3.3. P.Personal_Data

Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder 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 [2].

Application Note 8 The organizational security policy P.Personal_Data is drawn from the ICAO ICAO Doc 9303 [2]*. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.*

4.4. Assumptions

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

4.4.1. 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).

4.4.2. 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.

4.4.3. A.Pers_Agent

Personalization of the MRTD's chip

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

4.4.4. A.Insp_Sys

Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [2]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

Application Note 9 *According to* [2] *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.*

4.4.5. 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' [2], 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 10 *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.*

5. Security Objectives

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

5.1. Security Objectives for the TOE

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

5.1.1. 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 [6] 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.DG 3 to EF.DG16 are added.

Application Note 11 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) cannot 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.*

5.1.2. OT.Data_Int

Integrity of personal data

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

5.1.3. 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'* [2] *that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this security target. Thus the read access must be prevented even in case of a successful BAC Authentication.*

5.1.4. 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.

5.1.5. 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.

5.1.6. OT.Prot_Inf_Leak

Protection against Information Leakage

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

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

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.

5.1.7. 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 representing a direct physical probing on the chip's 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.

5.1.8. OT.Prot_Malfunction

Protection against Malfunctions

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have 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.

5.2. Security Objectives for the Operational Environment

Issuing State or Organization

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

5.2.1. 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.

5.2.2. 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.

5.2.3. 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.

5.2.4. 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 all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [6] and [7].

5.2.5. 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’ [2] 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.

5.2.6. 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 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 [2].

5.2.7. OE.Passive_Auth_Verif

Verification by Passive Authentication

The border control officer of the receiving State uses the inspection system to verify the traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects

and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

5.2.8. 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).

5.3. Security Objective Rationale

The following table provides an overview for security objectives coverage.

Table 4 Security Objective Rationale

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

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 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 through 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 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.

6. Extended Components Definition

This security target uses components defined as extensions to CC part 2 [19]. All the components are drawn from the BAC PP [22].

6.1. Definition of the Family FAU_SAS

To define the security functional requirements of the TOE, a sensitive 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.

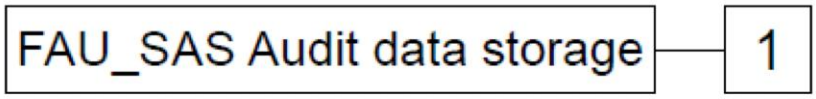
The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behavior

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: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

6.2. Definition of the Family FCS_RND

To describe the IT security functional requirements of the TOE, a sensitive 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.

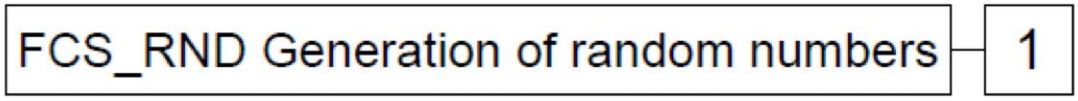
The family 'Generation of random numbers (FCS_RND)' is specified as follows:

FCS_RND Generation of random numbers

Family behavior

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*].

6.3. 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.

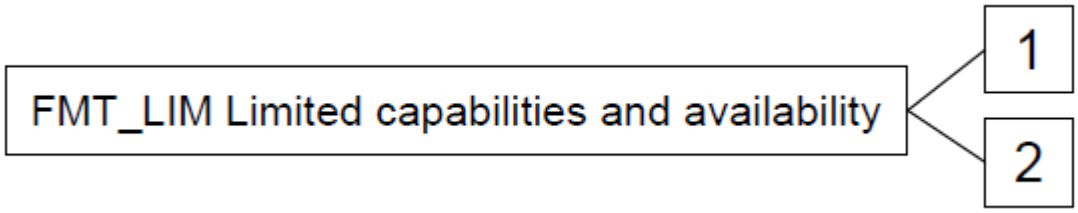
The family 'Limited capabilities and availability (FMT_LIM)' is specified as follows:

FMT_LIM Limited capabilities and availability

Family behavior

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*].

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

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 that there are 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.

6.4. Definition of the Family FPT_EMSEC

The sensitive 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 which are not directly addressed by any other component of CC part 2 [19].

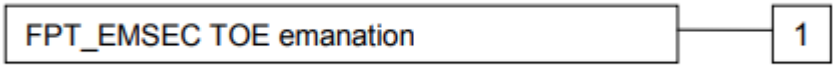
The family ‘TOE Emanation (FPT_EMSEC)’ is specified as follows:

FPT_EMSEC TOE emanation

Family behavior

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*].

7. Security Functional Requirements for the TOE

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment* and *iteration* are defined in sec. 8.1 of Part 1 [18] 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. Refinement of security requirements is denoted by showing the added/changed words in **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text. Selections that have been made by the ST author are denoted as **bold underlined text**.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text. Assignments that have been made by the ST author are denoted as **bold underlined text**.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/" and the iteration indicator after the component identifier.

The definition of the subjects "Manufacturer", "Personalization Agent", "Basic Inspection System" and "Terminal" used in the following chapter is given in section 4.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined in section 12. The operations "write", "read", "modify", and "disable read access" are used in accordance with the general linguistic usage. The operations "transmit", "receive" and "authenticate" are originally taken from [19].

Table 5 Definition of security attributes

Security Attribute	Values	Meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalization Agent	Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

7.1. TOE Security Functional Requirements

7.1.1. Class FAU Security Audit

7.1.1.1. FAU_SAS.1 Audit storage

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies

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

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 Inlay&MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).*

7.1.2. Class FCS Cryptographic Support

7.1.2.1. FCS_CKM.1 Cryptographic key generation

FCS_CKM.1 Cryptographic key generation – Generation of Document Basic Access Keys by the TOE

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [2], section 9.7.

