jTOP v#8.05 e-Passport Lite Security Target

Emission Date	:	January 12nd, 2006
Project Name	:	COCOON
Document Type	:	Technical report
Ref./Version	:	PU-2005-RT-624/1.0
Classification	:	Public
Number of pages	:	64

LEGAL NOTICE

COPYRIGHT NOTICE

DISCLAIMER OF WARRANTY

Table of contents

Table of figures

This page has been intentionally left blank

1 Introduction

This chapter identifies the document and the referenced material, presents its general structure, and introduces key notions and notation conventions used throughout the document. It also gives the precise identification of the Security Target Lite it embodies.

1.1 Identification of the Lite Security Target

Author	Trusted Logic SA
Address	5, rue du Bailliage 78000 Versailles - France
Title	jTOP v#8.05 e-Passport Lite Security Target
Registration Number	DCSSI-2005/52
Keywords	e-Passport; ICAO; MRTD; Java Card; GlobalPlatform; jTOP

1.2 Identification of the TOE

Commercial name	jTOP e-Passport
TOE version	8.05
LDS applet version	LDS version 1.7 with PKI version 1.1, 29/04/2005
IC identifier	SLE66CLX641P
IC development code	M1522
IC design step	A11

1.3 Revisions and Comments

Version	Issue date	Comments
1.0	January 12nd, 2006	First public version.

1.4 Document Overview

This document defines the security objectives and requirements for Trusted Logic's implementation of jTOP e-Passport based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) for the constitution of Machine Readable Travel Documents (MRTD).

ICAO Machine Readable Travel Documents are made of a contactless smart card containing the personal data of its owner, embedded in a paper passport book. The *jTOP e-Passport* is the software layer of the smart card. It consists in a Java Card application, called LDS, running on top of a closed runtime environment compliant with Java Card 2.1.1 and VISA GlobalPlatform 2.0.1' – Configuration 2 standards that forbids enlarging or restricting the set of applications installed on the card, at any time during its life-cycle.

This security target is a composite ST, composed of this one and the security target of the smartcard IC platform SLE66CLX641P [ICST], produced by Infineon Technologies AG.

The administration of the smart card is performed by the GlobalPlatform Issuer Security Domain (ISD), which is the on-card representative of the Issuing State. The LDS application offers personalization services to Issuing States, responsible for enrolling personal data into the passport and delivering the passport to its owner, and traveler's identification services to Receiving States through the baseline MRTD **Basic Access Control Authentication** and **Active Authentication** mechanisms.

This document is a lite version of the full jTOP v#8.05 e-Passport Security Target. The whole rationales, descriptions concerning threat scenarii and most of the application notes have been removed from the full version of the document. In some of the Security Functional Requirements (SFR), the phrase "***[proprietary information removed]***" replaces sensitive information contained in the full version of the Security Target..

1.5 CC Conformance

This Security Target is:

- CC version 2.2 conformant
- Part 2 extended
- Part 3 conformant
- EAL4 augmented

1.6 Typographic Conventions

A "T", like in T.INSTALL, prefixes the threats. Similarly, an "O" prefixes the security objectives for the TOE, etc. The instances of the security functional requirements in [CC2] are identified by the name of the instantiated component, followed by a suffix, like in FDP_ACC.1/MRTD.

1.7 Associated Documents

The following documents are referenced in this document.

[CC1] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*. Version 2.2. January 2004. CCIMB-2004-01-001.

[CC2] *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements*. Version 2.2. January 2004. CCIMB-2004-01-002.

[CC3] *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements*. Version 2.2. January 2004. CCIMB-2004-01-003.

[CEM] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*. Version 2.2. January 2004. CCIMB-2004-01-004.

[CSRS] *GlobalPlatform Card Security Requirements Specification*, Version 1.0, May 2003.

[GPCS] *GlobalPlatfrom Card Specification,* Version 2.0.1', April 2000.

[ICST] *SLE66CLX641P Security Target*. Infineon Technologies AG – Evaluation Document.

[VCPG] *VISA GlobalPlatform Card Production Guide*, Version 2.04, September 2002.

[VGP] *VISA GlobalPlatfrom 2.0.1' Card Implementation Requirements, Configuration 2 – Compact with PK*, Version 1.0, February 2000.

[VGPE] *VISA GlobalPlatfrom 2.0.1' Card Implementation Requirements, Configuration 2 – Compact with PK, Errata 2.0, June 2003*.

[JCVM] *Java Card 2.1.1 Virtual Machine Specification*, Sun Microsystems, Revision 1.0, May 18th 2000.

[JCRE] *Java Card 2.1.1 Runtime Environment Specification*, Sun Microsystems, Revision 1.0, May 18th 2000.

[JCAPI] *Java Card 2.1.1 Application Programming Interface*, Sun Microsystems, Revision 1.0, May 18th 2000.

[JAVASPEC]] *The Java Language Specification*. Gosling, Joy and Steele. ISBN 0-201-63451-1.

[MRTD] *PKI for Machine Readable Travel Documents offering ICC Read-Only Access*, International Civil Aviation Organization (ICAO). Version 1.1, October 1st 2004.

[MRTD-LDS] *Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies*, Revision –1.7, International Civil Aviation Organization, LDS 1.7, May 18th 2004

[MRTD-Annex] *ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS*, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[MRTD-PP] *Protection Profile - Machine Readable Travel Documents with ICAO Application*, version 0.92, T-Systems, 26th June 2004.

[MRTD-BIO] *Biometrics Deployment of Machine Readable Travel Document*, *Technical Report*, Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 1.9, ICAO TAG MRTD / NTWG, 19 May 2003.

[SSVG] *Smartcard IC Platform Protection Profile*, Version 1.0, July 2001, registered at the BSI under the reference BSI-PP-0002.

1.8 Acronyms

The following acronyms are used in this document:

Acronym	Meaning
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset
CAD	Card Acceptance Device
CAMS	Card and Application Management System
CC	Common Criteria
CCM	Card Content Management
CIN	Card Identification Number
CLA	Instruction class (of an APDU command)
CSRS	Card Security Requirements Specification
DES	Data Encryption Standard
DPA	Differential Power Analysis
EEPROM	Electrically Erasable Programmable Read Only Memory
GP	GlobalPlatform
GPCS	GlobalPlatform Card Specification
IIN	Issuer Identification Number
INS	Instruction code (of an APDU command)
ISD	Issuer Security Domain
JCSPP	Java Card System Protection Profile
jTOP	Java Trusted Open Platform
MAC	Message Authentication Code
GP	Global Platform
OPEN	Open Platform Environment
OS	Operating System
PP	Protection Profile

Acronym	Meaning
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RTE	Run Time Environment.
SCP	Secure Channel Protocol
SCSUG	Smart Card Security Users Group
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
VGP	VISA GlobalPlatform
VGPCS	VISA GlobalPLatform Card Specification

2 TOE Description

This chapter presents the general IT features of the TOE and the main security concerns.

2.1 The Target of Evaluation (TOE)

The Target of Evaluation (TOE) is the contactless smart card chip SLE66CLX641P with embedding software that transforms it into a secure e-Passport, compliant with ICAO's specifications [MRTD], [MRTD-LDS], [MRTD-Annex].

A MRTD containing the TOE is issued for international travels by a State or organization: the TOE holds at least as many personal information as the paper book, including the biographical data and the digital portrait of its owner. The rest of the section summarizes two processes: the delivery of a MRTD based on the jTOP e-Passport Security Component to its owner, under the responsibility of the Issuing State, and the use of such MRTD as identification means under the responsibility of the Traveler and the Receiving State. We refer to the ICAO documents [MRTD] and [MRTD-LDS] for a complete generic description.

2.1.1 MRTD delivery

The confidence infrastructure used to guarantee the integrity of the personal data embedded in the MRTD relies on two Signer entities: the Issuing State and the Document Signer.

The **Issuing State** generates the *Country Signing (CS) CA Key Pairs*, distributes the CS Public Key to the Receiving States and the ICAO and uses the CS Private Key to sign the Document Signer Public Key.

The **Document Signer** generates the *Document Signer (DS) Key Pairs*, distributes the DS Public Key to the Receiving States and the ICAO and uses the DS Private Keys to sign the digital personal data to be loaded into the e-Passport.

The **Personalization Agent** is in charge of building up the MRTD with the personal data of its final user and delivering it. He disposes of an unfilled MRTD (smart card with TOE, embodied in a paper book) delivered by the Manufacturer in a state that allows personalization. The Personalization Agent obtains the data from the final user, writes them down the paper book, put them in digital format and generates, on behalf of the Issuing State, the RSA *Active Authentication (AA) Key Pair*. The Document Signer signs the data composed of the digital personal data and the AA Public Key with the DS Private Key and obtains the *Security Data Object (SOD).* Then the Personalization Agent loads the digital data, the SOD and also the AA Private Key into the MRTD. On the MRTD side, the personalization process is performed by the TOE. After delivering, the TOE does reject any new personalization attempt.

Note that the MRTD data contains at least the biographical data of the owner of the passport, its digital portrait and the AA Public Key. It may also contain the certificate of the DS Public key. The Personalization Agent delivers the MRTD to its owner.

The AA Key Pair is used to prove to the Inspection System that the MRTD is genuine. The DS signature of the data is used to ensure their integrity. The next section develops these points.

Note that the Document Signer may be the Personalization Agent.

2.1.2 MRTD normal usage

The **Traveler** presents a MRTD to the Border Control Officer of the Receiving State to prove his/her identity. Only at this moment, the Border Control Officer, through the Inspection System (the terminal capable of reading the contactless MRTD), may start accessing the information contained in the MRTD.

