COMMON CRITERIA SECURITY TARGET LITE

Machine Readable Travel Document – Extended Access Control – CC IDeal Pass

Reference : *SSE-0000078622-01*

Date : *2010-03-24*

Sagem Orga
SAFRAN Group

TABLE OF CONTENTS

List of tables

List of figures

1 INTRODUCTION

1.1 SECURITY TARGET AND TOE REFERENCE

ST reference :

Title : MACHINE READABLE TRAVEL DOCUMENT – EXTENDED ACCESS CONTROL – CC IDEAL PASS

Version : 1

Security target identifier : SSE-0000078622

TOE reference :

Chip identifier ： SB23YR48 revision B

TOE Identifier   IDEAL/ST23YR48/1.5

Administration guidance : 0000074722 - IDeal - AGD - Pre-Personalization Manual

0000074723 - IDeal - AGD - Personalization Manual

User guidance : 0000074862 - IDeal - AGD - ICAO User Manual

CC compliance :

Version ： 3.1

Assurance level : EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

Chip certificate reference : DCSSI-2010/02

Protection Profile   BSI-CC-PP-0056, VERSION 1.10 [R5]

1.2 GENERAL OVERVIEW OF THE TARGET OF EVALUATION (TOE)

1.2.1 TOE type

The *Target of Evaluation* (TOE) is a chip programmed according to the *Logical Data Structure* (LDS) [R9] (i.e. the MRTD's chip) and providing the advanced security methods Extended Access Control (EAC), chip authentication as defined in [R10] and/or Active Authentication as defined in the Technical reports of "ICAO Doc 9303" [R9] in addition to the *Basic Access Control*[1]. The MRTD's chip allows the *authenticity* of the *travel document* and the identity of its holder to be checked during a border control, with the support of an inspection system.

The MRTD's chips are intended to be inserted into the cover page of traditional passport booklets. They can be integrated into modules, inlay or datapage. The final product can be a passport, a plastic card etc…

The Chip Authentication prevents data traces described in [R9] informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps:

---

[1] This BAC feature is not covered by the current ST

– the inspection system communicates by means of secure messaging established by Basic Access Control,

– the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object,

– the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and

– the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys).

The Chip Authentication requires collaboration of the TOE and the TOE environment.

1.2.2 Usage and major security features of the TOE

The MRTD's chip enables:

– protection of *integrity* of the holder's stored data: issuing state or organization, travel document number, expiration date, holder's name, nationality, birth date, sex, holder's face portrait, other optional data, additional biometric data and several other pieces of data for managing the security of the document,

– authentication between the travel document holder and the inspection system prior to any border control by the Basic Access Control mechanism[2],

– protection of integrity and confidentiality of data read by secure messaging,

– authentication of the genuine chip by the Active Authentication mechanism (optional),

– strong authentication of the chip and the inspection system prior to any biometric data retrieval by the Extended Access Control mechanism.

In addition to the protection provided by the chip, 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 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)[R9]. These security measures include the binding of the MRTD's chip to the passport book.

The details of these features are specified in [R9] and [R10].

---

[2] This BAC feature is not covered by the current ST but will be evaluated in another ST, see §3.3.3.

1.3 TOE DESCRIPTION

1.3.1 TOE Boundary

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) [R9] and providing Basic Access Control and Extended Access Control according to the ICAO Doc 9303 [R9] and BSI TR-03110 [R10], respectively. The TOE may also provide Active Authentication according to [R9].

The TOE boundary encompasses:

– The ICAO application

– The Operating System

– The ST embedded crypto library : NesLib V3.0

– The ST chip

The TOE does not allow any additional applets loading during its operational use.

1.3.2 TOE architecture

The TOE is embedding two applications:

– AIP Application, compliant with [R21], which performs the pre-personalization and the personalization operations of the CC IDeal Pass. This application is not accessible once in Operational Use phase.

– The ICAO/EAC application, which is compliant with [R9]. The ICAO application may be instantiated several times.

The TOE does not allow any additional applets loading during its operational use.

The architecture of the CC IDeal Pass is given in Figure 1.
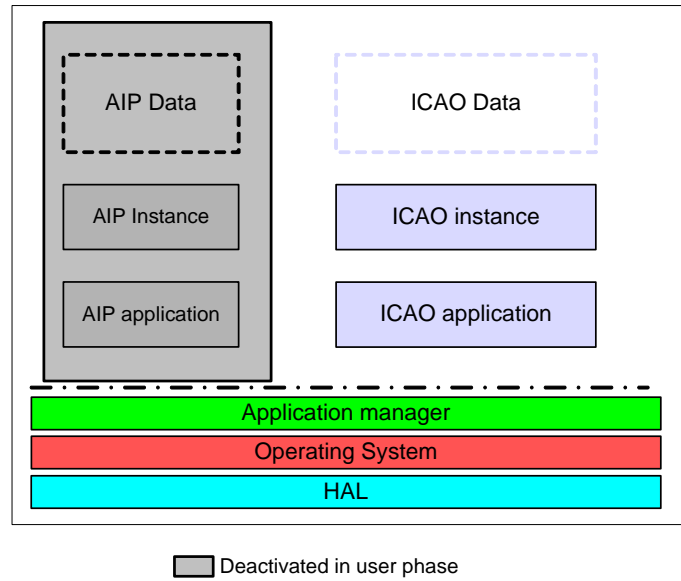
Figure 1: Architecture of the CC IDeal Pass

1.3.3   TOE life cycle

The product's life cycle is organised as follows:

	Machine Readable Travel Document – Extended Access Control – CC IDeal Pass	Ref. : SSE-0000078622-01 Page 9/83

Sagem Orga SAFRAN Group
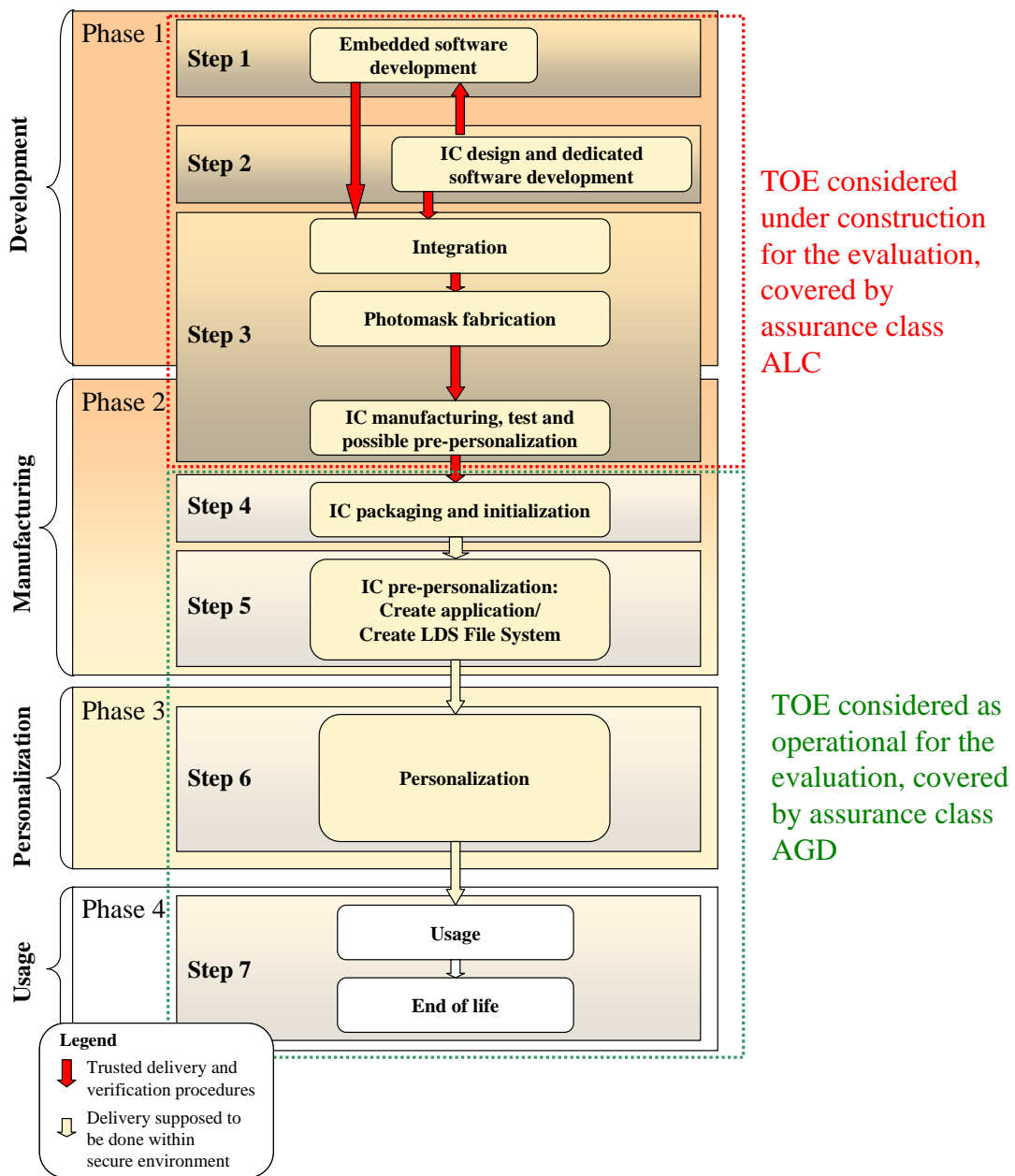
Figure 2 : TOE life cycle

This figure represents two views of the life-cycle:

1. an "end-user" view made of 4 phases, focusing on the main logical phases as defined in a protection profile like [R6]:

   a. Development phase: IC design, and embedded software development;

   b. Manufacturing phase: from IC manufacturing to booklet manufacturing, including patch loading, application creation and pre-personalization (loading the authentication key for the personalization agent);

   c. Personalization phase: loading of all data related to the MRTD holder;

d. Operational use phase: MRTD used by the traveler at the border control. 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.