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 ICAO Doc 9303 Part 11* [2]*, section 4.3, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in ICAO Doc 9303 Part 11* [2]*, section 9.7. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.*

Application Note 19 *Triple-DES algorithm with 112 bit key size and Retail MAC are already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM* [17]*. The hash function SHA-1 is required for key derivation, which is also deprecated according to SOG-IS ACM* [17]*. 112bit Triple-DES used in Retail mode and SHA-1 are included in the evaluation scope for compatibility with ePassport application standards.*

7.1.2.2. FCS_CKM.4 Cryptographic key destruction

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 **overwritten by random data** that meets the following: **none**.

Application Note 20 The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

7.1.2.3. FCS_COP.1 Cryptographic operation

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] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes none that meet the following: **FIPS 180-4**.

Application Note 21 This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [2]*.*

Application Note 22 The hash function SHA-1 is deprecated by SOG-IS ACM [17]*. It is in the evaluation scope for compatibility with ePassport application standards.*

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ENC	The TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [15] and [2] section 9.8.

Application Note 23 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.

Application Note 24 Triple-DES algorithm with 112 bit key size is already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [17]*. 112bit Triple-DES is included in the evaluation scope for compatibility with ePassport application standards.*

FCS_COP.1/AUTH Cryptographic operation – Authentication

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication – encryption and decryption in accordance with a specified cryptographic algorithm **AES** and cryptographic key sizes **128, 192, 256** bit that meet the following: **FIPS 197** [23]**.**

Application Note 25 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).

Application Note 26 The GP mutual authentication with SCP03 protocol is used as the authentication mechanism for the Personalization Agent.

FCS_COP.1/MAC Cryptographic operation – Retail MAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [16].

Application Note 27 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.

Application Note 28 The Retail MAC algorithm is already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [17]*. It is included in the evaluation scope for compatibility with ePassport application standards.*

7.1.2.4. FCS_RND.1 Random Number Generation

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 **quality criteria defined in AIS-31 publication by the German BSI. In particular, it considers requirements for devices belonging to the functional class PTG.2 (strength of mechanism: high)**.

Application Note 29 This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

7.1.3. Class FIA Identification and Authentication

The Table 6 provides an overview on the authentication mechanisms used.

Table 6 Overview of authentication mechanisms

Name	**SFR for the TOE**	**Algorithms and key sizes according to** [2]
Basic Access Control Authentication Mechanism	FIA_UAU.4 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	FIA_UAU.4	AES with 128 up to 256 bit keys (cf. FCS_COP.1/AUTH)

7.1.3.1. FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,

2. to read the random identifier in Phase 3 “Personalization of the MRTD”,

3. to read the random identifier in Phase 4 “Operational Use”.

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

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

Application Note 30 *The IC manufacturer and the Inlay&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 Inlay&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 31 *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 than one RFID. If this identifier is randomly selected it will not violate the OT.Identification.*

7.1.3.2. FIA_UAU.1 Timing of authentication

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

Application Note 32 *The Basic Inspection System and the Personalization Agent authenticate themselves.*

7.1.3.3. FIA_UAU.4 Single-use authentication mechanisms

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 is based on **AES**.

Application Note 33 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.

Application Note 34 The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [2]*. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.*

7.1.3.4. FIA_UAU.5 Multiple authentication mechanisms

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 by means of SCP03 protocol**

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) **the Symmetric Authentication Mechanism with the Personalization Agent Key**,

2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

Application Note 35 The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Basic Inspection System uses the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. The Personalization Agent can be authenticated using the symmetric AES-

based authentication mechanism by means of SCP03 protocol from GlobalPlatform card specification [12].

7.1.3.5. FIA_UAU.6 Re-authenticating

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

Application Note 36 *The Basic Access Control Mechanism specified in* [2] *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 37 *Note that in case the TOE should also fulfill* [24] *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.*

7.1.3.6. FIA_AFL.1 Authentication Failure handling

FIA_AFL.1 Authentication failure handling	
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when **1** unsuccessful authentication attempts occur related to **BAC authentication protocol**.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **met or surpassed**, the TSF shall **block next authentication attempts**.

7.1.4. Class FDP User Data Protection

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

7.1.4.1. FDP_ACC.1 Subset access control

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 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.

7.1.4.2. FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Basic 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 to objects based on the following: 1.Subjects: a. Personalization Agent, b. Basic Inspection System, c. Terminal, 2.Objects: a. data EF.DG1 to EF.DG16 of the logical MRTD, b. data in EF.COM, c. data in EF.SOD, 3.Security attributes: a. authentication status of terminals.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,

2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.

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

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

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.

2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.

3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.

Application Note 38 The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this security target (cf. [5] *for details).*

7.1.4.3. FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1 Basic data exchange confidentiality – MRTD

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure.

7.1.4.4. FDP_UIT.1 Data exchange integrity

FDP_UIT.1 Data exchange integrity - MRTD

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

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

7.1.5. Class FMT Security Management

The SFRs FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

The SFRs 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.

7.1.5.1. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1. Initialization, 2. Pre-personalization, 3. Personalization.

7.1.5.2. FMT_SMR.1 Security Roles

FMT_SMR.1 Security Roles

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

7.1.5.3. FMT_LIM.1 Limited capabilities

FMT_LIM.1 Limited capabilities	
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated 2. TSF data to be disclosed or manipulated 3. software to be reconstructed and 4. substantial information about construction of TSF to be gathered which may enable other attacks.

7.1.5.4. FMT_LIM.2 Limited availability

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 does not allow 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated 3. software to be reconstructed and 4. substantial information about construction of TSF to be gathered which may enable other attacks.

Application Note 39 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.