The **Receiving State** possesses the CS Public Key and the DS Public key and distributes them to the Inspection Systems. These keys are necessary for ensuring the integrity of the data contained in the MRTD (called Passive Authentication Mechanism by the ICAO).

An **Inspection System** attempting to read a MRTD based on the TOE is meant to authenticate itself to the TOE in order to verify the traveler's identity. Indeed, the TOE grants the access to the data only to Inspection System that performs a successful Basic Access Control Authentication. Once the Inspection System has been authenticated, it reads the digital MRTD data using a trusted channel that protects the data in integrity and confidentiality, and then performs the Passive Authentication of the data. Finally, the Inspection System may perform the Active Authentication of the MRTD, using also a trusted channel, to gain confidence in the authenticity of the MRTD.

The **Basic Access Control (BAC) Authentication** requires collaboration of the TOE and the Inspection System: (i) the Inspection system reads the printed data in the passport book, (ii) it generates, from these data, the *Document Basic Access Control Keys* used to authenticate itself to the TOE, (iii) then both the TOE and the Inspection System generates the same *Basic Access Control Session Keys* used for establishing a trusted channel protected in integrity and confidentiality (iv) and, finally, the Inspection System reads the digital data and their DS signature using this trusted channel with the TOE. Note that the BAC Authentication relies on the fact that the Inspection System knows the printed passport data, which supposes that the traveler has willingly offered his passport to the Border Control Officer.

The **Passive Authentication** is an exclusive Inspection System operation. It consists in verifying the Document Signer signature on the MRTD data (i.e. the SOD), performed during personalization. Successful signature verification proves the integrity of the data stored in the MRTD and the Border Control Officer gains confidence in the Traveler's identity. Since the TOE does not participate of this mechanism, it is not in the scope of evaluation.

The **Active Authentication (AA)** requires collaboration of the TOE and the Inspection System, which authenticates the TOE through a protocol based on the Active Authentication Key Pair, using the trusted channel opened after successful Basic Access Control Authentication. The Inspection System has already read the digital data and the SOD, performed Passive Authentication and get back the AA Public Key. If Passive Authentication succeeds, the AA Public Key is authentic. The Active Authentication asks the TOE to sign a given random data with its AA Private Key, and then checks the returned signature with the AA Public Key obtained in the previous step. This mechanism ensures that the personal data of the owner of the passport was signed for this specific MRTD: the AA Public Key and the AA Private Key formed together the AA Key Pair.

2.2 TOE Architecture

The *jTOP e-Passport* consists in a Java Card application, called LDS, running on top of a closed runtime environment compliant with Java Card 2.1.1 and VISA GlobalPlatform 2.0.1' – Configuration 2 standards that includes the OPEN and the Issuer Security Domain. The code of those software components is masked on the ROM memory of the chip.

Figure 2-1 shows the components of the TOE, i.e. the colored boxes, in the framework of the whole e-passport. The next sections give a brief description of each component.

From now on, MRTD, Passport and e-Passport are synonyms: they all stand for the whole product including the chip and the software layer, embodied in a paper book. LDS application and MRTD application are also used as synonyms.

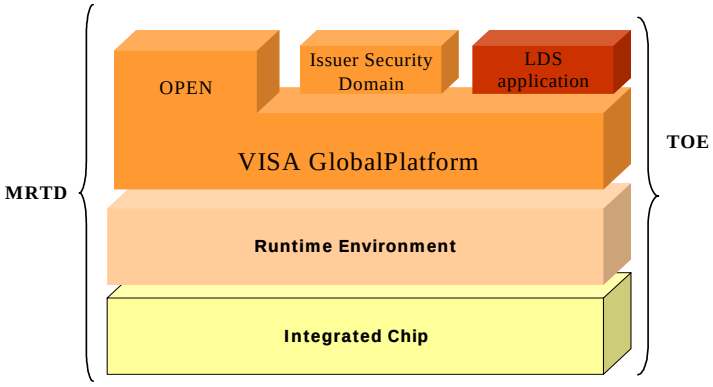

Figure 2-1: The components of the TOE

2.2.1 Integrated Circuit

- The integrated circuit is a smart card IC (SLE66CLX641P) manufactured by Infineon Technologies AG.

2.2.2 Runtime Environment

The Runtime Environment (RTE) is a generic Java Card environment capable of interpreting the bytecode of a JC application. It is compliant with the version 2.1.1 of the Java Card platform [JCRE][JCVM][JCAPI] and provides a security execution framework for the installed applications (Issuer Security Domain and LDS application in this TOE).

2.2.3 Visa Global Platform, OPEN and ISD

The VISA Global Platform (VGP) layer of the TOE is compliant with version 2.0.1' – Configuration 2 [VGP][VGPE]. It is made of the Global Platform Environment (OPEN), the VGP Application Programming Interface (VGP API) and the Issuer Security Domain (ISD).

2.2.4 LDS application

The LDS application is a JC application compliant with ICAO specifications [MRTD] and [MRTD-LDS]. The LDS application of the TOE enforces the Basic Access Control Authentication before any access to the data stored in it and offers the Inspection System the possibility to check that the MRTD is genuine through the Active Authentication Mechanism.

2.3 The TOE in the life cycle of the e-passport

The TOE's life cycle is made of four phases: Development, Manufacturing, Personalization, Operational Use that involve the participation of various users in different roles. Figure 2-2 shows the workflow of phases.

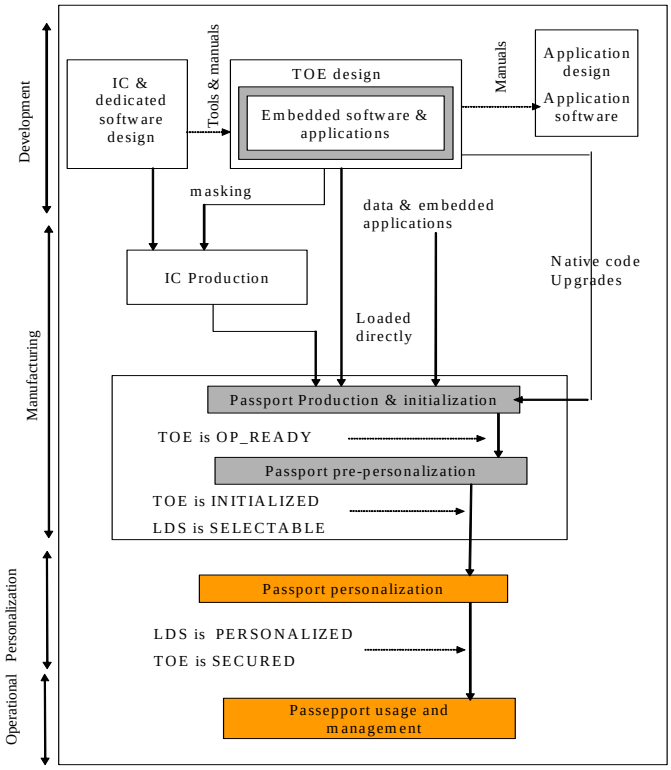

Figure 2-2: TOE's Life Cycle

2.3.1 Phase 1: Development

The IC Manufacturer develops the IC on its own. The Software Developer develops the IC Embedded Software (RTE and VGP), the LDS application and the guidance documentation associated with these components. The Software Developer uses tools and manuals provided by the IC Manufacturer and specifications of standards provided by SUN Microsystems, GlobalPlatform and ICAO..

2.3.2 Phase 2: Manufacturing

The IC Manufacturer has already developed the integrated circuit, the IC Dedicated Software and the associated guidance documentation. The IC Manufacturer produces an integrated circuit containing the Dedicated Software, the Initialization Data that corresponds to this step and the Embedded Software (TOE's components).

The IC is delivered from the IC Manufacturer to the Passport Manufacturer.

The Passport Manufacturer (i) packs the IC with hardware for the contactless interface in the passport book and (ii) writes Pre-personalization Data.

The pre-personalized MRTD is delivered from the Passport Manufacturer to the Personalization Agent.

2.3.3 Phase 3 Personalization of the TOE

The personalization of the TOE requires authentication as Personalization Agent and consists in the steps described in §2.1.1. Once the personalization is finished, the personalized MRTD is handed over to the MRTD holder for operational use. This phase is not re-entered once the MRTD reached the Operational Use phase.

2.3.4 Phase 4 Operational Use

The TOE is used embedded into a MRTD by the Traveler and the Inspection System as described in §2.1.2.

2.4 Users and Roles

The users of the TOE include people or institutions.

Manufacturer

The Manufacturer is a generic term introduced in [MRTD-PP] that includes all the actors involved in the Phase 2 (Manufacturing) of the MRTD life cycle. During this phase, the role of the Manufacturer is sequentially embodied by the Software Developer, the IC Manufacturer, the Passport Manufacturer and the Passport Enabler.

Software Developer

The Software Developer (Trusted Logic) is the organization responsible for designing and implementing the software embedded in the IC. This includes all the components of the IC Embedded Software as well as the LDS Application.

IC Manufacturer

The IC Manufacturer integrates the Embedded Software within the IC. This is usually known as the "masking" process.

Passport Manufacturer

The Passport Manufacturer integrates the masked IC with the carrier (a paper passport) in accordance with the Issuing State requirements, to produce a complete MRTD ready for delivery to the Passport Enabler.

Passport Enabler

The Passport Enabler is responsible for preparing the MRTD for the Phase 3 Personalization of the MRTD's life cycle state (passport personalization) according to the instructions of the Issuing State or Organization.