2. a business view made of 7 steps, focusing more on the different trades and actors involved in smartcard business, and commonly used in protection profile related to smartcard such as [R7]. For example, the company in charge of IC manufacturing may be different from the one in charge of IC packaging, as well as from the one in charge of packaging, initialisation, pre-personalization, not considering all other actors involved in this phase: antenna supplier, booklet supplier. The definition of the content of each step and the associated supply chain vary from one provider to another and the picture is just indicative.

Referring to the life-cycle, the **evaluated product** is the product that comes out of the IC manufacturing, test and possible pre-personalization operations (**step 3**).

At this step, the product is already self-protected before delivery to step 4 and all steps after.

2 CONFORMANCE CLAIMS

2.1 CONFORMANCE WITH THE COMMON CRITERIA

This Security Target claims conformance to:

Part 1 of the Common Criteria, Version 3.1, Release 1, dated September 2006 (see [R1])

– Part 2 of the Common Criteria, Version 3.1, Release 2, dated September 2007 (see [R2]),

– Part 3 of the Common Criteria, Version 3.1, Release 2, dated September 2007 (see [R3]),

as follows

– Part 2 extended,

– Part 3 conformant.

2.2 CONFORMANCE WITH AN ASSURANCE PACKAGE

The level of assurance targeted by this Security Target is EAL5, augmented by the following components defined in CC part 3 [R3]:

– ALC_DVS.2,

– AVA_VAN.5.

2.3 CONFORMANCE WITH A PROTECTION PROFILE

2.3.1 Protection Profile reference

This Security Target claims strict conformance to the Protection Profile MRTD EAC [R5].

2.3.2 Protection Profile Refinements

No specific refinement was performed to the Protection Profile MRTD EAC [R5].

2.3.3 Protection Profile Additions

The following asset which is optional the PP MRTD EAC [R5] has been added explicitly:

➢ *Active Authentication Private Key*

This additional asset is marked in italics in this ST.

The following assumptions have been added to the PP MRTD EAC [R5]:

➢ *A_Pers_Agent_Active_Auth*
➢ *A_Insp_Sys_Active_Auth*

These additional assumptions are marked in italics in this ST.

The following objective has been added to the PP MRTD EAC [R5]:

➢ *OT.Active_Auth_Proof*

This additional objective is marked in italics in this ST.

The following objectives for the environment have been added to the PP MRTD EAC [R5]:

> *OE.Active_Auth_Key_MRTD*
> *OE.Exam_MRTD_Active_Auth*

These additional objectives for the environment are marked in italics in this ST.

The following requirements have been added to the PP MRTD EAC [R5]:

> *FCS_COP.1/SIG_GEN*
> *FIA_API.1/AAP*
> *FMT_MTD.1/AAPK*

Additional requirements are marked in italics in this ST.

Assignments of the following requirements have been augmented compared to those of the PP MRTD EAC [R5]:

> FMT_MTD.1/KEY_READ
> FPT_EMSEC.1

Augmentations are marked in italics inside the SFRs.

2.3.4 Application notes

Application notes from the PP MRTD EAC [R5] have been copied in this ST when relevant.

Moreover, application notes dedicated to the TOE described in this ST have been stated in addition to the application notes of the PP MRTD EAC [R5]. Those additional application notes should be marked in italics.

2.3.5 Protection Profile Claims rationale

The differences between this Security Target security objectives and requirements and those of PP MRTD EAC [R5], to which conformance is claimed, have been identified and justified in chapter 4 and in 6. They have been recalled in the previous section.

The TOE type defined in this security target is exactly the same than the one defined in the PP MRTD EAC [R5]: an IC with embedded software, and the MRTD application conformant to ICAO [R9] and EAC [R10].

In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the PP MRTD EAC [R5].

The security problem definition presented in chapter 3 clearly shows the additions to the security problem statement of the PP MRTD EAC [R5].

The security objectives rationale presented in chapter 4.4 clearly identifies modifications and additions made to the rationale presented in the PP MRTD EAC [R5].

All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness has been argued in the rationale sections of the present document.

2.4   CONFORMANCE WITH THE CC SUPPORTING DOCUMENTS

This security target address a smartcard TOE and therefore, the associated evaluation shall be performed in compliance with all CC mandatory supporting documents related to smartcard evaluations:

2.4.1   Application of Attack Potential to Smartcards

This document [R11] shall be used instead of the CEM [R4] when calculating the attack potential of the successful attack performed during AVA_VAN analysis. This document impacts only the vulnerability analysis performed by the ITSEF, and is not detailed here.

2.4.2   Composite product evaluation for Smartcards and similar devices

This document [R12] shall be used in addition to the CC part 3 [R3] and to the CEM [R4]. This document specifies the additional information to be provided by a developer, and the additional checks to be performed by the ITSEF when performing a "composite evaluation". This is the case for the current TOE as the underlying IC SB23YR48 revision B is already evaluated and certified under the reference: 2010/02. Therefore, the following additional assurance requirements apply for this TOE:

– ASE_COMP.1 for the security target ;
– ALC_COMP.1 for the life cycle support ;
– ADV_COMP.1 for the development activity ;
– ATE_COMP.1 for the tests activity ;
– AVA_COMP.1 for the vulnerability assessment.

3 SECURITY PROBLEM DEFINITION

3.1 ASSETS

The assets to be protected by the TOE include the following User Data on the MRTD's chip. The codes of the assets are the one used in the document [R9] part 1, volume 2, section III:

– EF.DG1: document data (type, issuing state or organization, document number, date of expiry) and holder's *biographical data* (name, nationality, date of birth, sex),

– Sensitivity: integrity,

– EF.DG2: Sensitive biometric *reference data* – face,

– Sensitivity: integrity,

– EF.DG3 : Sensitive biometric reference data - Fingerprints,

– Sensitivity: confidentiality, integrity,

– EF.DG4: Sensitive biometric reference data – Iris,

– Sensitivity: confidentiality, integrity,

– EF.DG5: Displayed Portrait,

– Sensitivity: integrity,

– EF.DG6 to EF.DG16: optional fields and additional holder and document data (among which Active the Authentication Public Key in EF.DG15 and the Chip Authentication Public Key in EF.DG14),

– Sensitivity: integrity.

The assets to be protected by the TOE include the following security data embedded on the MRTD's chip. The codes of the assets are the one used in the document [R9] part 1, volume 2, section III and [R10] appendix A.3.2.4

– EF.COM: Common Data Elements, containing the version information and tag list,

– Sensitivity: integrity,

– EF.SOD: Document Security Object, containing data integrity and authenticity information,

– Sensitivity: integrity,

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. This means that all assets used for that purpose (active authentication private key KPr_{AA}, chip authentication private key SK_{PICC}…) have to be protected in terms of confidentiality and integrity.

Due to interoperability reasons the 'ICAO Doc 9303' [R9] requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG16 and files EF.COM, EF.SOD. Therefore, considering the intrinsic resistance of BAC mechanism, these data shall be protected at a high level (AVA_VAN.5) in terms of integrity only.

3.2 SUBJECTS

The following individuals and IT systems have access to the TOE:

Manufacturer

"Manufacturer" is the generic term for the IC Manufacturer producing the integrated circuit as well as for the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing (step 3 to step 5). In this Security Target, the TOE does not distinguish between the users "IC Manufacturer" and the "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:

–   establishing the identity of the holder for the biographic data in the MRTD,

–   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),

–   writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability,

–   writing the initial TSF data and

–   signing the Document Security Object defined in [R9].

Country Verifying Certification Authority

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

Document Verifier

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

Terminal

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

Inspection system (IS)

A technical system used by the border control officer of the *receiving State*:

– examining an MRTD presented by the traveler and verifying its authenticity,

– verifying the traveler as the MRTD holder.

The **Basic** Inspection **System** (BIS):

– contains a terminal for the communication with the MRTD's chip,

– implements the terminals part of the Basic Access Control Mechanism,

– gets the authorization to read the logical MRTD under the Basic Access Control by optically 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 in addition the Chip Authentication Mechanism.