7.1.5.5. FMT_MTD.1 Management of TSF data

The following SFRs are iterations of the component Management of TSF data (FMT_MTD.1) addressing different management functions and different TSF data. The TSF data include but are not limited to those identified below.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/INI_ENA	The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

Application Note 40 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 Data and Pre-personalization Data

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.

Application Note 41 According to P.Manufact the IC Manufacturer and the Inlay&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 may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The Inlay&MRTD manufacturer will write the Pre-personalization Data.

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

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

Application Note 42 The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

7.1.6. 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.

7.1.6.1. FPT_EMSEC.1 TOE Emanation

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

FPT_EMSEC.1.1	The TOE shall not emit **the shape and amplitude of signals, the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines during internal operations or data transmissions** in excess of **unintelligible limits** enabling access to Personalization Agent Key(s) and **Document Basic Access Keys and User Data.**
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and **Document Basic Access Keys and User Data**.

Application Note 43 *The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2* [25] *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.

7.1.6.2. FPT_FLS.1 Failure with preservation of secure state

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.

7.1.6.3. FPT_TST.1 TSF testing

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** to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Application Note 44 The self test for the verification of the integrity of stored TSF executable code is executed during initial start-up in the Phase 2 Manufacturing.

7.1.6.4. FPT_PHP.3 Resistance to physical attack

FPT_PHP.3 Resistance to physical attack

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

Application Note 45 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.

8. Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3

The following table shows the list of Security Assurance Requirements (SARs) for the TOE.

Table 7 TOE assurance requirements

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_INT.2, ADV_TDS.4
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2
ASE	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
ATE	ATE_COV.2, ATE_DPT.3, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.3

9. Security Requirements Rationale

9.1. Security Functional Requirements Rationale

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

Table 8 Coverage of TOE security objectives by SFRs

	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					
FCS_CKM.4	X		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	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					
FDP_ACC.1	X	X	X					
FDP_ACF.1	X	X	X					
FDP_UCT.1		X	X					
FDP_UIT.1		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		

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

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR **FIA_UAU.4** and **FIA_UAU.5**. The Personalization Agent can be authenticated based on GlobalPlatform SCP03 protocol by using the symmetric authentication mechanism (**FCS_COP.1/AUTH**). The random challenge used in SCP03 protocol is generated according to SFR **FCS_RND.1**.

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 of the groups EF.DG1 to EF.DG16 of the logical MRTD (**FDP_ACF.1.2, rule 1**) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. **FDP_ACF.1.4**). The SFR **FMT_SMR.1** lists the roles (including Personalization Agent) and the SFR **FMT_SMF.1** lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR **FIA_UAU.4**, **FIA_UAU.5** and **FIA_UAU.6** using **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 34). 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.

9.2. Dependency Rationale

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

The table below shows the dependencies between the SFR of the TOE.

Table 9 SFR dependencies

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, or 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, or 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],	Fulfilled by FCS_CKM.1, Fulfilled by FCS_CKM.4

	FCS_CKM.4 Cryptographic key destruction	
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_IFC.1 Subset information flow control or FDP_ACC.1 Subset access 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_IFC.1 Subset information flow control or FDP_ACC.1 Subset access 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 Limited availability	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1 Limited capabilities	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_READ	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

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

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

Justification 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

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

Justification 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.

Justification 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.

9.3. 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 assurance components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3 are augmented to EAL4.

ADV_FSP.5 Complete Semi-formal functional specification with additional error information

The selection of the component ADV_FSP.5 provides a better coverage of the functional specification with semi-formal modelling and additional error information.

The component ADV_FSP.5 has the following dependencies: ADV_TDS.1 and ADV_IMP.1. The dependencies are fulfilled by ADV_TDS.4 and ADV_IMP.1.

ADV_INT.2 Well-structured internals

The selection of the component ADV_INT.2 provides additional information regarding the TSF internals by analyzing the complexity to justify it is well-structured.

The component ADV_INT.2 has the following dependencies: ADV_IMP.1, ADV_TDS.3 and ALC_TAT.1. The dependencies are fulfilled by ADV_IMP.1, ADV_TDS.4 and ALC_TAT.2.

ADV_TDS.4 Semiformal modular design

The selection of the component ADV_TDS.4 provides enhanced design of the TOE introducing semi-formal modelling of the subsystems and differentiating the roles of the modules regarding each TSF.

The component ADV_TDS.4 has the following dependency: ADV_FSP.5. The dependency is fulfilled by ADV_FSP.5.

ALC_CMS.5 Development tools CM coverage

The selection of the component ALC_CMS.5 provides improved configuration management by covering the development tools (compiler options, build options etc…).

The component ALC_CMS.5 has no dependencies.

ALC_DVS.2 Sufficiency of security measures

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

The component ALC_DVS.2 has no dependencies.

ALC_TAT.2 Compliance with implementation standards

The selection of the component ALC_TAT.2 provides additional information on the implementation standards applied by the developer.

The component ALC_TAT.2 has the following dependency: ADV_IMP.1. The dependency is fulfilled by ADV_IMP.1.

ATE_DPT.3 Testing: modular design

The selection of the component ATE_DPT.3 provides improved testing depth by requiring modular testing versus testing focused on the TSF-enforcing modules.

The component ATE_DPT.3 has the following dependencies: ADV_ARC.1, ADV_TDS.4 and ATE_FUN.1. The dependencies are fulfilled by ADV_ARC.1, ADV_TDS.4 and ATE_FUN.1.

9.4. 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´s security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in section 9.2 “Dependency Rationale” for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 9.3 “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 section 9.2 “Dependency rationale” and 9.3 “Security assurance requirements rationale”. Furthermore, as also discussed in section 9.3 “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.