Passport Administrator

The Passport Administrator has the ultimate control of the MRTD with regard to content and life cycle management of the MRTD. During the Phase 2 of the MRTD's life cycle, this role is embodied by the Passport Enabler. Then, during the Phase 3, it is embodied by the Personalization Agent. Finally, during the Phase 4, the Passport Administrator can perform administration operations on the MRTD.

Personalization Agent

The Personalization Agent acts on the behalf of the Issuing State or Organisation to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, (iii) writing these data on the MRTD for the holder as defined for global and international and national interoperability and (iv) signing the Document Security Object defined in [MRTD].

Border Control Officer

The Border Control Officer is the person representing the Receiving State. It has access to the TOE through an Inspection System during the Operational Use phase.

General Inspection System

A General Inspection System is the role played by the Border Control Officer after successful authentication using the Basic Access Control Mechanism during the Operational Use phase.

MRTD Holder

The MRTD Holder is the rightful holder of the MRTD for whom the Issuing State personalized the MRTD.

Traveler

The Traveler is the person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

2.5 Scope of evaluation

The scope of the TOE is the masked software in the three layers of the architecture given in §2.1 in addition to the integrated circuit.

Regarding the TOE's life cycle, this Security Target only covers the orange boxes of the Figure 2-2: TOE's Life Cycle: the Personalization and the Operational Use phases. The construction of the IC and the smart card and embedding process itself are addressed in [ICST].

3 TOE security environment

3.1 Assets

The assets to be protected by the TOE include the User Data, the security TSF data of the LDS application and the security TSF data of the ISD, for the passport administration.

3.1.1 LDS Security Data

Document Basic Access Control Keys

This asset consists of two symmetric keys K_ENC and K_MAC computed from the MRZ Data (optically readable data). These keys are used by the terminal and the LDS application in the challenge-response protocol of the Basic Access Control to prove that the inspection system knows the MRZ Data (hence that the passport was willingly handed over for inspection).

Random Numbers

This asset stands for the session random numbers managed by the LDS application during the challenge-response protocols used in Basic Access Control and Active Authentication.

BAC Session Keys

This asset consists of two symmetric session keys SK_ENC computed during Basic Access Control in order to open a BAC secure channel. These keys are used by the terminal and the LDS application for secure messaging: command data is encrypted with SK_ENC and the commands carries a MAC authentication and integrity value computed with SK_MAC.

Active Authentication Private Key

This asset is the private part of the Active Authentication Key Pair used to prove that the passport is genuine.

Internal state

The internal life cycle state of the LDS application.

3.1.2 Administration Security Data

Initialization Data

This asset concerns the administration data concerning the initialization of the MRTD, like the Issuing State's identifier, Personalization Agent information, serial number of hte MRTD's chip, etc.

Administration Data

This asset consists of the data used for the personalization of the ISD, and the administration of the passport.

Application Code

The code of the LDS applet embedded into the MRTD.

Application Instances

The MRTD contains two Application instances: the Issuer Security Domain (ISD) and the LDS Application instance (or LDS Application, for short). Each application instance provides a collection of services to the users of the MRTD. The ISD provides passport administration services. The LDS Application provides different authentication services and access control to the LDS Data Groups.

GlobalPlatform Registry

Internal information about the identification, life cycle state, privileges and resources assigned to the Issuer Security Domain and the LDS applet.

3.1.3 User Data

Digital MRZ data

The digital MRZ data reflects the entire content of the visual readable MRZ data of the passport. It may be read by all inspection systems of receiving states.

Digitalized portrait of the MRTD holder

The digital portrait (encoded face image) of the MRTD holder used as biometric reference data for face authentication of the MRTD holder.

Other personal data

The MRTD contains data elements other than digital MRZ data and digitized portrait, as created by the issuing State or organization. They are personal data of the MRTD holder: displayed signature, person to be notified in case of accident, etc.

Active Authentication Public Key

This asset is the public part of the Active Authentication Key Pair used to prove that the passport is genuine.

Document Security Object

The Document Security Object (SOD) contains:

- a hash of each User Data
- the certificate of the Document Signer Public Key that serves to verify the signature of this Document Security Object. Its presence within SOD is optional, either the inspection system holds it (that is, it has been distributed by the Document Signer) or the inspection system gets it from the LDS application with the SOD.
- other optional data
- the digital signature of these elements, computed using the Document Signer Private Key, kept secret by the Document Signer.

3.2 Assumptions

This section describes the assumptions that are made regarding the TOE security environment.

3.2.1 Smartcard Embedded Software Assumptions

A.KEYS

Only the Manufacturer and the Passport Administrator know the secret keys protecting the assets on the MRTD (that is, the Document Basic Access Keys, the Active Authentication Private Key and the ISD static keys). They do not divulgate them by any means.

A.MANUFACTURING

The Passport Manufacturer ensures the quality, confidentiality and integrity of the manufacturing process as well as the disabling of all test, debug and patching mechanisms from the product once the MRTD is in the OP_READY state (at the beginning of the pre-personalization).

It is assumed that the different actors embodying the role of the Passport Manufacturer (IC Manufacturer, Passport Manufacturer and Passport Enabler) apply security procedures to maintain confidentiality and integrity of the TOE and of its manufacturing and test data up to delivery to the end-user (to prevent any possible copy, modification, retention, theft or unauthorised use). In particular, the TOE is assumed to be protected appropriately when it is delivered from one actor to the other.

A.SIGNATURE-PKI

All the Issuing State keys shall be generated, maintained, used, distributed and destroyed in a secure manner. This includes the Country Signing CA Key Pair, The Document Signer Key Pair, the Active Authentication Key Pair.

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 distributes the Country Signing CA Public Key to ICAO, all receiving State and organization in a way that protects its integrity.

The Document Signer

- o generates the Document Signer Key Pair,
- o hands over the Document Signer Public Key to the CA for certification,
- o keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs.

The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and organizations.

A.PERSONALIZATION

The Personalization Agent ensures the correctness of the User Data with respect to the MRTD holder and the integrity of the

- o Document Basic Access Keys,
- o Active Authentication Key Pair and

- o Document Signer Public Key Certificate (if stored on the Document Security Object).

The loading of data into the MRTD protects their integrity and confidentiality.

A.INSPECTION-SYSTEM

The Inspection System does not disclose User Data nor generate evidence to a third party that a specific MRTD was presented by the traveler at a certain date. Moreover, the Inspection System shall perform the passive authentication of the MRTD and use the Active Authentication Mechanism to verify the authenticity of the presented MRTD.

3.2.2 Integrated Circuit Assumptions

The scope of the TOE addressed in this Security Target has been enlarged with respect to [ICST] so as to include the embedded software. In addition to this, the part of the life cycle under evaluation has been both restricted (manufacturing of the IC is excluded) and enlarged (some of the phases after delivering of the IC are included). As a consequence, the assumptions included in [ICST] are not longer pertinent for the TOE addressed in this Security Target. Those assumptions are not relevant either because they are covered by a larger assumption included in this Security Target, or because they are discharged (represented) by a threat or a requirements included in it. In this latter case the TOE must be designed so as to counter the threat or fulfill the requirement, so there is not need to relay on an assumption.

The following assumptions from [ICST] are covered by larger ones included in this Security Target:

- A. Process-Card, which assumes that the IC is protected after the IC Manufacturer delivers it to the other actors, is covered by the larger assumption A.MANUFACTURING, which includes all the roles involved in the Phase 1 of the TOE: Software Developer, IC Manufacturer, Passport Manufacturer and Passport Enabler.

The following assumptions from [ICST] have been discharged:

- A.Resp-App, which assums that the embedded software protects the keys and other sensitive data, is discharged by the threats considered in the section General Threats.
- A.Key-Function, which assumes that the embedded software protects the cryptographic keys from information leakage, is also discharged by the threats considered in the section General Threats.
- A.Plat-Appl, which assumes the correct design of the embedded software according to requirements of IC manufacturer, is discharged by the assurance measures concerning the development of smartcard embedded software and its environment.

3.3 Threats

This section describes the threats to the assets against which specific protection within the TOE or its environment is required.

3.3.1 General Threats

T.REPLAY

The attacker may penetrate passport security through reuse of a (partially) completed operation that was previously performed by an authorized user.

A completed (or partially completed) operation may be replayed in an attempt to bypass security mechanisms or to expose security-related information. For instance, the attacker may try to send to the MRTD an APDU command that he intercepted in a previous session.

The attacker may also use authentication information that was previously delivered to him in order to disclose or modify a piece of information stored in the MRTD. For instance, the attacker may use authentication information that was once valid, but that is not longer valid, like an old cryptographic key.

All the assets are threatened.

Application note:

The following list illustrates some possible scenarios for this kind of attack:

- The attacker tries to use a previous session key in order to decrypt or falsify a message sent to the MRTD.
- The attacker tries to intercept a command containing a secret key to be loaded on the MRTD, guess the key by some means, and replay the intercepted message later on in order to set the broken key again.

T.ABUSE-FUNC

This threat concerns the abusive use of TOE functionalities. The attacker may exploit commands, which were necessary for a precedent state of the MRTD life cycle but are not in the current one, to expose TSF data or sensitive LDS application data, or to bypass or deactivate security functions. It may also attempt to gain undue privileges or to read, modify, delete, or prevent the use of applications, keys or other resources of the MRTD without having the necessary permissions or authentication status.

This threat covers the possibility that the attacker uses a TSF before this function has been correctly created and its internal data structures initialized.

All the assets are threatened.

Application note:

The following list illustrates some possible scenarios for this kind of attack:

- The attacker may send to the MRTD a suite of commands that is not in the expected order, like for example a sequence of STORE DATA commands personalizing the ISD data where the commands are not arranged in the expected order,
- The attacker may perform an authentication operation before all the parameters required by the authentication service have been supplied.
- The attacker may try to use a key after the end of its lifetime.