The **Extended** Inspection **System** (EIS) in addition to the General Inspection System:

– implements the Terminal Authentication Protocol,

– 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 by 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.

3.3 THREATS

3.3.1 Attacker

Threats may occur as a result of a threat agent trying:

– to manipulate the logical MRTD without authorization,

– to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4),

– to forge a genuine MRTD.

Application note 1: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

3.3.2 Attack potential

Individuals performing attacks have a **high** attack potential. They correspond to malicious persons possessing the skills of an expert.

3.3.3 Threats not included

An attacker trying to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD) is not considered by this Security Target since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys. These threats are covered by [R6] through the threats T.CHIP_ID and T.Skimming. The same hold for the confidentiality of the user data EF.DG1, EF.DG2, EF.DG5 to EF.DG16 and of the security data EF.SOD and EF.COM.

3.3.4 Threats relative to the TOE in operation

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

T.Read_Sensitive_Data   Read the sensitive biometric reference data

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

The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [R6]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.

T.Forgery   Forgery of data on MRTD's chip

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to 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 data* of finger read from the logical MRTD of a traveler into an other MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another chip.

T.Counterfeit   MRTD's chip

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

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

The TOE shall also avert the threats as specified below:

T.Abuse-Func   **Abuse of Functionality**

An attacker may use functions of the TOE which shall not be used in "TOE operational Use" phase in order

- to manipulate User Data,
- to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or
- 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.

T.Information_Leakage   **Information Leakage from MRTD's chip**

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Phys-Tamper   **Physical Tampering**

An attacker may perform physical probing of the MRTD's chip in order

- to disclose TSF Data, or
- to disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD's chip in order to

- modify security features or functions of the MRTD's chip,
- modify security functions of the MRTD's chip Embedded Software,

    –   modify User Data or,

    –   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.

T.Malfunction   **Malfunction due to Environmental Stress**

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to

    –   deactivate or modify security features or functions of the TOE or

    –   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.

3.4   ORGANISATIONAL SECURITY POLICIES (OSP)

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

P.BAC-PP   **Fulfilment of the Basic Access Control Protection Profile**

The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the 'ICAO Doc 9303' [R9] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [R6] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

Application note 2: The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [R9] is addressed by the [R6] (cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG3 and EF.DG4 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [R6]). The TOE shall protect the sensitive biometric reference data in EF.DG3 and EF.DG4 against attacks with high attack potential. Due to the different resistance the protection of EF.DG3 and EF.DG4 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG2 and

EF.DG5 to EF.DG16 are addressed separated security target, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates.

P.Sensitive_Data   **Privacy of sensitive biometric reference data**

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the MRTD holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the MRTD is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The MRTD's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip authentication.

P.Manufact   **Manufacturing of the MRTD's chip**

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

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

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

3.5   ASSUMPTIONS

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

3.5.1   Assumptions for the manufacturing and personalization environment

A.MRTD_Manufact   **MRTD manufacturing on step 4 to 6**

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

A.MRTD_Delivery   **MRTD delivery during step 4 to 6**

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

– Procedures shall ensure protection of TOE material/information under delivery and storage.

– Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.

– Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent   **Personalization of the MRTD's chip**

The Personalization Agent ensures the correctness of

– the logical MRTD with respect to the MRTD holder,

– the Document Basic Access Keys,

– the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and

– the Document Signer Public Key Certificate (if stored on the MRTD's chip).

The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A_Pers_Agent_Active_Auth   Personalization of the MRTD's chip including Active Authentication

The Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

3.5.2   Assumptions for the operational environment

A.Insp_Sys   **Inspection Systems for global interoperability**

The Inspection System is used by the border control officer of the receiving State

– Examining an MRTD presented by the traveler and verifying its authenticity and

– verifying the traveler as MRTD holder.

The Basic Inspection System for *global interoperability*

– includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and

– implements the terminal part of the Basic Access Control [R9].

The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the *Passive* Authentication to verify the logical MRTD. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System

– supports the Terminal Authentication Protocol and

– is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

A_Insp_Sys_Active_Auth   ***Inspection Systems for global interoperability supporting Active Authentication***

The Extended Inspection System in addition may also support the terminal part of the Active Authentication Protocol.

A.Signature_PKI   **PKI for Passive Authentication**

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distributes the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer

– generates the Document Signer Key Pair,

– hands over the Document Signer Public Key to the CA for certification,

– keeps the Document Signer Private Key secret and

– uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs.

The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

A.Auth_PKI   **PKI for Inspection Systems**

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

4 SECURITY OBJECTIVES

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

4.1 SECURITY OBJECTIVES FOR THE TOE

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

OT.AC_Pers   **Access Control for Personalization of logical MRTD**

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [R9] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Application note 3: The OT.AC_Pers implies that

–   the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,
–   the Personalization Agents may :
    - add (fill) data into the LDS data groups not written yet, and
    - update and sign the Document Security Object accordingly.

The support for adding data in the "Operational Use" phase is optional.

OT.Data_Int   **Integrity of personal data**

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

OT.Sens_Data_Conf   **Confidentiality of sensitive biometric reference data**

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended inspection systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the *certificate chain* to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

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 Authentication key*(s).

OT.Chip_Auth_Proof   Proof of MRTD's chip authenticity

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [R10]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

Application note 4: The OT.Chip_Auth_Proof implies the MRTD's chip to have

– a unique identity as given by the MRTD's Document number,
– a secret to prove its identity by knowledge i.e. a private authentication key as TSF data.

The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by

– the Chip Authentication Public Key (EF.DG14) in the LDS [R9] and
– the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

OT.Active_Auth_Proof   Proof of MRTD's chip authenticity by Active Authentication

The TOE may support the Extended Inspection System to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [R9].

The following TOE security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

OT.Prot_Abuse-Func   Protection against Abuse of Functionality

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to

– disclose critical User Data,
– manipulate critical User Data of the IC Embedded Software,
– manipulate Soft-coded IC Embedded Software or
– bypass, deactivate, change or explore security features or functions of the TOE.

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

OT.Prot_Inf_Leak   Protection against Information Leakage

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

– by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and

– by forcing a malfunction of the TOE and/or

– by a physical manipulation of the TOE.

Application note 5: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper   Protection against Physical Tampering

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

– measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or

– measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

– manipulation of the hardware and its security features, as well as

– controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

OT.Prot_Malfunction   Protection against Malfunctions

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

Application note 6: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE's internals.

4.2   SECURITY OBJECTIVES FOR THE DEVELOPMENT AND PRODUCTION ENVIRONMENT

OE.MRTD_Manufact   Protection of the MRTD Manufacturing

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

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

OE.MRTD_ Delivery   Protection of the MRTD delivery

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

– non-disclosure of any security relevant information,

– identification of the element under delivery,

– meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),

– physical protection to prevent external damage,

– secure storage and handling procedures (including rejected TOE's),

– traceability of TOE during delivery including the following parameters:

  • origin and shipment details,

  • reception, reception acknowledgement,

  • location material/information.

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

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

4.3   SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Issuing State or Organization

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

OE.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

– establish the correct identity of the holder and create biographical data for the MRTD,

– 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

– personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

Sagem Orga
SAFRAN Group

Machine Readable Travel Document –
Extended Access Control – CC IDeal Pass

Ref. : SSE-0000078622-01

Page 27/83

OE.Pass_Auth_Sign   Authentication of logical MRTD by Signature

The issuing State or Organization must

– generate a cryptographic secure Country Signing CA Key Pair,

– ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and

– 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

– generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys,

– sign Document Security Objects of genuine MRTD in a secure operational environment only and

– distribute the Certificate of the Document Signer Public Key to receiving States and Organizations.

The digital signature in the Document Security Object EF.SOD relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [R9].

OE.Auth_Key_MRTD   MRTD Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to

– generate the MRTD's Chip Authentication Key Pair,

– sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and

– support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data   Authorization for Use of Sensitive Biometric Reference data

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

OE.BAC_PP   Fulfillment of the Basic Access Control Protection Profile

It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [R6]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

Receiving State or Organization

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

OE.Exam_MRTD   Examination of the MRTD passport book

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability

–   includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and

–   implements the terminal part of the Basic Access Control [R9].

Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

OE.Active_Auth_Key_MRTD   MRTD Active Authentication Key

The issuing State or Organization may establish the necessary public key infrastructure in order to :

–   generate the MRTD's Active Authentication Key Pair,

–   sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and

support inspection systems of receiving States or Organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of he Document Security Object.*OE.Exam_MRTD_Active_Auth   Examination of the MRTD passport book using Active Authentication*

During examination of the MRTD presented by the traveler, the Extended Inspection Systems may perform the Active Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

OE.Passive_Auth_Verif   *Verification* by Passive Authentication

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

OE.Prot_Logical_MRTD   Protection of data 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 inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

Application note 7: The figure 2.1 in [R10] supposes that the GIS and the EIS follow the order

– running the Basic Access Control Protocol,
– reading and verifying only those parts of the logical MRTD that are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key),
– running the Chip Authentication Protocol, and
– reading and verifying the less-sensitive data of the logical MRTD after Chip Authentication.