10. TOE Summary Specification

10.1. Implementation of SFRs in the TOE

The following table provides a general understanding of how the TOE is implemented by describing how the TOE meets each SFR.

Table 10 Implementation of SFRs in the TOE

SFR	Implementation
FAU_SAS.1	The Manufacturer stores IC identification data in the audit records.
FCS_CKM.1	The TOE generates session keys for Secure Messaging soon after a successful BAC authentication of the Basic Inspection System. The TOE uses 112 bit Triple-DES encryption key and the Retail-MAC message authentication key as the session keys.
FCS_CKM.4	Session keys in RAM are filled with random numbers when a Secure Messaging session is closed.
FCS_COP.1/SHA	The TOE implements hashing algorithm SHA-1 to be used for key derivation during BAC authentication.
FCS_COP.1/ENC	During a Secure Messaging session after a BAC authentication, the TOE encrypts transmitted data to ensure confidentiality, and decrypts received data, to restore original content. To this end, the TOE uses Triple-DES in CBC mode with 112-bit encryption key.
FCS_COP.1/AUTH	The TOE implements symmetric authentication mechanism for the Personalization Agent by means of GP SCP03 protocol. The TOE uses AES with key size 128, 192 or 256 bit (depending on the personalization of the security domains) as the Card Manager Key.
FCS_COP.1/MAC	During a Secure Messaging session after a BAC authentication, the TOE computes a Message Authentication Code (MAC) to check integrity of received data, and to allow integrity check by the terminal. The MAC computation is performed according to Retail MAC algorithm and cryptographic key sizes 112 bit according to ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2 [16].
FCS_RND.1	The TOE generates random numbers to be used during authentication protocols according to AIS31 class PTG.2 [26].
FIA_UID.1	The TOE applies access control policies to guarantee that the following actions can be performed before the user is identified: • read access to the initialization data and to the random identifier, • read access to any other data requires a successful execution of BAC protocol (in the operational use phase).

	Any other action is forbidden without prior user identification. The required access privileges are set for each data set by the agent that writes the related persistent object.
FIA_UAU.1	The TOE applies access control policies to guarantee that the following actions can be performed before the user is authenticated: • read access to the initialization data and to the random identifier, • read access to any other data requires a successful execution of BAC protocol (in the operational use phase). Any other action is forbidden without prior user authentication. The required access privileges are set for each data set by the agent that writes the related persistent object.
FIA_UAU.4	The TOE generates the random challenge or nonce used for the authentication mechanisms by a random number generator of class PTG.2. The reuse of these authentication data is forbidden.
FIA_UAU.5	The TOE provides: • the BAC authentication mechanism to authenticate the user in the operational use phase with 112-bit 3DES Document Basic Access Keys; • the symmetric authentication mechanism (SCP03 protocol) to authenticate the Personalization Agent with Card Manager Keys.
FIA_UAU.6	Secure Messaging established after a successful BAC authentication provides re-authentication of the user by the verification of message authentication code. The TOE only accepts the commands received from the previously authenticated BAC user.
FIA_AFL.1	When the BAC authentication fails, the TOE closes the current session, overwrites SSC (Send Sequence Counter) and session keys with random numbers and goes to the initial BAC state.
FDP_ACC.1	The TOE applies the Basic Access Control Policy to check that terminals wanting to access protected data possess the required privileges and have successfully completed the required authentication. The TSF checks the possess of the above requirements before any access to protected data.
FDP_ACF.1	The TOE keeps a security status for each of the data object related to the protected data listed in this SFR to guarantee entitlement to read and/or write those data. The TSF checks the security status is checked before any access to the protected data. In the personalization phase, only the authenticated personalization agent through GP SCP03 authentication can write and read the data of TOE. In the operational use phase, only the authenticated Basic Inspection System through BAC authentication can read the less sensitive data stored in the TOE.
FDP_UCT.1	The TOE protects data confidentiality of received and transmitted data by means of Triple-DES cryptography within Secure Messaging

	sessions in MAC-ENC mode, which is established after successful BAC authentication.
FDP_UIT.1	The TOE guarantees data integrity by means of a Message Authentication Code (MAC) within Secure Messaging sessions in MAC-ENC mode, which is established after successful BAC authentication. The MAC is computed on data to be transmitted and sent by the TOE to the terminal together with the data and is checked upon data reception to allow tampering detection. The TOE also checks the MAC of data received from the terminal to verify the integrity.
FMT_SMF.1	The TOE provides features for storing Initialization data, Pre-personalization Data and Personalization Data, ensuring that only the entitled manufacturers and agents are able to do so.
FMT_SMR.1	The TOE distinguishes between the roles Manufacturer, Personalization Agent and Basic Inspection System, and grants each of them the access privileges allowed by the security policies. All the above roles are implicitly identified via the corresponding authentication key.
FMT_LIM.1	The test features of the OS, as well as the authentication mechanism granting access to them, are permanently disabled in the evaluated configuration of the OS. As regards the test features of the IC, information on their limitation is provided in the TOE summary specification of the public security target of the supported IC for platform SFRs FMT_LIM.1, FMT_LIM.2 [27].
FMT_LIM.2	The same as in FMT_LIM.1
FMT_MTD.1/INI_ENA	In the manufacturing phase, only the entitled manufacturers can write the initialization data and pre-personalization data into TOE. The TSF checks the access privileges before any access is made.
FMT_MTD.1/INI_DIS	Only the Personalization Agent can block the read access to the initialization data. The Personalization Agent must be successfully authenticated before the execution of this action. The initialization data is not allowed to be read out by the users in the operational use phase.
FMT_MTD.1/KEY_WRITE	The Document Basic Access Keys can be written by the Personalization Agent only. The Personalization Agent must be successfully authenticated before writing the keys.
FMT_MTD.1/KEY_READ	The property defining read access conditions of Document Basic Access Keys and Personalization Agent Keys are set when those keys are written, so that the keys cannot be read by anyone under any circumstances. The TSF checks the access privileges before any access is made to those keys.
FPT_EMSEC.1	Leakage of confidential data through side channels is prevented by the security features of both the IC and the OS, in accordance with the security recommendations contained in the IC guidance documentation [28].