T.FAULT-INSERTION

The attacker may determine sensitive data through observation of the results of repetitive insertion of selected data.

Insertion of selected inputs followed by monitoring of the output for changes is a relatively well-known attack method for cryptographic devices. The intent is to determine application and passport management related information based on how the MRTD responds to the selected inputs. This threat is distinguished by the deliberate choice and manipulation of input data as opposed to random selection or manipulation of the physical characteristics involved in input/output operations.

All the assets are threatened.

Application note:

The following list illustrates some possible scenarios for this kind of attack:

- The attacker may try to observe the result of ciphering or deciphering a selected command or response in order to gain information that could be used to guess the key used to encrypt another piece of data, or this piece of data itself.
- The attacker may try to observe the result of signing/verifying a selected command in order to gain information that could be used to guess the key used to sign another piece of data.
- The attacker may try to observe the reaction of the platform to a selected collection of challenges and key versions in order to gain information that could be used to determine the cryptogram used by the MRTD to authenticate the Passport Administrator.

T.BRUTE-FORCE

The attacker may search the entire user-accessible data space to identify MRTD data such as cryptographic keys.

This threat is distinguished by the use of valid commands with valid range requests that are repeated to cover as much as possible the data space.

All the assets are threatened.

T.INVALID-INPUT

The attacker may determine security relevant information, cause the MRTD to malfunction or otherwise compromise security through introduction of invalid inputs.

Invalid input may take the form of operations that are not formatted correctly, requests for information beyond register limits, or attempts to search for possible undocumented commands. Such inputs could be generated at any time during the normal usage of the passport, even before authentication, through normal operations. The attack could use invalid data or inappropriate operations, such as commands/functions with requests/formats that are out of range or otherwise non-conforming to the *accepted* usage.

All the assets are threatened.

Application note:

An invalid parameter is a piece of data that is not encoded in the expected format, or which has been forged by the attacker by other means that those defined in the functional specification. An invalid parameter represents a value that should never be used according to the implementation chosen for a particular type of data.

The following are examples of possible invalid parameters concerning security sensitive information:

- a command with one of the INS bytes defined by GlobalPlatform which does not have the expected values in the P1 and P2 parameters, or the expected TLV structure in its data field;
- a key of an invalid length;
- a reference to a component of the key which does not exist for the given key;
- a cryptographic algorithm that is not supported by the platform;
- a message to be encrypted or signed that is not correctly aligned with respect to the cryptographic algorithm to be used;

- a byte-encoded record structure which does not respect the expected encoding format (like a byte where some bits are expected to be set to some value, for instance).

T.FORCED-RESET

The attacker may force the MRTD into an insecure life cycle state through inappropriate termination of current operations.

Attempts to generate a non-secure life cycle state in the MRTD may be made through premature termination of transactions or communications between the MRTD and the terminal, by insertion of interrupts, or by stopping the execution of an application instance that may leave files open. The attacker may also corrupt security sensitive data through the interruption of the execution of the TSF. This includes unexpected loss of the radio frequency field of the terminal as well as firing any other mechanism that could stop or deviate the normal execution of a TSF, like hardware interruptions, input/output interruptions, etc.

All the assets are threatened.

Application note:

The following list illustrates some possible scenarios for this kind of attack:

- The attacker tries to interrupt the copy of a secret key into the buffer used by hardware cryptographic functions, in order to shrink the length of the key during an encryption operation.
- The attacker tries to reset an open Secure Channel, in order to decrease the security level established for the communication with the terminal.

T.USURPATION

The attacker may usurp the role of a rightful Passport Administrator, thus gaining access to the whole TOE.

All the assets are threatened.

3.3.2 Administration Threats

The threats herein described adapt those described in [CSRS] to the specificities of the MRTD administration.

T.DELETION

The attacker tries to delete the ISD, the LDS Application, or their Executable Files.

The deletion of an application could be intended as a *denial of service* attack, or as part of an attack directed to replace the LDS Application by a spurious one.

The threatened assets are the code of applications, the application instances and their attributes.

Application note:

- An attacker may try to delete a package of the API that is necessary for the correct execution of the JCVM.
- An attacker may also try to delete a package in order to free the memory blocks allocated for it, and then try to gain access to the information contained in that block through the allocation functions.

T.INSTALL

The attacker may try to fraudulently install an Executable File or Application instance on the MRTD.

The applications runs onto a Java Card platform that is capable of interpreting any piece of code written in Java Card. This threat concerns either the installation of a Java Card application that could be used to perform a software attack from inside the MRTD. For instance, the attacker's application could try to write the files that the LDS Application uses, or read the keys of the LDS Application or the ISD and send their value out of the MRTD. The attacker may also try to install its own version of the LDS Application to masquerade the genuine one. This threat also concerns the attribution of abusive or incorrect privileges during the activation of the true LDS Application.

The threatened assets are the code of applications, the application instances and their attributes.

T.CHIP-ID

This threat concerns the identification of the MRTD's chip without authorization of the MRTD Holder.

An attacker may try to identify remotely the MRTD's chip by accessing the Initialization Data through its communication interface without knowing the Digital MRZ Data and to trace the movement of the MRTD.

The threatened asset is the Initialization Data.

3.3.3 Operational Use Threats

T.SKIMMING

The threat concerns the skimming of digital MRZ data or the digital portrait.

An attacker may imitate the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

T.EAVESDROPPING

This threat concerns the eavesdropping of the communication between the TOE and the inspection system.

An attacker may listen to the communication between the TOE and an inspection system to obtain private information of the MRTD. Note that the inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know this data in advance.

The threatened assets are the User Data and the Initialization Data.

T.COUNTERFEIT

This threat concerns the counterfeit of the MRTD (unauthorized copy or reproduction of a genuine MRTD).

An attacker may produce an unauthorized copy or reproduction of a genuine MRTD to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD used for authentication of a traveller by possession of a MRTD.

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

All the assets are threatened.

T.FORGERY

This threat concerns the forgery of the MRTD data.

An attacker may alter fraudulently the MRTD data, including its security related data, to change MRTD Holder's identity.

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 an other identity of the traveller.

The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition.

The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker write the digitized portrait from the MRTD of a traveller into an other MTRD leaving their digital MZR unchanged to claim the identity of the holder of this MRTD.

The threatened asset is the User Data.

3.3.4 Integrated Circuit Threats

The following threats come from [ICST]. The term *TOE* or *SmartCard* used in that Security Target has been replaced here by the more specific term *MRTD's chip*, as the scope of the TOE in this Securtiy Target has been enlarged so as to include the Embedded Software. The threat T.ABUSE-FUNC in [ICST] is covered by the threat of the same name that has been previously introduced in this Security Target.

T.PHYS-TAMPER

An attacker may perform physical probing of the MRTD?s chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD?s chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) to modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the discloser or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a prerequisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

This threat menaces all the assets.

Application note:

This threat gathers toghether the threats T.Phys-Probing and T.Phys-Manipualtion in [ICST].

T.MALFUNCTION

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

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

All assests are threatened.

T.INF-LEAK

The 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. No direct contact with the MRTD's chip internals is required here. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA).

All assests are threatened, specially User Data and cryptographic keys.

Application note:

This threat from [ICST] concerns the threat T.EAVESDOPPING introduced in this Security Target.

3.4 Organisational security policies

This section describes the rules that both the TOE and its human environment shall comply to when addressing the security needs.

The organisational security policies included in this document are taken from those introduced in [CSRS] for the configuration of GlobalPlatform targeted in this document and from the MRTD Protection profile [MRTD-PP].

3.4.1 Smartcard Embedded Software OSP

OSP.INIT

The TOE Manufacturer must ensure that the development and production of the MRTD (Phase 1 and Phase 2) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data shall be guaranteed; access to samples, development tools and other material shall be restricted to authorised persons only; scrap will be destroyed etc. This concerns all the actors embodying the role of the Manufacturer during the Phase 1 and Phase 2: Software Developer, the IC Manufacturer, the Passport Manufacturer and the Passport Enabler.

The passport shall be stored and used only in a secured environment, until it becomes operational.

OSP.SECURE-COMMUNICATIONS

Passport Administrator requests administration operations to the MRTD only through a Secure Channel.

OSP.PERSONAL-DATA

The User Data are personal data that the Inspection Systems may use only with the agreement of the MRTD holder.

3.4.2 Integrated Circuit OSP

As already explained for the assumptions, this Security Target enlarges the scope of [ICST] so as to include the embedded software. As a consequence, those organizational policies referring to the correct use of the interfaces of the IC by the Software Developer are not pertinent for this Security Target, as they are discharged (represented) by the assurance measures of the class ADV (and in particular ADV_HLD). This is the case of the P.Add-Functions policy in [ICST]. The other organizational policy included in [ICST], called P.Process-TOE, is covered by the larger OSP.INIT one described in this Security Target.

4 Security objectives

4.1 Security objectives for the TOE

This section defines the security objectives that the TOE must satisfy.

4.1.1 General Objectives

O.LIFE-CYCLE

The TOE shall ensure that the Personalization, and the Operational Use phases of its life cycle are performed in that order and that each operation and sequence of operations performed in a phase is allowed in that phase. The Termination of the TOE may arise at any moment during its life cycle.

O.IDENTIFICATION

The TOE shall provide means to control the access to Initialization Data during the Operational Phase, so that only authenticated administration terminals may obtain the Initialization Data. During the Operational Use phase, the Initialization Data may be obtained only using secure messaging with a Passport Administrator that prevents information disclosure (the information can not be used to prove MRTD's chip identity to a third party).