The supposed sequence has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. The inspection system will prevent additionally eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. Note that reading the less-sensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this PP. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

OE.Ext_Insp_Systems   Authorization of Extended Inspection Systems

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

4.4   RATIONALE

4.4.1   Coverage matrix

The following table provides an overview for security objectives coverage:

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	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.Auth_Key_MRTD	OE.Active_Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.BAC-PP	OE.Exam_MRTD	OE.Exam_MRTD_Active_Auth	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System
T.Read_Sensitive_Data			X														X						X
T.Forgery	X	X							X					X					X		X		
T.Counterfeit					X	X									X	X			X	X			
T.Abuse-Func							X																
T.Information_Leakage								X															
T.Phys-tamper									X														
T.Malfunction										X													
P.BAC-PP																		X					
P.Sensitive_Data			X														X						X
P.Manufact				X																			
P.Personalization	X			X									X										
A.MRTD_Manufact											X												
A.MRTD_Delivery												X											
A.Pers_Agent													X										
A.Pers_Agent_Active_Auth													X										
A.Insp_Sys																			X			X	
A.Insp_Sys_Active_Auth																				X			
A.Signature_PKI														X							X		
A.Auth_PKI																	X						X

Table 1: Security problem definition / Security objectives

4.4.2   Coverage of threats in the operational environment

T.Read_Sensitive_Data

The OSP **P.Sensitive_Data** "Privacy of sensitive biometric reference data" is fulfilled and the threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the TOE-objective **OT.Sens_Data_Conf** "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by **OE.Authoriz_Sens_Data** "Authorization for use of

sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems".

T.Forgery

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".

T.Counterfeit

The threat **T.Counterfeit** "MRTD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of MRTD's chip authentication" using a authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_MRTD** "MRTD Authentication Key". According to **OE.Exam_MRTD** "Examination of the MRTD passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip.

This threat is also thwarted by chip identification and authenticity proof required by ***OT.Active_Auth_Proof*** "Proof of MRTD's chip authentication by Active Authentication" using a authentication key pair to be generated by the issuing State or Organization. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by ***OE.Active_Auth_Key_MRTD*** "MRTD Active Authentication Key". According to ***OE.Exam_MRTD_Active_Auth*** "Examination of the MRTD passport book using Active Authentication", the Extended Inspection system may perform the Active Authentication Protocol to verify the authenticity of the MRTD's chip.

T.Abuse-Func

The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks of misusing MRTD's functionality to disable or bypass the TSFs. The security objective for the TOE **OT.Prot_Abuse-Func** "Protection against abuse of functionality" ensures that the usage of functions which may not be used in the

"operational Use" phase is effectively prevented. Therefore attacks intending to abuse functionality in order to disclose or manipulate critical (User) Data or to affect the TOE in such a way that security features or TOE's functions may be bypassed, deactivated, changed or explored shall be effectively countered.

T.Information_Leakage, T.Phys-Tamper, T.Malfunction

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".

4.4.3   Coverage of organisational security policies

P.BAC-PP

The OSP **P.BAC-PP** is directly addressed by the **OE.BAC-PP**.

P.Sensitive_Data

See "T.Read_Sensitive_Data".

P.Manufact

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 Prepersonalization Data as being fulfilled by **OT.Identification**.

P.Personalization

The OSP **P.Personalization** "Personalization of the MRTD by issuing State or Organization only" addresses the:

– 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

– the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD".

Note the manufacturer equips the TOE with the Personalization Agent Authentication key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

4.4.4 Coverage of assumptions

A.MRTD_Manufact

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.

A.MRTD_ Delivery

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.

A.Pers_Agent

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.

A.Pers_Agent_Active_Auth

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

A.Insp_Sys

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

A.Insp_Sys_Active_Auth

The examination of the MRTD passport book addressed by the assumption *A.Insp_Sys_Active_Auth* "Inspection Systems for global interoperability supporting Active Authentication" is covered by the security objectives for the TOE environment *OE.Exam_MRTD_Active_Auth* "Examination of the MRTD passport book using Active Authentication" which requires the Extended Inspection Systems to implement and to perform the Active Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

A.Signature_PKI

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

A.Auth_PKI

The assumption **A.Auth_PKI** "PKI for Inspection Systems" is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data" requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organizations only. The Document Verifier of the receiving State is required by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organization has to establish the necessary public key infrastructure.

5 EXTENDED COMPONENTS DEFINITION

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [R7], other components are defined in protection profile MRTD EAC [R5].

5.1 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 behaviour

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

Component levelling

```
┌─────────────────────────────────┐            ┌─────┐
│  FAU_SAS Audit data storage      │────────────│  1  │
└─────────────────────────────────┘            └─────┘
```
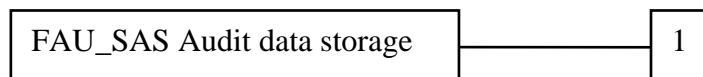
FAU_SAS.1   Requires the TOE to provide the possibility to store audit data.

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.

5.2 DEFINITION OF THE FAMILY FCS_RND

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

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

FCS_RND Generation of random numbers

Family behaviour

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

Component leveling:

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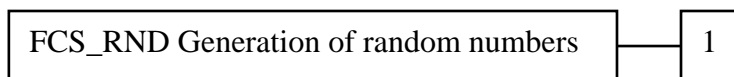
FCS_RND.1   Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1   Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3 DEFINITION OF THE FAMILY FIA_API

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

	Machine Readable Travel Document – Extended Access Control – CC IDeal Pass	Ref. : SSE-0000078622-01 Page 37/83

![Sagem Orga SAFRAN Group logo]

for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Application note 8: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behaviour

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

Component levelling

FIA_API.1   Authentication Proof of Identity.

Management: FIA_API.1

               The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

               There are no actions defined to be auditable.

FIA_API.1   Authentication Proof of Identity.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1   The TSF shall provide a [assignment: *authentication mecha*nism] to prove the identity of the [assignment: *authorized user or role*].

5.4   DEFINITION OF THE FAMILY FMT_LIM

The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other

class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

FMT_LIM Limited capabilities and availability

Family behaviour

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

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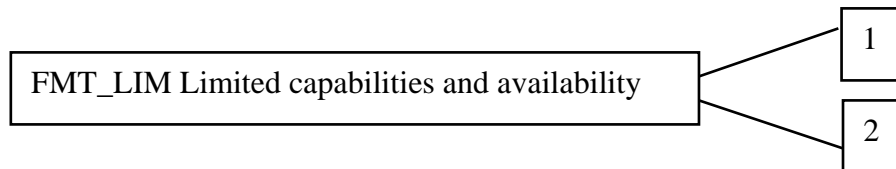
FMT_LIM.1   Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

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 and implemented in a manner that limits its 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 its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].

Application note 9: 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 policy. This also allows that

– 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

– 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 requirements shall enforce the policy.

5.5   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 requirement 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 [R2].

The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

FPT_EMSEC TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling

```
┌────────────────────────────────────┐     ┌─────┐
│  FPT_EMSEC TOE emanation            │─────│  1  │
└────────────────────────────────────┘     └─────┘
```
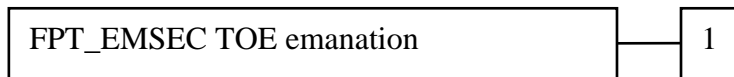
FPT_EMSEC.1   TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6 IT SECURITY REQUIREMENTS

6.1 INTRODUCTION

This section identifies the security functional requirements for the TOE.

Some refinement/selection/assignment operations in the SFRs are determined in the PP MRTD EAC [R5], some are let with unspecified values. Assignments made by the PP MRTD EAC [R5] authors are marked as bold text, while assignments made by the ST author are marked as bold text and in italics.

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

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

Name	Data
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute *Current Date* as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [R10] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.

Name	Data
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Active Authentication Key Pair	The Active Authentication Key Pair (KPrAA, KPuAA) is used for Active Authentication Protocol: RSA according to ISO9796-2 Digital Signature scheme 1
Active Authentication Public Key	The Active Authentication Public Key (KPuAA) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Active Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Active Authentication Private Key	The Active Authentication Private Key (KPrAA) is used by the TOE to authenticate itself as authentic MRTD's chip using the Active Authentication protocol. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

Table 2: Overview of the keys and certificates

Application note 10: The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization.

6.2   TOE SECURITY FUNCTIONAL REQUIREMENTS

6.2.1   Class FAU Security Audit

The TOE shall meet the requirement « Audit storage (FAU_SAS.1) » as specified below (Common Criteria Part 2 extended).