FPT_TST.1	During initial start-up, the IC performs a self-test procedure that tests alarm lines and environmental sensor mechanisms, and the OS checks the integrity of the specific code space that is sensitive for the system (configuration data, internal states, memory boundaries…) by computing a hash value of the code and comparing it with a reference hash value stored internally. In case any one of such checks fails, the OS will call the sec_reset() macro following the IC security recommendation. A fallback to an infinite loop is present in the case the call to the security reset won't work for any reason.
FPT_FLS.1	In case self-test fails or a physical attack is detected, the OS enters an endless loop, so that all cryptographic operations and data output interfaces are inhibited.
FPT_PHP.3	Detection of physical attacks is ensured by the security features of both the IC and the OS, in accordance with the security recommendations contained in the IC guidance documentation [28].

10.2. Assurance Measures

Assurance measures applied to the TOE are fully compliant to those described in part 3 of the Common Criteria v3.1 [20].

The implementation is based on a description of the security architecture of the TOE and on a semi-formal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements. These documents, together with the source code of the software, address the ADV_ARC, ADV_FSP, ADV_TDS and ADV_IMP families.

The configuration management plan addresses the ALC_CMC and ALC_CMS families and enforces good practices to securely manage configuration items including, but not limiting to, design documentation, user documentation, source code, test documentation and test data.

The configuration management process guarantees the separation of the development configuration libraries from the configuration library containing the releases and also supports the generation of the TOE.
All the configuration items are managed with the help of automated tools. In particular configuration items regarding security flaws are managed with the support of an issue tracking system, while all the other configuration items are managed with the help of a version control system.

The software test process, addressing the class ATE, is machine-assisted to guarantee a repeatable error-free execution of the same test chains in both the system test and in the validation phases.

A secure delivery of the TOE is guaranteed by the application of dedicated procedures. The prevention measures, the checks and all the actions to be performed at the developer's site are described in the secure delivery procedure addressing the family ALC_DEL, while the security measures related to delivery to be applied at the user's site are defined in the personalization guidance. The latter document also addresses the family AGD_PRE.

The information for TOE usage after delivery to the legitimate holder is provided by the guidance for the operational use. These documents address the AGD_OPE assurance family.

To protect the confidentiality and integrity of the TOE design and implementation, the development and production environment and tools conform to the security policies defined in the documentation dedicated to the development security, which addresses the family ALC_DVS.

The life-cycle model adopted in the manufacturing phases and the tools supporting the development and production of the TOE are described in dedicated documents addressing the families ALC_LCD and ALC_TAT.

An independent vulnerability analysis, meeting requirements of the family AVA_VAN, is conducted by a third party.

Due to the composite nature of the evaluation, which is based on the CC evaluation of the hardware, the assurance measures related to the platform (IC) are covered by documents from the IC manufacturer [29] [27]. The security procedures described in such documents have been taken into consideration.

11. Statement of Compatibility

This section provides an analysis of the compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) [27].

The following sections identify the parts of the Platform-ST that are relevant for the composite TOE. Subsequent sections aim to demonstrate the compatibility of each of those parts of the Platform-ST with their counterpart of the Composite-ST (the document at hand).

11.1. Relevance of the parts of the Platform-ST

The parts of the Platform-ST taken into account for the relevance evaluation are:

- Security Functional Requirements (SFRs)
- Security Objectives for the TOE
- Security Objectives for the operational environment

In the Platform-ST, some SFRs are defined inside the ST itself, and for the remaining SFRs the Platform-ST relies on the definition given in the IC Protection Profile BSI-CC-PP-0084-2014 [30].

The following table shows the mapping between the SFRs for the composite product (defined in the current ST) with the SFRs defined in the platform-ST [27]. In those cases where a matching exists, the platform-SFR is considered as relevant; otherwise, the platform-SFR is considered as not relevant (IP_SFR).

The irrelevant platform-SFRs (**IP_SFR**) are listed as below:

FDP_SDC.1, FDP_SDI.2, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG, FCS_RNG.1/DRNG4, FCS_RNG.1/RCL/TRNG, FCS_RNG.1/RCL/DRNG3, FCS_RNG.1/RCL/DRNG4, FMT_LIM.1/Loader, FMT_LIM.2/Loader, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader, FDP_ACF.1/Loader, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FCS_COP.1/SCL/AES-MAC, FCS_COP.1/RSA/ENC_v3.02.000, FCS_COP.1/RSA/ENC_v3.33.003_v3.34.000_v3.35.001, FCS_COP.1/RSA/DEC, FCS_COP.1/RSA/DEC_CRT, FCS_COP.1/RSA/SIG, FCS_COP.1/RSA/VER, FCS_COP.1/RSA/RSA_DH, FCS_CKM.1/RSA/<iteration>, FCS_CKM.4/RSA, FCS_COP.1/ECC/<iteration>, FCS_CKM.1/ECC, FCS_CKM.4/ECC, FCS_COP.1/HCL, FMT_MTD.1/Loader, FMT_SMR.1/Loader, FMT_SMF.1/Loader, FIA_UID.2/Loader, FPT_FLS.1/Loader, FIA_API.1, FCS_COP.1/RSA/SIG_CRT

The relevant Platform-ST SFRs are categorized to two groups:

- **RP_SFR-SERV**: Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.
- **RP_SFR-MECH:** Relevant Platform-SFRs being used by the Composite-ST because of its security properties providing protection against attacks to the TOE as a whole and are addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the Platform TOE.