O.AC-PERSO

The TOE shall ensure that the User Data and the persistent LDS Security Data (Active Authentication Private Key, Document Basic Control Keys) can be written during the Personalization phase only, by an authenticated Personalization Agent and in a way that protects their integrity and confidentiality.

The TOE shall also ensure that these data can not be updated after personalization and that no other data of any kind may be loaded into the MRTD.

O.PROT-PERS

During the Operational Use phase, the TOE shall ensure the integrity and the confidentiality of the User Data by granting read access only to Inspection Systems that performed a successful Basic Access Control Authentication. The TOE shall ensure the integrity of these data during storage on the MRTD (i.e. they can be written only once by the Personalization Agent and are read-only afterwards) and during transmission to the inspection system.

O.ACTIVE-AUTH-PROOF

The TOE shall allow the inspection systems to verify the authenticity of the MTRD as issued by the identified Issuing State of organization.

The TOE has a unique identity given by the MRTD Document number, and a secret to prove its identity i.e. its Active Authentication Private Key. The TOE shall protect this key to prevent their misuse and disclosure.

O.NO-KEY-REUSE

The TOE shall ensure that all the session keys used to authenticate the origin and the integrity of a request from a Passport Administrator or an Inspection System and to guarantee the data confidentiality are used only in the session they were generated. To prevent the potential reuse of a session key, each session key shall contain an unpredictable piece of data that the TOE randomly chooses for each session.

O.REQUEST

The TOE shall reject any request containing data that is not in the expected format.

O.RECOVERY

The TOE shall permit to rollback an incomplete loading of static ISD keys or an incomplete personalization of the LDS application.

O.LOGICAL-PROTECTION

The TOE shall implement a well-defined behavior for all possible chainings of valid operations and all possible valid values, including limit or hardly ever used values. The TOE shall define at least one default value for any security attribute having an impact on the behavior of the TSFs.

O.CRYPTO

The TOE shall provide a means to cipher sensitive data for application instances in a secure way. In particular, the TOE must support cryptographic algorithms consistent with cryptographic usage policies and standards.

Cryptography operations include data encryption and decryption, electronic signature generation and verification, computation of a hash value and random number generation.

O.KEY-MNGT

The TOE shall provide a means to securely manage cryptographic keys. This concerns the correct generation, distribution, use and destruction of cryptographic keys, including the following points:

- Keys shall be generated accordingly with specified cryptographic key algorithms and specified cryptographic key sizes,
- Keys shall be distributed accordingly with specified cryptographic key distribution methods. In particular, keys must be loaded through a secure channel ensuring the origin, the authenticity and the confidentiality of the key.
- Keys shall be completely initialized before being used.
- Keys shall be correctly used.
- Keys shall be protected in confidentiality.
- Keys shall be destroyed in accordance with specified cryptographic key destruction methods that prevent an old key from being reused.

O.DISALLOWED-FUNCTIONS

The code embedded on the MRTD shall no longer accept debugging or code patching commands from the MRTD personalization step (the MRTD state is INITIALIZED).

O.STORAGE-INTEGRITY

The TOE shall provide means to preserve the integrity of sensitive assets, including the static and session keys managed by the applications. The TOE shall mute upon an integrity violation.

4.1.2 Passport Administration

This section introduces those security objectives that are specific to passport administration operations.

O.INFO-ORIGIN-INTEGRITY

The TOE shall be able to authenticate the origin and the integrity of the passport administration requests that the MRTD receives.

O.INFO-CONFIDENTIALITY

The TOE shall be able to process confidential passport administration requests containing encrypted data.

O.NO-LOAD

The TOE shall refuse to load Executable Files on the platform.

O.NO-DELETION

The TOE shall refuse to delete any installed Executable File or Application instance.

4.1.3 Integrated Circuit Objectives

The following objectives for the TOE come from [ICST]. The objective O.IDENTIFICATION of that Security Target is covered by the abovementioned objective of the same name. The objectives O.Leak-Inherent and O.Leak-Forced have been gather together into a single goal O.PROT-INF-LEAK. Similarly, the objectives O.Phys-Probing and O.Phys-Manipulation have been collapsed into a single goal O.PROT-PHYS-TAMPER.

When approriate, the term "TOE" used in [ICST] has been replaced in the statement of the objectives by the preciser term "IC", as the TOE of this Security Target is larger than the one used in [ICST].

O.ABUSE-FUNC

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Embedded Software, (iii) to manipulate Soft-coded Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

O.PROT-INF-LEAK

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

- o 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

- o by forcing a malfunction of the TOE and/or
- o by a physical manipulation of the TOE.

Application note:

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.

O.PROT-PHYS-TAMPER

The IC must provide protection 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:

- o 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
- o 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)
- o manipulation of the hardware and its security features, as well as
- o controlled manipulation of memory contents (User Data, TSF Data).

with a prior

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

O.PROT-MALFUNCTION

The IC must ensure its correct operation. The IC 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.

4.2 Security objectives for the environment

Security objectives for the environment are divided into two categories: objectives for the IT environment and objectives for the operational environment of the TOE.

Security objectives on the environment are related to assumptions or organisational security policies. In some cases they are just a replication of the assumption that the security objective have to uphold.

4.2.1 Non-IT Environment

This section states the objectives for the humans and the terminals interacting with the MRTD.

OE.PASSPORT-ADMIN

The Manufacturer and the Passport Administrator shall never perform an action that could weaken the security level that the MRTD provides. All the keys that allow a user to endorse the role of Passport Administrator are kept secret and protected from disclosure in a secure environment that also ensures their integrity. This concerns the TOE keys

administration keys (ISD keys), the Document Basic Access Keys and the Active Authentication Private Key, as well as the Document Signer Private Key.

OE.PERSONALIZATION

The Issuing State or Organization shall ensure that users acting in the role of a Personalization Agent (i) establish the correct identity of the MRTD holder and create biographic data for the MRTD, (ii) enrol the biometric reference data of the MRTD holder i.e. the portrait, and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures (including the digital signature in the Document Security Object).

The Personalization Agent enables the Basic Access Control function of the TOE and generates and loads the Basic Access Control keys into the MRTD.

OE.PASSIVE-AUTH-SIGN

The Issuing State or Organization shall

- o generate a cryptographic secure Country Signing Key Pair,
- o ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment, and
- o distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity.

The Issuing State or organization shall also

- o generate a cryptographic secure Document Signing Key Pair,
- o ensure the secrecy of the Document Signer Private Key and sign Document Security Objects of genuine MRTD in a secure operational environment only and
- o distribute the Certificate of the Document Signing Public Key to receiving States and organizations.

The digital signature in the Document Security Object include all data in the data groups DG1 to DG16 stored in LDS according to [MRTD-LDS].

OE.ACTIVE-AUTH-KEY

The Issuing State or Organization shall

- o generate the MRTD's Active Authentication Key Pair
- o sign and store the Active Authentication Public Key Info in DG15 and
- o support inspection systems of receiving States or organizations to verify the authenticity of the MRTD by certification of the MRTD Public Authentication Key by means of the Document Security Object.

OE.EXAMINATION

The Inspection System of the Receiving State or Organization shall use the MRTD presented by the traveller to verify its identity and to verify the authenticity of the MRTD.

The Inspection System is a trusted terminal that will not use its privileges to disclose the assets to which it has access nor to track the MRTD use.

OE.PASSIVE-AUTH-VERIF

The Inspection Systems shall verify the signature of Document Security Object before they are used for identifying the traveller as the MRTD Holder. The receiving States and

organizations shall manage the Country Signing Public Key and the Document Signing Public Key maintaining their authenticity and availability in all Inspection Systems (the Document Signing Public Key may also be obtained from the MRTD itself).

OE.PROT-DATA

The Inspection System of the Receiving State or Organization shall ensure the confidentiality and integrity of the data read from the MRTD. The Inspection Terminal used at the Receiving State shall implement the terminal part of the BAC protocol and use of the secure messaging with fresh generated keys for the communication between the terminal and the MRTD.

OE.ACTIVE-AUTH-VERIF

The Inspection System of the Receiving State or Organization shall use the Active Authentication Mechanism to verify the authenticity of the MRTD presented by the traveller, provided the terminal has the capability to do that.

OE.MANUFACTURING

The Passport Manufacturer shall ensure the quality and integrity of the manufacturing process as well as the disabling of all test, debug and patching mechanisms from the product once the MRTD is in OP_READY state (at the beginning of the pre-personalization).

The different actors embodying the role of the Passport Manufacturer (IC Manufacturer, Passport Manufacturer and Passport Enabler) shall apply security procedures to maintain confidentiality and integrity of the TOE and of its manufacturing and test data up to delivery to the end-user (to prevent any possible copy, modification, retention, theft or unauthorised use). In particular, the TOE must be protected appropriately when it is delivered from one actor to the other.

4.2.2 Integrated Circuit Objectives for the Environment

This Security Target enlarges the scope of [ICST] so as to include the embedded software. As a consequence, those security objectives for the IC environment that refer to the correct use of the hardware by the Software Developer are not pertinent for this Security Target, as they are discharged (represented) either by the assurance measures or by the objectives for the TOE. This is the case of the following security objectives in [ICST]:

- OE.Plat-Appl, which concerns the correct use of the hardware, is mainly covered by the ADV and ALC assurance measures.
- OE.Resp-Appl, which concerns the correct treatment of cryptographic keys by the Embedded Software, is covere by O.KEY-MNGT, O.STORAGE-INTEGRITY, O.INFO-ORIGIN-INTEGRITY and O.INFO-CONFIDENTIALITY.