FAU_SAS.1   Audit storage

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.
Assignment	Authorized users : **the Manufacturer** List of Audit Information : **the IC Identification Data**

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

6.2.2   Class Cryptographic Support (FCS)

6.2.2.1   CRYPTOGRAPHIC KEY MANAGEMENT (FCS_CKM)

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

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

FCS_CKM.1.1 / DH	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment : cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	Cryptographic key generation algorithm : **See Table 3.** Cryptographic key sizes : **See Table 3.** List of standards : **[R10], Annex A.1**

Cryptographic key generation algorithm	Cryptographic key size	Standard

Diffie-Hellman Protocol (PKCS#3)	*1024, 1536 and 2048 bits*	*[R10], Annex A.1 and [R13]*
ECDH (ISO 15946)	*192, 224 and 256 bits*	*[R10], Annex A.1 and [R14]*

Table 3: Cryptographic key generation methods

Application note 12: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [R10], sec. 3.1 and Annex A.1. This protocol is based on the Diffie-Hellman Protocol compliant to PKCS#3 (i.e. a modulo arithmetic based cryptographic algorithm, cf. [R13]) or on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf.[R10], Annex A.1, [R15] and [R14] for details). The shared secret value is used to derive the 112 bit Triple-DES key for encryption and the 112 bit Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [R9] normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC.

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

FCS_CKM.4   **Cryptographic key destruction – MRTD**

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment : cryptographic key destruction method]** that meets the following : **[assignment : list of standards]**.
Assignment	Cryptographic key destruction method : ***Overwriting of data*** List of standards : ***none***

Application note 13: The TOE shall destroy the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

6.2.2.2   CRYPTOGRAPHIC OPERATION (FCS_COP)

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

FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation by MRTD

FCS_COP.1.1 / SHA	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment :**

	cryptographic key sizes] that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **hashing** Cryptographic algorithm : ***SHA-1, SHA224, SHA-256*** Cryptographic key sizes : **none** List of standards : ***FIPS 180-2***

Application note 14: The Chip Authentication Protocol use SHA-1 hash mechanism (cf. [R10], normative appendix 5, A5.1 and Annex A.2.2 for details). The TOE implements additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol (cf. [R10], Annex A.2.2 for details).

FCS_COP.1/SYM Cryptographic operation – Symetric Encryption / Decryption

FCS_COP.1.1 / SYM	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **secure messaging – encryption and decryption** Cryptographic algorithm : ***Triple-DES in CBC mode*** Cryptographic key sizes : ***112 bits*** List of standards : ***FIPS 46-3 [R16] and*** [R10]

Application note 15: This SFR requires the TOE to implement the secure messaging with encryption for the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol according to the FCS_CKM.1/DH. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

FCS_COP.1/MAC Cryptographic operation –MAC

FCS_COP.1.1 / MAC	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.

Assignment	List of cryptographic operations : **secure messaging – message authentication code**
	Cryptographic algorithm : *Retail MAC*
	Cryptographic key sizes : *112 bits*
	List of standards : **[R10]**

Application note 16: 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 as part of the Chip Authentication Protocol according to the FCS_CKM.1/DH.

FCS_COP.1/SIG_VER   **Cryptographic operation – Signature verification by MRTD**

FCS_COP.1.1 / SIG_VER	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : **digital signature verification**
	Cryptographic algorithm : *See Table 4*
	Cryptographic key sizes : *See Table 4*
	List of standards : *See Table 4*

Cryptographic algorithm	Cryptographic key size	Standard
RSA	*1024, 1536, 2048, 3072 and 4096 bits*	*RSASSA-PKCS1-v1_5*
ECDSA	*192, 224, 256, 384 and 521 bits*	*ISO15946 ECDSA*

Table 4: Cryptographic signature verification methods

Application note 17: The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

FCS_COP.1/SIG_GEN   *Cryptographic operation – Signature generation by MRTD*

FCS_COP.1.1 / SIG_GEN	The TSF shall perform **[assignment : list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment : cryptographic algorithm]** and cryptographic key sizes **[assignment : cryptographic key sizes]** that meet the following : **[assignment : list of standards]**.
Assignment	List of cryptographic operations : ***digital signature generation*** Cryptographic algorithm : ***RSA*** Cryptographic key sizes : ***1024, 1536, 2048 and 3072 bits*** List of standards : ***ISO9796-2 Digital Signature scheme 1***

Application note 18*: The signature generation is used during the Active Authentication Protocol.*

6.2.2.3   RANDOM NUMBER GENERATION (FCS_RND)

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

FCS_RND.1   Quality metric for random numbers

FCS_RND.1.1	The TSF shall a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].
Assignment	A defined quality metric: ***AIS31 Class P2 quality metric***

Application note 19: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

6.2.3   Class FIA Identification and Authentication

The following table provides an overview on the authentication mechanisms used:

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/MRTD
Chip Authentication Protocol	FIA_API.1/CAP, FIA_UAU.5/MRTD FIA_UAU.6/MRTD
Active Authentication Protocol	*FIA_API.1/CAP*
Terminal Authentication Protocol	FIA_UAU.5/MRTD

Table 5: Overview on authentication SFR

Note the Chip Authentication Protocol as defined in this Security target[3] includes:

– the BAC authentication protocol as defined in 'ICAO Doc 9303' [R9] in order to gain access to the Chip Authentication Public Key in EF.DG14,

– the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol,

– the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The BAC mechanism does not provide a security function on its own. The Chip Authentication Protocol may be used independent of the Terminal Authentication Protocol. But if the Terminal Authentication Protocol is used the terminal shall use the same public key as presented during the Chip Authentication Protocol.

6.2.3.1 USER IDENTIFICATION (FIA_UID)

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

FIA_UID.1 Timing of identification

FIA_UID.1.1	The TSF shall allow **[assignment : list of TSF-mediated actions]** on behalf of the user to be performed before the user is identified.
Assignment	List of TSF-mediated actions: **(1) to establish the communication channel,** **(2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,** **(3) to carry out the Chip Authentication Protocol**
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 20: In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the Document Basic Access Keys, the Chip authentication data and Terminal Authentication

---

[3]   The BAC Authentication Protocol is included here as part of the Chip Authentication Protocol because it is a necessary condition to read the EF.DG14.

Reference Data are written into the TOE. The Basic Inspection System (cf. [R6]) 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 run the BAC Authentication Protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol (i.e. the BAC mechanism is not seen as an independent mechanism in this PP, it is a mandatory part within the chip authentication protocol, and thus noted here for reasons of completeness). After successful authentication of the chip the terminal may identify itself as

– Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or

– if necessary and available by symmetric authentication as Personalization Agent (using the Personalization Agent Authentication Key).

6.2.3.2 USER AUTHENTICATION (FIA_UAU)

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

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow **[assignment : list of TSF-mediated actions]** on behalf of the user to be performed before the user is authenticated.
Assignment	List of TSF-mediated actions: **(1) to established the communication channel,** **(2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,** **(3) to identify themselves by selection of the authentication key,** **(4) to carry out the Chip Authentication Protocol**
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.

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

FIA_UAU.4 Single-use authentication mechanism – Single-use authentication of the Terminal by the TOE

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to **[assignment : identified authentication mechanism(s)]**.

Assignment	Identified authentication mechanism(s):
	(1) Terminal Authentication Protocol, **(2) Authentication Mechanism based on *Triple-DES***

Application note 21: 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.

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

FIA_UAU.5   Multiple authentication mechanisms

FIA_UAU.5.1	The TSF shall provide **[assignment : list of multiple authentication mechanisms]** to support user authentication.
Assignment	List of multiple authentication mechanisms: **(1) Terminal Authentication Protocol,** **(2) Secure messaging in MAC-ENC mode,** **(3) Symmetric Authentication Mechanism based on *Triple-DES***
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the **[assignment : rules describing how the multiple authentication mechanisms provide authentication]**.
Assignment	Rules describing how the multiple authentication mechanisms provide authentication: **(1) The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with Personalization Agent Key *during personalization phase of the product's life cycle (phase 3),*** **(2) After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism,** **(3) The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism.**

Application note 22: Depending on the authentication methods used the Personalization Agent holds a key for the Symmetric Authentication Mechanism.

The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use

Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal.

The authentication of the personalization agent is only possible during phase 3 of the life-cycle, using symetric authentication mechanism.

This can be considered as a refinement of the SFR FIA_UAU.5 of the PP.

However, this refinement is more restrictive than the PP, increase the level off security and therefore, do not impact the conformity to the PP.

The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

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

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

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions **[assignment : list of conditions under which re-authentication is required]**.
Assignment	List of conditions under which re-authentication is required: (1) **Each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.**

Application note 23: The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [R9] include 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 accept only those commands received from the previously authenticated user.