Table 11 Relevance of the Platform-ST SFRs

Platform-ST SFRs	Composite-ST SFRs	Category
FAU_SAS.1	FAU_SAS.1	RP_SFR-SERV
FCS_COP.1/SCP/TDES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/TDES-MAC FCS_RNG.1/TRNG	FCS_CKM.1	RP_SFR-SERV
FCS_CKM.4/SCP FCS_CKM.4/SCL	FCS_CKM.4	RP_SFR-SERV
FCS_COP.1/SCP/TDES FCS_COP.1/SCL/TDES	FCS_COP.1/ENC	RP_SFR-SERV
FCS_COP.1/SCP/AES FCS_COP.1/SCL/AES	FCS_COP.1/AUTH	RP_SFR-SERV
FCS_COP.1/SCL/TDES-MAC	FCS_COP.1/MAC	RP_SFR-SERV
FCS_RNG.1/TRNG	FCS_RND.1	RP_SFR-SERV
FCS_RNG.1/TRNG	FIA_UAU.4	RP_SFR-SERV
FMT_LIM.1 FMT_LIM.2	FMT_LIM.1	RP_SFR-SERV
FMT_LIM.1 FMT_LIM.2	FMT_LIM.2	RP_SFR-SERV
FDP_ITT.1 FDP_IFC.1 FPT_ITT.1	FPT_EMSEC.1	RP_SFR-MECH
FRU_FLT.2 FPT_FLS.1	FPT_FLS.1	RP_SFR-MECH
FRU_FLT.2 FPT_FLS.1 FPT_TST.2	FPT_TST.1	RP_SFR-MECH
FPT_PHP.3	FPT_PHP.3	RP_SFR-MECH

The following table shows the mapping between the relevant platform-SFRs (analyzed above) with the platform-ST security objectives [27]. In those cases where a matching exists, the platform-ST security objective is considered as relevant; otherwise, the platform-ST security objective is considered as not relevant and not listed.

Table 12 Relevance of the Platform-ST security objectives for the TOE

Relevant Platform-ST SFRs	Platform-ST Security objectives for the TOE
FAU_SAS.1	O.Identification
FCS_CKM.4/SCP	O.TDES
FCS_CKM.4/SCL	O.TDES O.AES-TDES-MAC
FCS_COP.1/SCP/TDES	O.TDES
FCS_COP.1/SCL/TDES	O.AES-TDES-MAC O.TDES
FCS_COP.1/SCP/AES	O.AES

FCS_COP.1/SCL/AES	O.AES-TDES-MAC O.AES
FCS_COP.1/SCL/TDES-MAC	O.AES-TDES-MAC
FCS_RNG.1/TRNG	O.RND
FMT_LIM.1	O.Abuse-Func
FMT_LIM.2	O.Abuse-Func
FDP_ITT.1	O.Leak-Inherent O.Leak-Forced O.Abuse-Func O.RND
FDP_IFC.1	O.Leak-Inherent O.Leak-Forced O.Abuse-Func O.RND
FPT_ITT.1	O.Leak-Inherent O.Leak-Forced O.Abuse-Func O.RND
FRU_FLT.2	O.Malfunction O.Leak-Forced O.Abuse-Func O.RND
FPT_FLS.1	O.Malfunction O.Leak-Forced O.Abuse-Func O.RND
FPT_TST.2	O.Phys-Manipulation
FPT_PHP.3	O.Phys-Probing O.Phys-Manipulation O.Leak-Forced O.Abuse-Func O.RND

11.2. Compatibility of the security functional requirements

According to the analysis presented in section 11.1, the compatibility of the security functional requirements is presented in the following table:

Table 13 Compatibility of the security functional requirements

Relevant Platform-ST SFRs	Composite-ST SFRs	Rationale
FAU_SAS.1	FAU_SAS.1	The platform provides the capability to load the Initialization Data and Pre-personalization Data to the TOE memory.
FCS_COP.1/SCP/TDES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/TDES-MAC FCS_RNG.1/TRNG	FCS_CKM.1	The platform supports the security feature of TOE for cryptographic key generation.
FCS_CKM.4/SCP FCS_CKM.4/SCL	FCS_CKM.4	The platform supports the security feature of TOE for cryptographic key destruction.

FCS_COP.1/SCP/TDES FCS_COP.1/SCL/TDES	FCS_COP.1/ENC	The platform supports the security feature of TOE to perform secure messaging – encryption and decryption in accordance with a specified Triple-DES cryptographic algorithm.
FCS_COP.1/SCP/AES FCS_COP.1/SCL/AES	FCS_COP.1/AUTH	The platform provides an authentication mechanism to support TOE for Personalization Agent Authentication.
FCS_COP.1/SCL/TDES-MAC	FCS_COP.1/MAC	The platform supports the security feature of TOE to perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC.
FCS_RNG.1/TRNG	FCS_RND.1	The platform provides the capability for TOE to generate random numbers.
FCS_RNG.1/TRNG	FIA_UAU.4	The platform supports the security feature of TOE to prevent reuse of authentication data.
FMT_LIM.1 FMT_LIM.2	FMT_LIM.1	The platform supports the security feature of TOE to provide protection against misuse of test features.
FMT_LIM.1 FMT_LIM.2	FMT_LIM.2	The platform supports the security feature of TOE to provide protection against misuse of test features.
FDP_ITT.1 FDP_IFC.1 FPT_ITT.1	FPT_EMSEC.1	The platform supports the TOE to detect the attacks based on inherent observable physical phenomena.
FRU_FLT.2 FPT_FLS.1	FPT_FLS.1	The platform supports the TOE to preserve a secure state when certain types of failures occur.
FRU_FLT.2 FPT_FLS.1 FPT_TST.2	FPT_TST.1	The platform supports the TOE to run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF and verify the integrity of the TSF data.
FPT_PHP.3	FPT_PHP.3	The platform supports the TOE to implement appropriate mechanisms to continuously counter physical manipulation and physical probing.