Those security objectives for the environment concerning the protection of the IC all along the manufacturing phase of the MRTD are covered by the larger security objective OE.MANUFACTURING, which includes all the roles involved in the Phase 1 of the TOE: Software Developer, IC Manufacturer, Passport Manufacturer and Passport Enabler. This is the case of the OE.Process-TOE and OE.Process-Card security objectives introduced in [ICST].

5 IT security requirements

5.1 TOE security functional requirements

This section describes the requirements imposed on the security functions of the TOE in order to achieve the security objectives that were laid down for it in the previous chapter.

Functional requirements are grouped into two categories. The first one comes from [MRTD-PP] and mainly concern the operational phase of the MRTD. The second one contains extra requirements regarding the administration of the passport, and specially the pre-personalization of the MRTD.

5.1.1 Security management

FMT_SMR.1/MRTD Security roles

FMT_SMR.1.1/MRTD The TSF shall maintain the roles **Passport Administrator, Personalization Agent and General Inspection System**.

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

FMT_LIM.1/MRTD Limited capabilities

FMT_LIM.1.1/MRTD 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 ***[proprietary information removed]***.

FMT_LIM.2/MRTD Limited availability

FMT_LIM.2.1/MRTD The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced ***[proprietary information removed]***.

FDP_SDI.2/MRTD Stored data integrity monitoring and action

FDP_SDI.2.1/MRTD The TSF shall monitor user data stored within the TSC for **integrity errors** on all objects, based on the following attributes: ***[proprietary information removed]***.

FDP_SDI.2.2/MRTD Upon detection of a data integrity error, the TSF shall ***[proprietary information removed]***.

FMT_MSA.2/Checksum Secure security attributes

FMT_MSA.2.1/Checksum The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.1/Checksum Management of security attributes

FMT_MSA.1.1/Checksum The TSF shall enforce the **Issuer Security Domain, LDS access control SFPs** to restrict the ability to **compute** the security attributes **checksums of a key** to **Passport Administrator, Personalization Agent and General Inspection System**.

FMT_SMF.1/Checksum Specification of management functions

FMT_SMF.1.1/Checksum The TSF shall be capable of performing the following security management functions: **computation of checksums on cryptographic keys stored in the MRTD (sessions and static ones), application code and initialization data**.

5.1.2 Identification and authentication

FIA_UID.1/MRTD Timing of identification

FIA_UID.1.1/MRTD The TSF shall allow

- **Selecting the ISD or the LDS application.**
- **Requesting the opening of an Administration Secure Channel.**
- **Requesting the opening of a Basic Access Control secure channel, in Phase 4 "Operational Use"**

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

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

FIA_UAU.1/MRTD Timing of authentication

FIA_UAU.1.1/MRTD The TSF shall allow **the TSF-mediated actions listed in FIA_UID.1/MRTD** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/MRTD The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4/MRTD Single-use authentication mechanisms

FIA_UAU.4.1/MRTD The TSF shall prevent reuse of authentication data related to**:**

- **Basic Access Control Authentication Mechanism**
- **Administration Secure Channel Mechanism**.

FIA_UAU.5/MRTD Multiple authentication mechanisms

FIA_UAU.5.1/MRTD The TSF shall provide**:**

- **Basic Access Control Authentication Mechanism [MRTD]**
- **Administration Secure Channel Mechanism [VGP2.0.1']**

to support user authentication.

FIA_UAU.5.2/MRTD The TSF shall authenticate any user's claimed identity according to the **following rules:**

- **The Basic Access Control (BAC) Authentication: (i) the Border Control Officer (the Inspection system) reads the printed data in the passport book, (ii) it generates, from these data, the Document Basic Access Control Keys used to authenticate itself to the TOE, (iii) then both the TOE and the Inspection System generates the same Basic Access Control Session Keys used for establishing a trusted channel protected in integrity and confidentiality.**
- **Administration Secure Channel: (i) the Passport Administration uses the static ISD keys to authenticate itself to the TOE, (ii) then both the TOE and the Passport Administrator generates the same Administration Session Keys used for establishing a trusted channel. The Passport Administrator indicates the security level of the channel: the channel may be protected in integrity and also in confidentiality (from the data entering into the TOE)**

.

5.1.3 Passport Administration Security Policy

This section introduces an access control policy controlling the operations for pre-personalizing the MRTD and performing life cycle management. This policy addresses requirements regarding the use of a general purpose card manager (VGP2.0.1') for the

administration of the MRTD and a general runtime environment (a Java Card Virtual Machine) for its computing capabilities. Those requirements concern the following three issues: controlling the passport administration commands allowed for each life cycle state of the MRTD, controlling the evolution of the life cycle of both the LDS application and the MRTD, disabling the installation of other Java Card applications apart from the LDS one and the deletion of any installed application.

FDP_ITC.1-KL Import of user data without security attributes

FDP_ITC.1.1-KL The TSF shall enforce the **Issuer Security Domain access control SFP** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2-KL The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3-KL The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **if the imported data is a pre-personalization (static ISD) key set, then:**

- **If the command specifies the replacement of a key set, the specified key set must exist on the MRTD, and it must contain the same number of keys, each one with the same number of components, and each component with the same type and length as the proposed new ones.**
- **The type of the imported keys shall be supported by [VGP2.0.1']**
- **The data field of the command shall be decrypted using the data encryption key**
- **the check value attached to each DES key shall be correct**.

FDP_ETC.1/ISD Export of user data without security attributes

FDP_ETC.1.1/ISD The TSF shall enforce the **Issuer Security Domain access control SFP** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2/ISD The TSF shall export the user data without the user data's associated security attributes.

FDP_ACC.1/ISD Subset access control

FDP_ACC.1.1/ISD The TSF shall enforce the **Issuer Security Domain access control SFP** on **the following list of subjects, objects and operations:**

- **Subjects: the ISD and LDS application instances**
- **Objects: Executable Files, application instances, ISD static and session keys, initialization and administration data,**
- **Operations: GlobalPlatform APDU commands**.

FDP_ACF.1/ISD Security attribute based access control

FDP_ACF.1.1/ISD The TSF shall enforce the **Issuer Security Domain access control SFP** to objects based on the following:

- **security attributes of the ISD application instance: *[proprietary information removed]*,**
- **security attribute of LDS application instance: *[proprietary information removed]*,**
- **security attribute of initialization data and ISD 's static and session keys: *[proprietary information removed]***.

FDP_ACF.1.2/ISD The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[proprietary information removed]***.

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

FDP_ACF.1.4/ISD The TSF shall explicitly deny access of subjects to objects based on the **following rule: *[proprietary information removed]***.

FMT_MSA.3/States Static attribute initialisation

FMT_MSA.3.1/States The TSF shall enforce the **Issuer Security Domain and LDS access control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/States The TSF shall allow the **following role: none** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Security_level Static attribute initialisation

FMT_MSA.3.1/Security_level The TSF shall enforce the **Issuer Security Domain access control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Security_level The TSF shall allow the **Passport Administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1/States Management of security attributes

FMT_MSA.1.1/States The TSF shall enforce the **Issuer Security Domain and LDS access control SFP** to restrict the ability to **modify** the security attributes **MRTD state and the LDS state** to **the Passport Administrator**.

FMT_MSA.1/Security_level Management of security attributes

FMT_MSA.1.1/Security_level The TSF shall enforce the **Issuer Security Domain access control SFP** to restrict the ability to **change_default** the security attributes **security level** to **the Passport Administrator**.

FMT_SMF.1/ISD Specification of management functions

FMT_SMF.1.1/ISD The TSF shall be capable of performing the following security management functions: **modification of the following security attributes of the ISD policy: *[proprietary information removed]***.

Non editorial refinement:

[proprietary information removed]

FDP_ROL.1/ISD Basic rollback

FDP_ROL.1.1/ISD The TSF shall enforce **the Issuer Security Domain access control SFP** to permit the rollback of the **incomplete loading** on the **static keys enabling to open a Secure Channel with the MRTD for passport administration**.

FDP_ROL.1.2/ISD The TSF shall permit operations to be rolled back within the **following boundary limit: all states of the MRTD's life cycle**.

FTP_ITC.1/ISD Inter-TSF trusted channel

FTP_ITC.1.1/ISD The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ISD The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/ISD The TSF shall initiate communication via the trusted channel for **loading a key set of the ISD, getting Initialization Data, personalizing the LDS**

application (only once), changing the life cycle state of the ISD or the LDS application.

Global refinement:

The remote IT product is the terminal placed in the Passport Administrator secured environment.

5.1.4 LDS Security Policy

FDP_ITC.1/LDS Import of user data without security attributes

FDP_ITC.1.1/LDS The TSF shall enforce the **LDS Access Control SFP** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2/LDS The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3/LDS The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: ***[proprietary information removed]***.

FDP_ETC.1/LDS Export of user data without security attributes

FDP_ETC.1.1/LDS The TSF shall enforce the **LDS Access Control SFP** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2/LDS The TSF shall export the user data without the user data's associated security attributes.

FDP_ACC.1/LDS Subset access control

FDP_ACC.1.1/LDS The TSF shall enforce the **LDS Access Control SFP** on **the following subjects, objects and operations:**

- **Subjects: LDS application instance, ISD application instance,**
- **Objects: User Data (Digital MRZ Data, Digital portrait of the MRTD Holder, Other personal data, Document Security Object, Active Authentication Public Key), Document Basic Access Control Keys, Active Authentication Private Key and session keys used to communicate**
- **Operations: read and write User Data**.

FDP_ACF.1/LDS Security attribute based access control

FDP_ACF.1.1/LDS The TSF shall enforce the **LDS Access Control SFP** to objects based on the following:

- **security attributes of ISD application instance: authentication status of administration secure channel and *[proprietary information removed]*,**
- **security attributes of LDS application instance: authentication status of Basic Access Control Authentication *[proprietary information removed]*,**
- **security attributes of keys: *[proprietary information removed]***.