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

FIA_API.1/CAP   Authentication Proof of Identity - MRTD

FIA_API.1.1 / CAP	The TSF shall provide a **[assignment : authentication mechanism]** to prove the identity of the **[assignment : authorized user or rule]**.
Assignment	Authentication mechanism: **Chip Authentication Protocol according to [R10]** Authorized user or rule : **TOE**

Application note 24: This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [R10]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [R9], normative appendix 5, A5.1. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AAP   *Authentication Proof of Identity – MRTD using Active Authentication*

FIA_API.1.1 / AAP	The TSF shall provide a **[assignment : authentication mechanism]** to prove the identity of the **[assignment : authorized user or rule]**.
Assignment	Authentication mechanism: *Active Authentication Protocol according to [R9]* Authorized user or rule : *TOE*

Application note 25: The TOE may implement the Active Authentication Mechanism specified in [5]. The terminal randomly generates a challenge, then the MRTD chip digitally signs this challenge using RSA and finally the terminal verifies that the returned signature is correct.

6.2.4   Class FDP User Data Protection

6.2.4.1   ACCESS CONTROL POLICY (FDP_ACC)

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

FDP_ACC.1   Subset access control

FDP_ACC.1.1	The TSF shall enforce the **[assignment : access control SFP]** on **[assignment: list of subjects, objects and operations among subjects and objects covered by the SFP]**.
Assignment	Access control SFP : **Access Control SFP** List of subject, objects and operations among subjects and objects covered

	by the SFP : **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD**

6.2.4.2 ACCESS CONTROL FUNCTIONS (FDP_ACF)

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

FDP_ACF.1   **Security attribute based access control**

FDP_ACF.1.1	The TSF shall enforce the **[assignment : access control SFP]** to objects based on the following : **[assignment : list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]**.

Assignment	Access control SFP : **Access Control SFP**
	
	List of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes:
	
	  (1) Subjects :
	      a) Personalization Agent,
	      b) Extended Inspection System
	      c) Terminal,
	
	  (2) Objects :
	      d) data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
	      e) data EF.DG3 and EF.DG4 of the logical MRTD,
	      f) Data in EF.COM,
	      g) Data in EF.SOD.
	
	  Security attributes :
	      h) Authentication status of terminals,
	      i) Terminal authorization.

FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment : rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]**.
Assignment	Rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects : **(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 Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization is allowed to read the data in EF.DG3 of the logical MRTD,
	(3) the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization is allowed to read the data in EF.DG4 of the logical MRTD.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following sensitive rules: **[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]**.
Assignment	Rules, based on security attributes, that explicitly authorize access of subjects to objects : **none**
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rule: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.
Assignment	Rules, based on security attributes, that explicitly deny access of subjects to objects : (1) **A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,** (2) **A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,** (3) **A terminal authenticated as DV is not allowed to read data in the EF.DG3,** (4) **A terminal authenticated as DV is not allowed to read data in the EF.DG4,** (5) **Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,** (6) **Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD.**

Application note 26: The relative certificate holder authorization encoded in the CVCA of the inspection system is defined in [R10], Annex A.5.1, table A.8. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the

Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

Application note 27: Note the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG16 of the logical MRTD. According to P.BAC-PP this security features of the MRTD are not subject of this Security Target.

6.2.4.3   INTER-TSF USER DATA CONFIDENTIALITY TRANSFER PROTECTION (FDP_UCT)

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

FDP_UCT.1   **Basic data exchange confidentiality - MRTD**

FDP_UCT.1.1	The TSF shall enforce the **[assignment : access control SFP(s) and/or information flow control SFP(s)]** to be able to **[selection : transmit, receive]** user data in a manner protected from unauthorized disclosure **after Chip Authentication**.
Assignment	Access control SFP(s) and/or information flow control SFP(s): **Access Control SFP**
Selection	**Transmit and receive**

6.2.4.4   INTER-TSF USER DATA INTEGRITY TRANSFER PROTECTION (FDP_UIT)

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

FDP_UIT.1   **Basic data exchange integrity - MRTD**

FDP_UIT.1.1	The TSF shall enforce the **[assignment : access control SFP(s) and/or information flow control SFP(s)]** to be able to **[selection : transmit, receive]** user data in a manner protected from **[selection : modification, deletion, insertion, replay]** errors **after Chip Authentication**.
Assignment	Access control SFP(s) and/or information flow control SFP(s): **Access Control SFP**
Selection	**transmit and receive** **modification, deletion, insertion and replay**
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether **[selection : modification, deletion, insertion, replay]** has occurred **after**

	Chip Authentication.
Selection	modification, deletion, insertion and replay

Refinement: Note that the Access Control SFP (cf. FDP_ACF.1.2) allows the Extended Inspection System (as of [R9] and [R6]) to access the data EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD. Nevertheless there is explicitly no rule for preventing access to these data. More over their data integrity (cf. FDP_UIT.1) and confidentiality (cf. FDP_UCT.1) is ensured by the BAC mechanism being addressed and covered by [R6]. The fact that the BAC mechanism is not part of the Security Target in hand is addressed by the refinement "after Chip Authentication".

Application note 28: 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 Chip Authentication to the General Inspection System. The authentication mechanism as part of Basic Access Control Mechanism and the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

6.2.5 Class FMT Security Management

Application note 29: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

6.2.5.1 SPECIFICATION OF MANAGEMENT FUNCTIONS (FMT_SMF)

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

FMT_SMF.1   **Specification of Management Functions**

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions **[assignment : list of security management functions to be provided by the TSF]**.

Assignment	List of security management functions to be provided by the TSF :
	   (1) Initialization,
	   (2) Personalization,
	   (3) Configuration.

Application note 30: The configuration capabilities of the TOE are available during the pre-personalization (initialization) and personalization phases.

6.2.5.2 SECURITY MANAGEMENT ROLES (FMT_SMR)

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

FMT_SMR.1   **Security roles**

FMT_SMR.1.1	The TSF shall maintain the roles **[assignment : the authorized identified roles]**.

Assignment	The authorized identified roles:
	
	    (1) Manufacturer,
	
	    (2) Personalization Agent,
	
	    (3) Country Verifying Certification Authority,
	
	    (4) Document Verifier,
	
	    (5) Domestic Extended Inspection System,
	
	    (6) Foreign Extended Inspection System.

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

Application note 31: Note that the MRTD also maintains the role Basic Inspection System due to a direct consequence of P.BAC-PP resp. OE.BAC-PP. Nevertheless this role is not explicitly listed in FMT_SMR.1.1, above since the TSF cannot maintain the role with respect to the assumed high attack potential due to the known weaknesses of the Document Basic Access Keys.

6.2.5.3 LIMITED CAPABILITIES AND AVAILABILITY (FMT_LIM)

Application note 32: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

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

FMT_LIM.1   **Limited capabilities**

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]**.
Assignment	Limited capability and availability policy :

	Deploying Test Features after TOE Delivery does not allow: (1) **User Data to be manipulated,** (2) **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,** (3) **TSF data to be disclosed or manipulated** (4) **software to be reconstructed and** (5) **substantial information about construction of TSF to be gathered which may enable other attacks.**

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

FMT_LIM.2   **Limited availability**

FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capability (FMT_LIM.1)" the following policy is enforced: **[assignment : Limited capability and availability policy]**.
Assignment	Limited capability and availability policy : **Deploying Test Features after TOE Delivery does not allow,** (1) **User Data to be manipulated,** (2) **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,** (3) **TSF data to be disclosed or manipulated** (4) **software to be reconstructed and** (5) **substantial information about construction of TSF to be gathered which may enable other attacks.**

Application note 33: 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 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

6.2.5.4   MANAGEMENT OF TSF DATA (FMT_MTD)

Application note 34: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

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

FMT_MTD.1.1 / INI_ENA	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **write**
Assignment	List of TSF data : **Initialization Data and Pre-Personalization Data** The authorized identified roles : **the Manufacturer**

Application note 35: 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 Authentication Key.

FMT_MTD.1/INI_DIS   **Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization data**

FMT_MTD.1.1 / INI_DIS	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **disable read access for users to**
Assignment	List of TSF data : **Initialization Data** The authorized identified roles : **the Personalization Agent**

Application note 36: According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by

– allowing to write these data only once and
– 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 MRTD Manufacturer will write the Pre-personalization Data.

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

FMT_MTD.1.1 / CVCA_INI	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **write**
Assignment	List of TSF data : **(1) initial Country Verifying Certification Authority Public Key,** **(2) initial Country Verifying Certification Authority Certificate,** **(3) initial Current Date.** The authorized identified roles : ***Personalization Agent***

Application note 37: The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or prepersonalization phase or by the Personalization Agent (cf. [R10], sec. 2.2.6). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifier Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

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

FMT_MTD.1.1 / CVCA_UPD	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **update**
Assignment	List of TSF data : **(1) Country Verifying Certification Authority Public Key,** **(2) Country Verifying Certification Authority Certificate,** The authorized identified roles : **Country Verifying Certification Authority**

Application note 38: The Country Verifier Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifier CA Link-Certificates (cf. [R10], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifier CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [R10], sec. 2.2.3 and 2.2.4).