11.3. Compatibility of the security objectives for the TOE

According to the analysis presented in section 11.1, this section shows that the relevant security objectives of the Platform-ST are compatible with the ones of this Composite-ST with no contradictions. The mapping of the security objectives for the TOE is presented in the following table:

Table 14 Compatibility of the security objectives for the TOE

Relevant Platform-ST Security Objectives for the TOE	Composite-ST Security Objectives for the TOE
O.Identification	OT.Identification
O.AES	OT.AC_Pers OT.Data_Int
O.TDES	OT.Data_Int OT.Data_Conf

O.AES-TDES-MAC	OT.AC_Pers OT.Data_Int OT.Data_Conf
O.RND	OT.AC_Pers OT.Data_Int OT.Data_Conf OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys_Tamper
O.Leak-Inherent	OT.AC_Pers OT.Prot_Inf_Leak
O.Leak-Forced	OT.AC_Pers OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys_Tamper OT.Data_Int
O.Abuse-Func	OT.Data_Int OT.AC_Pers OT.Prot_Inf_Leak OT.Prot_Abuse-Func OT.Prot_Malfunction OT.Prot_Phys_Tamper
O.Malfunction	OT.Prot_Inf_Leak OT.Prot_Malfunction
O.Phys-Manipulation	OT.Data_Int OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys_Tamper
O.Phys-Probing	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper

11.4. Compatibility of the security objectives for the operational environment

The following table determines the *significant* Security Objectives for the Operational Environment of Platform-ST and their relevance for the TOE.
The Security Objectives for the Operational Environment of Platform-ST are classified as three groups:

- **IrOE:** The objectives for the environment being not relevant for the Composite-ST, e.g. the objectives for the environment about the developing and manufacturing phases of the base component.
- **CfPOE:** The objectives for the environment being fulfilled by the Composite-ST automatically.
- **SgOE**: The remaining objectives for the environment of the Platform-ST belonging neither to the group IrOE nor CfPOE. This group makes up the significant objectives for the environment for the composite-ST, which shall be addressed in the composite-ST.

Table 15 Tracing of Security Objectives of the Platform ST for Operational Environment

Security objectives of Platform ST for Operational Environment	**IrOE**	**CfPOE**	**SgOE**
OE.Resp-Appl		X	

OE.Process-Sec-IC	X		
OE.Lim_Block_Loader		X	
OE.Loader_Usage		X	
OE.TOE_Auth	X		
OE.Prevent_Masquerade		X	
OE.Secure_Load_ACode		X	

NOTE: The “OE.Process-Sec-IC” has been addressed by the assurance class ALC in the platform-ST. The “OE.TOE_Auth” is not relevant since the composite-ST has no any security objective related to the authentication with external entities.

Table 16 Mapping of Security Objectives of the Platform-ST for Operational Environment (CfPOE)

Security objectives of Platform ST for Operational Environment (CfPOE)	**Security objectives of Composite ST for TOE**	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
OE.Resp-Appl			X	X		X	X	X	
OE.Lim_Block_Loader						X			X
OE.Loader_Usage		X			X				
OE.Prevent_Masquerade			X	X		X			X
OE.Secure_Load_ACode		X							

11.5. Compatibility of the security assurance requirements

The Platform-ST claims conformance to the protection profile BSI-PP-0084 [30] with the following assurance level and augmentation:

- EAL6 augmented with ALC_FLR.1

The Composite-ST claims conformance to the following assurance level and augmentations:

- EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3

Therefore, the security assurance requirements of Platform-ST and Composite-ST are compatible as all the requirements of Composite-ST are covered by those of Platform-ST.

11.6. Results of compatibility analysis

The compatibility analysis is based on the evaluation of the relevance for the composite TOE of the parts of the Platform-ST. The relevance criteria have been determined according to ASE_COMP [31].

The rationale provided in the previous sections proved that there is no contradiction between the relevant parts of the Platform-ST and their counterparts in the Composite-ST.

12. Glossary and Acronyms

Glossary

Term	Definition
Active Authentication	Security mechanism defined in ICAO Doc 9303 [2] 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 ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the MRTD's chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined in ICAO Doc 9303 [2] 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. [6]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [2]
Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the document issuer with respect to confirming correctness of user and TSF data stored in the MRTD. The CSCA represents the country specific root of the PKI for the MRTDs and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA certificate (CCSCA) having to be distributed by strictly secure diplomatic means; see [7].
Country Signing CA Certificate (CCSCA)	Self-signed certificate of the Country Signing CA Public Key (KPUCSCA) issued by Country Signing Certification Authority 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 [2]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SOD)	A RFC3369 CMS Signed Data Structure [32], signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [6] [7]
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. [6]
Extended Access Control (EAC)	Security mechanism identified in [3] [4] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [6]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs.
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
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 Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document 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.
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required.
Initialization	Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.4.4, 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.
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).
Issuing State	The Country issuing the MRTD.
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [6]. The capacity expansion technology used is the MRTD's chip.

Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [6] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (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
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [6]
Machine readable visa (MRV)	A visa or, where appropriate, an entry clearance (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.
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [6]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a MRTD in a form that can be read and verified by machine. [6]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [6] - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14, EF.DG 16, 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 [33] [34] and programmed according to the Logical Data Structure as specified by ICAO [6].
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 finger print and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. sec. 1.4.4, 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 their identity and get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to): 1.biographical data, 2.data of the machine-readable zone, 3.photographic image and 4.other data.
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf. sec. 1.4.4, 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 Inlay&MRTD manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
Primary Inspection System (PIS)	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. [6]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [13]
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Travel document	A passport or other official document of identity issued by a State or Organization, which may be used by the rightful holder for international travel.
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 [18]).
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 [18]).
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. [6]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
AA	Active Authentication
AES	Advanced Encryption Standard
ASC	Application Secret Code
ASCII	American Standard Code for Information Interchange
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CAN	Card Access Number
CBC	Cipher Block Chaining
CC	Common Criteria
CSCA	Country Signing Certification Authority
CV	Card Verifiable
CVCA	Country Verifying Certification Authority
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DF	Dedicated File
DG	Data Group
DH	Diffie-Hellman
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman

ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
EIS	Extended Inspection System
ICAO	International Civil Aviation Organization
ICCSN	Integrated Circuit Card Serial Number.
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine readable zone
N/A	Not applicable
OSP	Organizational security policy
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PKI	Public Key Infrastructure
PP	Protection Profile
PT	Personalization Terminal
RF	Radio Frequency
SAR	Security assurance requirements
SFR	Security functional requirement
SHA	Secure Hash Algorithm
SIP	Standard Inspection Procedure
SPA	Simple Power Analysis
ST	Security Target
TA	Terminal Authentication
TDES	Triple DES
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
TSP	TOE Security Policy (defined by the current document)

13. References

[1] Network Working Group, RFC2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.

[2] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Doc 9303, Machine Readable Travel Documents Part 11: Security Mechanisms for MRTDs, Eighth Edition, 2021.

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

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

[5] MK Smart JSC, Security Target Lite MK Lotus GovID IMDa V4.6.8.8 - Extended Access Control with PACE, Version 1.0, 2025-12-12.

[6] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Doc 9303, Machine Readable Travel Documents Part 10: Logical Data Structure (LDS) for Storage of Biometrics, Eighth Edition, 2021.

[7] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Doc 9303, Machine Readable Travel Documents Part 12 — Public Key Infrastructure for MRTDs, Eighth Edition, 2021.

[8] ICAO Applet Personalization Guide - Additional Information, V1.3.

[9] ePassport Applet Information, V1.8.

[10] Operational User Guidance, Version 1.8.

[11] Preparative Procedures, Version 1.9.

[12] GlobalPlatform Inc., "GlobalPlatform Card Specification, version 2.3.1," December 2017.

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

[14] ISO/IEC, International Standard 11770-2, Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques, Edition 3, 2018-10.

[15] NIST, FIPS PUB 46-3, Federal Information Processing Standards Publication, Data Encryption Standard (DES), October 1999.

[16] ISO/IEC, International Standard 9797-1, Information Technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, Edition 2, 2011-03.

[17] SOG-IS Crypto Working Group, SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.3, February 2023.

[18] CCMB, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1, revision 5, April 2017.

[19] CCMB, Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, revision 5, April 2017.

[20] CCMB, Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version 3.1, revision 5, April 2017.

[21] CCMB, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, version 3.1, revision 5, April 2017.

[22] BSI, Common Criteria Protection Profile, BSI-CC-PP-0055, Machine Readable Travel Document with„ICAO Application", Basic Access Control, Version 1.10, March 2009.

[23] NIST, FIPS PUB 197, Federal Information Processing Standards Publication, Advanced Encryption Standard (AES), November 2001.

[24] BSI, Common Criteria Protection Profile, BSI-CC-PP-0056-V2-2012, Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2, December 2012.

[25] ISO/IEC, International Standard 7816-2, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimensions and location of the contacts, Edition 2, 2007-10.

[26] Bundesamt für Sicherheit in der Informationstechnik, AIS 31: Funcrtionality Classes and Evaluation Methodology for Physical Random Number Generators, Version 1, 25.09.2001.

[27] Infineon, IFX_CCI_00002Dh,IFX_CCI_000039h,IFX_CCI_00003Ah, IFX_CCI_000044h,IFX_CCI_000045h,IFX_CCI_000046h,IFX_CCI_000047h,IFX_CCI_000048h,IFX_CCI_000049h,IFX_CCI_00004Ah,IFX_CCI_00004Bh,IFX_CCI_00004Ch,IFX_CCI_00004Dh,IFX_CCI_00004Eh T11 Security Target Lite, v6.5, 2024-08-20.

[28] Infineon, 32-bit Security Controller - V11, Security Guidelines, v1.00-2976, 2023-06-19.

[29] Infineon, 32-bit Security Controller - V11, Hardware Reference Manual, V6.2, 2020-12-21.

[30] BSI, BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, January 2014.

[31] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.

[32] Network Working Group, RFC3369, Cryptographic Message Syntax (CMS), August 2002.

[33] ISO/IEC, International Standard 14443-3, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision, Edition 4, 2018-07.

[34] ISO/IEC, International Standard 14443-4, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol, Edition 4, 2018-06.

[35] MKLotus-OS User Manual, V1.4.

[36] MK.QT.IT.13 Composite OS Production procedure, Version 01.

A. Platform identification

A.1. Identification of integrated circuits

The integrated circuits on which the TOE is based are the secure microcontrollers IFX_CCI_000039h with firmware 80.306.16.0, including HSL v3.52.9708, UMSLC lib v01.30.0564, NRG SW 05.03.4097, SCL v2.15.000 and ACL v3.35.001.

The IC family received a Common Criteria certification at the EAL6 assurance level augmented with ALC_FLR.1 with certification ID:

- BSI-DSZ-CC-1107-V5-2024

The certificate of these integrated circuits is valid and up-to-date.