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

[proprietary information removed].

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

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

[proprietary information removed].

FMT_MSA.3/LDS Static attribute initialisation

FMT_MSA.3.1/LDS The TSF shall enforce the **LDS Access Control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/LDS The TSF shall allow the **following role: Passport Administrator, Personalization Agent and General Inspection System** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1/Authentication_status Management of security attributes

FMT_MSA.1.1/Authentication_status The TSF shall enforce the **LDS Access Control SFP** to restrict the ability to **modify** the security attributes **authentication status of the administration secure channel and authentication status of the Basic Control Access Authentication** to **Personalization Agent (for the administration secure channel) and General Inspection System (for the Basic Access Control)**.

FMT_SMF.1/LDS Specification of management functions

FMT_SMF.1.1/LDS The TSF shall be capable of performing the following security management functions: **initializing the authentication status for the administration secure channel and the BAC authentication**.

FDP_ROL.1/LDS Basic rollback

FDP_ROL.1.1/LDS The TSF shall enforce **the LDS access control SFP** to permit the rollback of the **incomplete personalization of the LDS application** on the **MRTD holder data**.

FDP_ROL.1.2/LDS The TSF shall permit operations to be rolled back within the **following boundary limit:** ***[proprietary information removed]***.

FTP_ITC.1/LDS Inter-TSF trusted channel

FTP_ITC.1.1/LDS The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/LDS The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/LDS The TSF shall initiate communication via the trusted channel for **reading the User Data and for performing Active Authentication**.

Global refinement:

The remote IT product is the Inspection System.

FDP_UCT.1/LDS Basic data exchange confidentiality

FDP_UCT.1.1/LDS The TSF shall enforce the **LDS Access Control SFP** to be able to **receive and transmit** objects in a manner protected from unauthorised disclosure.

FDP_UIT.1/LDS Data exchange integrity

FDP_UIT.1.1/LDS The TSF shall enforce the **LDS Access Control SFP** to be able to **transmit and receive** user data in a manner protected from **replay, insertion, deletion and modification** errors.

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

5.1.5 Cryptographic support

5.1.5.1 General

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[proprietary information removed]*** that meets the following: ***[proprietary information removed]***.

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **all users and subjects** are unable to observe the operation **cryptographic computation and key management** on **resources** by **subjects**.

5.1.5.2 ISD keys

FCS_CKM.1-SCP01-SESSION-KEY Cryptographic key generation

FCS_CKM.1.1-SCP01-SESSION-KEY The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[GPCS] session key generation algorithm** and specified cryptographic key sizes **of 112 bit** that meet the following: **[VGP]**.

FCS_COP.1-DES3/CBC Cryptographic operation

FCS_COP.1.1-DES3/CBC The TSF shall perform **decryption of the data field of the messages exchanged through a Secure Channel with the Passport Administrator** in accordance with a specified cryptographic algorithm **Triple DES in CBC mode** and cryptographic key sizes **of 112 bits** that meet the following: **[VGP]**.

FCS_COP.1-DES3/ECB Cryptographic operation

FCS_COP.1.1-DES3/ECB The TSF shall perform **the following cryptographic operations:**

- **session key derivation**
- **key encryption/decryption**
- **DES Key check value generation and verification**

in accordance with a specified cryptographic algorithm **Triple DES in ECB mode** and cryptographic key sizes **of 112 bits** that meet the following: **[VGP]**.

FCS_COP.1-DES3/FULL Cryptographic operation

FCS_COP.1.1-DES3/FULL The TSF shall perform **the following cryptographic operations related to passport administration:**

- **generation of the MRTD authentication cryptogram,**
- **verification of the terminal authentication cryptogram,**
- **MAC verification of the messages exchanged through a Secure Channel**

in accordance with a specified cryptographic algorithm **full triple DES** and cryptographic key sizes **of 112 bit** that meet the following: **[VGP]**.

5.1.5.3 Active Authentication keys

FCS_COP.1/AA_MRTD Cryptographic operation

FCS_COP.1.1/AA_MRTD The TSF shall perform **digital signature generation for proving that the MRTD is genuine** in accordance with a specified cryptographic algorithm **RSA with SHA-1** and cryptographic key sizes **1024 bits** that meet the following: **ISO/IEC 9796-2:2002 (Digital Signature Scheme 1)**.

5.1.5.4 Document Basic Access Control keys

FCS_CKM.1/BAC_SESSION_KEYS Cryptographic key generation

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

FCS_COP.1/BAC_ENC Cryptographic operation

FCS_COP.1.1/BAC_ENC The TSF shall perform **secure messaging: encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bit** that meet the following: **[MRTD], Annex E**.

FCS_COP.1/BAC_MAC Cryptographic operation

FCS_COP.1.1/BAC_MAC The TSF shall perform **secure messaging: message authentication code** in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bit** that meet the following: **ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)**.

FCS_COP.1/SHA_MRTD Cryptographic operation

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

5.1.6 Integrated Circuit

The section contains those SFRs considered in [ICST] that are also relevant for this Security Target. They mainly concern protecting the MRTD's chip against physical tampering, preventing the disclosure of information when it is transferred from different physical parts of the chip, providing the basic DES operation, and keeping a secure state when a malfunction is detected and providing an independent security domain for the hardware.

The following SFRs come from [ICST] and are defined as SFRs for the non-IT environment:

- RE.Phase-1on correct design of the smartcard embedded software according to requirements of IC manufacturer. This requirement is covered by the assurance measures concerning the development of smartcard embedded software and its environment.
- RE.Process-Card on the protection of IC after its delivery. This requirement is covered by the assurance measures concerning the life cycle support of the smartcard embedded software.
- RE.Cipher on the usage of key-dependent functions. This requirement corresponds to all the requirements on the TOE concerning cryptographic support (FCS class) and FDP_ITC.1-KL, which ensure a correct management of keys and related functions.

FRU_FLT.2-IC Limited fault tolerance

FRU_FLT.2.1-IC The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: **exposure to operating conditions which are not detected according to the requirement FPT_FLS.1-IC**.

FPT_FLS.1-IC Failure with preservation of secure state

FPT_FLS.1.1-IC The TSF shall preserve a secure state when the following types of failures occur:

- **exposure to operating conditions when a malfunction could occur;**
- **failure detected by TSF according to FPT_TST.1-IC**.

FPT_SEP.1-IC TSF domain separation

FPT_SEP.1.1-IC The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2-IC The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_TST.1-IC TSF testing

FPT_TST.1.1-IC The TSF shall run a suite of self tests **at the request of the authorised user** to demonstrate the correct operation of **following environment sensor mechanisms: frequency monitoring, voltage sensor, light detection and temperature sensor**.

FPT_TST.1.2-IC The TSF shall provide authorised users with the capability to verify the integrity of **the TSF data**.

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

FPT_PHP.3-IC Resistance to physical attack

FPT_PHP.3.1-IC The TSF shall resist **physical manipulation and physical probing** to the **TSF of the IC** by responding automatically such that the TSP is not violated.

FCS_COP.1-IC Cryptographic operation

FCS_COP.1.1-IC The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **Triple Data Encryption Standard (Triple DES)** and cryptographic key sizes **112 bits** that meet the following: **FIPS 46-3**.

FDP_ITT.1-IC Basic internal transfer protection

FDP_ITT.1.1-IC The TSF shall enforce the **Data Processing Policy** to prevent the **disclosure** of user data when it is transmitted between physically-separated parts of the TOE.

FPT_ITT.1-IC Basic internal TSF data transfer protection

FPT_ITT.1.1-IC The TSF shall protect TSF data from **disclosure** when it is transmitted between separate parts of the TOE.

FDP_IFC.1-IC Subset information flow control

FDP_IFC.1.1-IC The TSF shall enforce the **Data Processing Policy** on **all confidential data when they are processed or transferred by the IC or the Embedded Software**.

5.2 TOE security assurance requirements

The security assurance requirement level is EAL4. The EAL is augmented with ADV_IMP.2 and ALC_DVS.2.

5.3 Security requirements for the IT environment

5.3.1 IT environment functional requirements

This Security Target does not impose any functional requirement for the IT environment refining the security objectives stated for it.

5.4 Security requirements for the non-IT environment

5.4.1 Non-IT environment functional requirements

This Security Target does not impose any functional requirement for the non-IT environment refining the security objectives stated for it.

6 TOE summary specification

6.1 TOE security functions

There is no minimum strength for the security functions.

6.1.1 Runtime Environment

6.1.1.1 General

SF.Integrity

This TSF ensures integrity protection of sensitive data.

This function has no strength.

SF.Confidentiality

This TSF ensures the confidentiality of sensitive data.

This function has no strength.

SF.AtomicTransactions

This TSF provides a means to execute a sequence of modifications and allocations on the persistent memory of the MRTD so that either all of them are completed, or the MRTD behaves as if none of them had been executed.

This function has no strength.

SF.SignatureGenerationVerification

This TSF provides means for generating electronic signatures of digitalized data.

This function has no strength.

SF.EncryptionDecryption

This TSF provides means for encrypting and decrypting data.

This function has no strength.

SF.Hashing

This TSF provides means for generating hash values.

This function has no strength.

6.1.1.2 Issuer Security Domain

SF.OPEN

This TSF manages the GlobalPlatform internal data structure, selects the application to be executed (ISD or LDS applet) and dispatches the APDU commands to it.

This function has no strength.

SF.ContentAdministration

This TSF manages the administrative information contained in the passport.

This function has no strength.