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

FMT_MTD.1.1 / DATE	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	**Modify**
Assignment	List of TSF data : **Current date** The authorized identified roles : (1) **Country Verifying Certification Authority,** (2) **Document Verifier,** (3) **Domestic Extended Inspection System.**

Application note 39: The authorized roles are identified in their certificate (cf. [R10], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [R10], annex A.3.3, for details).

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

FMT_MTD.1.1 / KEY_WRITE	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **write**
Assignment	List of TSF data : **Document Basic Access Keys** The authorized identified roles : **the Personalization Agent**

Application note 40: The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.

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

FMT_MTD.1.1 / CAPK	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations: [selection: create, load]]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : *load*
Assignment	List of TSF data : **Chip authentication Private Key**

	The authorized identified roles : *Personalization Agent*

Application note 41: The component FMT_MTD.1/CAPK is refined by

– selecting the "load" operation.

The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.

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

FMT_MTD.1.1 / CAPK	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations: [selection: create, load]]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : *load*
Assignment	List of TSF data : *Active authentication Private Key* The authorized identified roles : *Personalization Agent*

Application note 42: The component FMT_MTD.1/AAPK is refined by defining a selection between "create" and "load" for the assignment "other operations". "Load" means here that the Active Authentication Private Key is generated securely outside the TOE and written into the TOE memory. "Create" means here that the Active Authentication Private Key is generated by the TOE itself.

FMT_MTD.1/KEY_READ   **Management of TSF data – Key Read**

FMT_MTD.1.1 / KEY_READ	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorized identified roles]**.
Selection	Assignment : **read**
Assignment	List of TSF data : **(1) Document Basic Access Keys,** **(2) Chip Authentication Private Key,** **(3) Personalization Agent Keys,** *(4) Active Authentication Private Key* The authorized identified roles : **none**

The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below (Common Criteria Part 2).

FMT_MTD.3 **Secure TSF data**

FMT_MTD.3.1	The TSF shall ensure that only secure values **of the certification chain** are accepted for TSF data **of the Terminal Authentication Protocol and the Access Control**.
Refinement	**Refinement: The certificate chain is valid if and only if:** (1) **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,** (2) **the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,** (3) **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.** **The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.** **The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.**

Application note 43: The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.

6.2.6 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.

6.2.6.1 TOE EMANATION (FPT_EMSEC)

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

FPT_EMSEC.1   TOE Emanation

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]**.
Assignment	Types of emissions : *side channel* Specified limits : *limits of the state of the art* List of types of TSF data : **Personalization Agent Authentication Keys and Chip Authentication Private Key** *and Active Authentication Private Key* List of types of user data : *none*
FPT_EMSEC.1.2	The TSF shall ensure **[assignment: types of users]** are unable to use the following interface **[assignment: types of connection]** to gain access to **[assignment: list of types of TSF data]** and **[assignment: list of types of user data]**.
Assignment	Types of users : **any users** Types of connection : **smart card circuit contacts** List of types of TSF data : **Personalization Agent Authentication Keys and Chip Authentication Private Key** *and Active Authentication Private Key* List of types of user data : *none*

Application note 44: 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 may provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples

of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

6.2.6.2 FAIL SECURE (FPT_FLS)

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

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

FPT_FLS.1 **Failure with preservation of secure state**

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur : **[assignment: list of types of failures in the TSF]**.
Assignment	List of types of failures in the TSF : **(1) Exposure to out-of-range operating conditions where therefore a malfunction could occur, (2) Failure detected by TSF according to FPT_TST.1**

6.2.6.3 TSF PHYSICAL PROTECTION (FPT_PHP)

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

FPT_PHP.3 **Resistance to physical attack**

FPT_PHP.3.1	The TSF shall resist **[assignment: physical tampering scenarios]** to the **[assignment: list of TSF devices/elements]** by responding automatically such that the SFRs are always enforced.
Assignment	Physical tampering scenarios : **physical manipulation and physical probing** List of TSF devices/elements : **TSF**

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

– assuming that there might be an attack at any time and

– countermeasures are provided at any time.

6.2.6.4 TSF SELF TEST (FPT_TST)

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

FPT_TST.1   **TSF testing**

FPT_TST.1.1	The TSF shall run a suite of self tests **[selection : during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment : conditions under which self test should occur]]** to demonstrate the correct operation of the TSF.
Selection	*During initial start-up*
FPT_TST.2.1	The TSF shall provide authorized users with the capability to verify the integrity of **TSF data**.
FPT_TST.3.1	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Application note 46: the FPT_TST.1 requirement describes requirement for the Personalization and Operational Use phases. Self-tests during the Manufacturing phase are described in the chip security target and have been evaluated during the chip evaluation.

6.3   SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The TOE shall be evaluated according to Evaluation Assurance Level 5 (EAL5)

And augmented by the following components:

– ALC_DVS.2,
– AVA_VAN.5.

Application note 47: The TOE shall protect the assets against high attack potential under the assumption that the inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol (OE.Prot_Logical_MRTD). Otherwise the confidentiality of the standard data shall be protected against attacker with at least Enhanced-Basic attack potential (AVA_VAN.3).

7 TOE SUMMARY SPECIFICATION

7.1 SECURITY FUNCTIONS DESCRIPTION

7.1.1 Chip security functions

The following functionalities of the product are directly addressed by the chip. The complete list the chip security functionality can be check in the chip Security Target [R8].

TSF_INTEGRITY

This security functionality is responsible for :

– correcting single bit fails upon a read operation on each NVM byte,

– verifying valid CPU usage,

– checking integrity loss when accessing NVM, ROM or RAM,

– providing a sign engine to check code and/or data integrity loss,

– monitoring various manifestations of fault injection attempts,

– providing a security timeout feature (watchdog timer),

– providing the embedded software developer with the traceability information of the TOE.

TSF_PHYSICAL_TAMPERING

This security functionality ensures that:

– The TOE detects clock and voltage supply operating changes by the environment,

– The TOE detects attempts to violate its physical integrity, and glitch attacks,

– The TOE is always clocked with shape and timing within specified operating conditions.

TSF_SECURITY_ADMIN

This security functionality ensures the management of the following security violation attempts:

– Incorrect CPU usage,

– Integrity loss in NVM, ROM or RAM

– Code signature alarm,

– Fault injection attempt,

– access attempt to unavailable or reserved memory areas,

– MPU errors,

– Clock and voltage supply operating changes,

– TOE physical integrity abuse.

TSF_UNOBSERVABILITY

This security functionality prevents the disclosure of user data and of TSF data when it is transmitted between separate parts of the TOE (the different memories, the CPU and other functional units of the TOE such as a cryptographic co-processor are seen as separated parts of the TOE) :

This functionality provides additional support mechanisms to the SICESW developer contributing to avoid information leakage.

TSF_SYM_CRYPTO

This security functionality provides DES and TDES data encryption / decryption capability, in order to compute Message Authentication code (MAC) or the encrypted data.

TSF_ASYM_CRYPTO

This security functionality provides:

– RSA verification (encryption) with an RSA modulo up to 4096 bits,
– RSA signature (decryption) using or not using the Chinese Remainder Theorem (CRT), with an RSA modulo up to 4096 bits,
– RSA private and public keys computation with an RSA modulo up to 4096 bits,
– Prime number generation up to 3200 bits, with Rabin-Miller primality tests.

This functionality implements also the following standard hash function:

– SHA-1 hash function chaining blocks of 512 bits to get a 160 bits result,
– SHA-224 hash function chaining blocks of 512 bits to get a 224-bit result,
– SHA-256 hash function chaining blocks of 512 bits to get a 256-bit result.

This security function provides also the following basic functions for Elliptic Curves Cryptography over prime fields:

– general point addition,
– point expansion and compression,
– public scalar multiplication,
– private scalar multiplication.

TSF_ALEAS

This security functionality provides a hardware Random Number Generator (RNG) to support security operations performed by cryptographic applications. The RNG complies with the AIS31 Class P2 quality metric.

7.1.2   Low level security functions

TSF_PHYS

This security function provides protection mechanism of the TOE towards observation and physical tampering, such as random delay and desynchronization capability. This security function may call TSF_UNOBSERVABILITY.

7.1.3 Operating system security functions

TSF_ACCESS

This security function manages the access to objects (files, directories, data and secrets) stored in E²PROM.

TSF_INIT

This security performs TOE testing and initialization after each reset of the TOE.

TSF_MEMORY

This security function manages E²PROM and RAM erasure.

TSF_OTP

This security function manages the OTP area in E²PROM and in particular the « life cycle parameter », enforcing non-reversibility of the life cycle.

TSF_CPLC

This security function manages the CPLC area. The CPLC area contains Manufacturing data, pre-personalization data and Personalization data. The CPLC area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Read access to the CPLC area is allowed during Personalization phase. During Operational Use phase, the CPLC area read access is only possible after BAC authentication.

TSF_CHECK

This security function performs data integrity checks.

TSF_TEST

This security function performs self-tests at start-up and monitors code integrity during execution.

TSF_AUDIT

This security function reacts when a fault or an anomaly is detected.

7.1.4 Application manager security functions

TSF_GESTION

This security function manages:

– Management of the secure state of the TOE.

– Application selection.

– Application separation.

7.1.5 Application security functions

TSF_SECRET

This security function ensures secure management of secret such as cryptographic keys.

TSF_CRYPTO

This security function performs high level cryptographic operations.

TSF_TERM_AUTH

TSF_TERM_AUTH performs the Terminal Authentication to authenticate the terminal.

TSF_TDES_AUTH

TSF_TDES_AUTH performs an authentication mechanism based on TDES.

TSF_CHIP_AUTH

This security function manages the capability of the TOE to authenticate itself to the terminal using the Chip Authentication Protocol as defined in [R10].

TSF_ACTIVE_AUTH

This security function manages the capability of the TOE to authenticate itself to the terminal using the Active Authentication Protocol as defined in [R9].

8 DEFINITIONS, GLOSSARY AND ACRONYMS

8.1 ACRONYMS

BIS   Basic Inspection System

CC   Common Criteria

EAL   Evaluation Assurance Level

EF   Elementary File

EIS   Extended Inspection System

GIS   General Inspection System

IAS   Identité Authentification Signature

ICAO   International Civil Aviation Organization

ICCSN   Integrated Circuit Card Serial Number

IT   Information Technology

ITSEF   Information Technology Security Evaluation Facility

JCRE   Java Card Runtime Environment

JVM   Java Virtual Machine

MF   Master File

MRTD   Machine Readable Travel Document

n.a.   Not applicable

OSP   Organizational security policy

PP   Protection Profile

RAD   Reference Authentication Data

RNG   Random Number Generator

SAR   Security assurance requirements

SDO   Signed Data Object

SFP   Security Function Policy

SFR   Security functional requirement

ST   Security Target

TOE   Target of Evaluation

TSF   TOE Security Functions

TSP   TOE Security Policy

VAD   Verification Authentication Data

VGP   Visa Global Platform

8.2   CONVENTIONS USED

The following list shows the roots used for the various elements.

Root   Elements described by this root
T.   Threats relative to the TOE and the TOE operational environment
OSP.   Organisational security policy
A.   Assumption
OT.   Security objectives for the TOE
OE.   Security objectives for the operational environment

8.3   DEFINITIONS

Active Authentication

Security mechanism defined in [5] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of Organization.

Application note

Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Audit records

Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.

Authenticity

Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.

Basic Access Control (BAC)

Security mechanism defined in [R9]] 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 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. [R9].

Biometric reference data

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

Certificate chain

Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (selfsigned certificate).

Chip

An integrated circuit and its embedded software as it come out of the IC manufacturing step.

Counterfeit

An unauthorized copy or reproduction of a genuine security document made by whatever means. [R9]

Country Signing CA Certificate (CC$_{SCA}$)

Certificate of the Country Signing Certification Authority Public Key (K$_{PuCSCA}$) issued by Country Signing Certification Authority stored in the inspection system.

Country Verifying Certification Authority

The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing State or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.

Current date

The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.

CVCA link Certificate

Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.

Document Basic Access Key Derivation Algorithm

The [R9], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

Document Basic Access Keys

Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [R9]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.

Document Security Object (SOD)

A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [R9]

Document Verifier

Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations.

Eavesdropper

A threat agent with 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. [R9]

Extended Access Control

Security mechanism identified in [R9] 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 Authentication Private Key and to get write and read access to the logical MRTD and TSF data.

Extended Inspection System

A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Extended Inspection System (EIS)

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

Forgery

Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [R9]

General Inspection System

A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.

Global Interoperability

The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [R9]

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.

Initialisation 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. [R9]

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 built on 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). [R9]

Issuing State

The Country issuing the MRTD. [R9]

Logical Data Structure (LDS)

The collection of groupings of Data Elements stored in the optional capacity expansion technology [R9]. The capacity expansion technology used is the MRTD's chip.

Logical MRTD

Data of the MRTD holder stored according to the Logical Data Structure [R9] as specified by ICAO on the MRTD's chip. It presents readable data including (but not limited to)

(1) personal data of the MRTD holder

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

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

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

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

(6) EF.COM and EF.SOD

Logical travel document

Data stored according to the Logical Data Structure as specified by ICAO in the integrated circuit including (but not limited to)

(1) data contained in the machine-readable zone (mandatory),

(2) digitized photographic image (mandatory) and

(3) fingerprint image(s) and/or iris image(s) (optional).

Machine readable travel document (MRTD)

Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [R9]

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. [R9]

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 [R9]
– the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13 and EF.DG16, EF.COM and EF.SOD) and
– the TSF Data including the definition the authentication data but except
– the authentication data itself.

MRTD Basic Access Control

Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.

MRTD holder

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

MRTD's Chip

A chip programmed according to the Logical Data Structure as specified by [R9] and ready for personalisation.

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 Step 1 and embedded into the MRTD's chip in Step 3 of the TOE life-cycle.

Optional biometric reference data

Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.

Patch

Additional executable code loaded in EEPROM of a chip after IC manufacturing step, in order to fix a bug or a problem encountered with the embedded software execution. A patch can fix

- a functional problem, eg. missing arguments in an APDU, bad timing in the protocol management…
- a security problem: typically, a patch that corrects a weakness discovered on a security function.

Note that a patch that fixes a functional problem can have an impact on the security of the chip if it affects the behaviour of a security function.

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". [R9]

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 Authentication Key

Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent.

Physical travel document

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

(1) biographical data,

(2) data of the machine-readable zone,

(3) photographic image and

(4) other data.

Pre-personalization Data

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

Pre-personalized MRTD's chip

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

Receiving State

The Country to which the Traveler is applying for entry. [R9]

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.

Secure messaging in encrypted mode

Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.

Skimming

Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.

Security Target (ST)

Reference document for the TOE evaluation: the certificate awarded by the DCSSI will attest conformity of the product and its documentation with the (functional and assurance) requirements formulated in the security target.

Target of Evaluation (TOE)

The product to be evaluated and its associated documentation.

Terminal Authorization

Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.

TOE Security Functionality (TSF)

A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP)

Set of rules stipulating how to manage, protect and distribute assets within a TOE.

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. [R9]

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 [R1]).

Unpersonalized MRTD

The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalisation 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 [R1]).

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. [R9]

Verification data

Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

9 REFERENCE AND APPLICABLE DOCUMENTS

9.1 REFERENCE DOCUMENTS

Designation	Reference	Title	Revision	Date
Common Criteria				
[R1]	CCMB-2006-09-001	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model	Version 3.1, Revision 1	September 2006
[R2]	CCMB-2007-09-002	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components	Version 3.1, Revision 2	September 2007
[R3]	CCMB-2007-09-003	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components	Version 3.1, Revision 2	September 2007
[R4]	CCMB-2007-09-004	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology	Version 3.1, Revision 2	September 2007
Protection Profiles and Security Target				
[R5]	BSI-PP-0056	Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application" - Extended Access Control	Version 1.10	March 2009
[R6]	BSI-PP-0055	Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control	version 1.10	March 2009
[R7]	BSI-PP-0002-2001	Protection Profile, Security IC Platform Protection Profile. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik).	Version 1.0	July 2001
[R8]	SMD_Sx23YRxx_ST_09_002	Sx23YRxxB Security Target - Public Version	Rev 02.01	February 2010
E-passport specifications				
[R9]	ICAO Doc 9303	part 1 volume 1, Sixth edition, 2006, Passports with Machine Readable Data Stored in Optical Character Recognition Format; part 1 volume 2, Sixth edition, 2006, Specifications for Electronically Enabled Passports with Biometric Identification Capability.	Sixth edition	2006

Designation	Reference	Title	Revision	Date
[R10]	TR-03110	Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)	Version 1.11	
CC supporting document				
[R11]	CCDB-2008-04-001	Supporting Document - Mandatory Technical Document - Application of Attack Potential to Smartcards	V2.5, R1	April 2008
[R12]	CCDB-2007-09-001	Supporting Document - Mandatory Technical Document - Composite product evaluation for Smartcards and similar devices	V1.0, R1	September 2007

9.2   APPLICABLE DOCUMENTS

Designation	Reference	Title	Revision	Date
Cryptography				
[R13]	PKCS#3	PKCS#3 : Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note	Version 1.4	Revised November 1, 1993
[R14]	ISO/IEC 15946	ISO/IEC 15946 : Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3 : Key establishment.		2002
[R15]		Technical Guideline :Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI		2006
[R16]	FIPS PUB 46-3	Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standards (DES), U.S. Department Of Commerce / National Institute of Standards and Technology.		Reaffirmed 1999 October 25
[R17]	ANSI X9.31	American Bankers Association, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998 - Appendix A.2.4		1998
[R18]		Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology		2002 August 1

OTHER				
[R19]		VISA global platform requirements configuration 3 – compact	v2.1.1	May 2003
[R20]		Plate-forme commune pour l'eAdministration – Spécification technique	Version 1.01	
[R21]		EMV CPS	1.0 Final	16 June 2003