SF.AdministrationCommandsControl

This TSF controls the passport administration commands that are allowed at each state of the MRTD's life cycle.

This function has no strength.

SF.LifeCycleManagement

This TSF enforces the TOE's life cycle.

This function has no strength.

SF.AdminKeyLoadReplace

This TSF enables to load or replace the key sets that the ISD uses to establish a secure channel with the Passport Administrator.

This function has no strength.

6.1.2 Administration Secure Channels

SF.AdminTerminalAuthentication

This TSF enforces the authentication of the Passport Administrator.

This function has no strength.

SF.AdminSessionKeyGeneration

This TSF generates the session keys used for opening a Secure Channel with the Passport Administrator.

This function has no strength.

SF.AdminMessageIntegrityAuthentication

This TSF enforces the integrity and the origin of the APDU commands received through an Administration Secure Channel.

This function has no strength.

SF.AdminMessageConfidentiality

This TSF enforces the confidentiality of the contents of an APDU message containing sensitive information.

This function has no strength.

SF.AdminSecureChannelTermination

This TSF enforces the correct termination of Administration Secure Channels.

This function has no strength.

6.1.3 LDS Application

SF.LDSCommandsControl

This TSF controls the commands that are allowed at each life cycle state of the LDS Application, thus restricting its available functionalities.

This function has no strength.

SF.Personalization

This TSF controls the personalization of the LDS application and the transition to the Operational Use phase.

This function has no strength.

SF.BasicAccessControl

This function stands for the Basic Access Control mechanism defined in [MRTD].

This function has no strength.

SF.ActiveAuthentication

This function stands for the Active Authentication mechanism defined in [MRTD].

This function has no strength.

6.1.4 Integrated Circuit TSFs

The following TSFs come from [ICST] >: < STFULL

- SEF1 Operating state checking, which supports SF.Integrity,
- SEF2 Phase management with test mode lock-out,
- SEF3 Protection against snooping,
- SEF4 Data encryption and data disguising, which supports SF.Confidentiality,
- SEF5 Random number generation,
- SEF6 TSF self test,
- SEF7 Notification of physical attack,
- SEF8 Memory Management Unit (MMU),
- SEF9 Cryptographic support < /STFULL >

SF.OperatingStateChecking

This is the security function SEF1 "Operating state checking" introduced in [ICST].

This function has no strength.

SF.PhaseManagement

This is the security function SEF2 "Phase Management with test mode lock-out" introduced in [ICST].

This function has no strength.

SF.ProtectionAgainstSnooping

This is the security function SEF3 "Protection against snooping" introduced in [ICST].

This function has no strength.

SF.DataEncryption

This is the security function SEF4 "Data Encryption and data disguising" introduced in [ICST].

This function has no strength.

SF.RNG

This is the security function SEF5 "Random Number Generation" introduced in [ICST].

This function has no strength.

SF.SelfTest

This is the security function SEF6 "TSF Self Test" introduced in [ICST].

This function has no strength.

SF.NotificationOfPhysicalAttack

This is the security function SEF7 "Notification of Physical Attack" introduced in [ICST].

This function has no strength.

SF.CryptographicSupport

This is the security function SEF9 "Cryptographic Support" introduced in [ICST].

This function has no strength.

7 Extended Components Definition

This security target uses components defined as extensions to CC part 2.

7.1 Definition of the Family FMT_LIM

The family "Limited capabilities and availability (FMT_LIM)" has been taken from the reference [SSVG]. It 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 Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component leveling:

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.

Rationale for the introduction of the family LIM.

To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF.

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

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: *Limited capability and availability policy*].
Dependencies:	FMT_LIM.2 Limited availability.

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

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].
Dependencies:	FMT_LIM.1 Limited capabilities.

Appendix A Glossary

This document uses the following terms:

Term	Definition
Active Authentication Key Pair	Asymmetric cryptographic key pair defined in **[MRTD]** for the Active Authentication. It is unique for the MRTD's chip. The Active Authentication Private Key is stored on the MRTD's chip and used by the MRTD's chip to prove its identity and authenticity. The Active Authentication Public Key is stored in the Active Authentication Public Key Info (DG15), signed by means of the Document Security Object on the MRTD's chip **[MRTD]** and read and used by the inspection system to verify the MRTD's proof.
Application instance	Instance of an Executable Module after it has been installed and made selectable.
Application Code Verification	A formal (e.g. mathematically based) analysis of an Executable Module to determine whether the software code possesses certain essential security properties or not
Application Protocol Data Unit (APDU)	Standard communication messaging protocol between a card accepting device and a smart card. See ISO-7816-4.
Application Provider	Role that owns an Application and is responsible for the Application's behaviour
Application Session	The link between the Application and the external world during a Card Session starting with the Application selection and ending with Application de-selection or termination of the Card Session
Asymmetric Cryptography	A cryptographic technique that uses two related transformations, a public transformation (defined by the Public Key component) and a private transformation (defined by the Private Key component); these two key components have a property so that it is computationally infeasible to discover the Private Key, even if given the Public Key.
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	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD based on MRZ information as key seed and access condition to data stored on the passport according to LDS.

Mis en forme : Anglais Royaume-Uni

Term	Definition
Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD and the inspection system **[MRTD]**. 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.
Biographical data (biodata).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa **[MRTD-Annex]**.
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD (digital portrait).
Card Content	Code and Application information (but not Application data) contained in the card that is under the responsibility of the OPEN e.g. Executable Load Files, Application instances, etc
Card Image Number (CIN)	An identifier for a specific GP card
Cardholder	The end user of a card
Card Issuer	Role that owns the card and is ultimately responsible for the behaviour of the card
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means **[MRTD-Annex]**.
Country Signing CA Certificate (CCSCA)	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
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. Stored in the MRTD. May carry the Document Signer Certificate (CDS) **[MRTD]**.
Eavesdropper	A threat agent with moderate attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD.
(IC) Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 3 or in later phases of the TOE life-cycle.
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 **[MRTD-BIO]**.

Term	Definition
Executable File	Actual on-card container of one or more Application's executable code (Executable Modules). It may reside in immutable persistent memory or may be created in mutable persistent memory as the resulting image of a Load File Data Block
Executable Load File	An Executable File that is in transit to the smart card.
Executable Module	Contains the on-card executable code of a single Application present within an Executable Load File
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait **[MRTD-Annex]**.
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. **[MRTD-BIO]**.
GlobalPlatform Registry	A container of information related to Card Content management
IC Dedicated Support Software	That part of the IC Dedicated 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 which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification (idem Card Unique Data)	Data that uniquely identifies a card/passport being the concatenation of the Issuer Identification Number and Card Image Number
IC Manufacturer	Role responsible for integrating the OS, RTE and GP software with the IC ("masking") process
Immutable Persistent Memory	Memory that can only be read
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. **[MRTD-Annex]**
(IC) Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the IC manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).

Term	Definition
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. **[MRTD-BIO]**.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
Issuing State (idem Card Issuer)	The Country issuing the MRTD **[MRTD-LDS]**. Role that owns the passport and is ultimately responsible for the behaviour of the passport.
Issuer Security Domain (ISD)	On-card entity providing support for the control, security, and communication requirements of the Card Issuer
Life Cycle	The existence of Card Content on an Global Platform card and the various stages of this existence where applicable
Life Cycle State	A specific state within the Life Cycle of the passport or of Card Content
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology **[MRTD-LDS]**. The capacity expansion technology used is the MRTD's chip.
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 **[MRTD-LDS]**.
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 **[MRTD-LDS]**.
LDS application	Java Card application defining the functionality of the e-Passport.
Message Authentication Code (MAC)	A symmetric cryptographic transformation of data that provides data origin authentication and data integrity
MRTD holder	The end user of a passport.
Mutable Persistent Memory	Memory that can be modified
Open Platform Environment (OPEN)	The central on-card administrator that owns the Global Platform Registry

Term	Definition
Passive Authentication	The process consisting in the verifying 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.
Passport Administrator	Role that has ultimate control of the passport, within the policy constraints set by the Issuing State, with regards to passport content and Life Cycle management; once the actor that plays the Issuing State role owns the passport, that actor will also play the role of Passport Administrator.
Passport Manager	Generic term for the 2 card management entities of a GlobalPlatform card i.e. the Global Platform Environment and the Issuer Security Domain.
Passport Manufacturer	Role responsible for integrating the “masked” IC with the carrier, in accordance with the Issuing State requirements, to produce a complete passport ready for delivery to the Passport Enabler.
Personalization	The process by which the portrait, signature and biographical data are applied to the document.
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, and (iii) writing these data on the MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Authentication Secret Key	Symmetric cryptographic key.
Pre-Issuance	Phase prior to the passport being issued to the MRTD holder.
Pre-personalization data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2).
Private Key	The private component of the asymmetric key pair
Public key	The public component of the asymmetric key pair
Secret key	One of the symmetric keys that belong to the key set used to generate Session Keys during the initiation of a Secure Channel.
Session key	Key associated to a Secure Channel and which is used for a secure communication session

Term	Definition
Secure Channel	A communication mechanism between an external entity and a passport that provides a level of assurance, to one or both entities
Secure Channel Session	A session starting with the Secure Channel Initiation and ending with a Secure Channel Termination during which the communications use secure messaging.
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 MRTD data or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Software Developer	The person or organization that designs and implements the Embedded Software. The role responsible for developing such code.
Symmetric Cryptography	A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation
Terminal	A logical term used to represent the back end systems that support the Global Platform system; terminals perform functions such as authorization and authentication, administration, post-issuance and transactional processing.
User	Either an external entity that makes a request to a Subject to perform some operation to be performed on an Object within scope of a Security Policy

Index

P

R

S

T