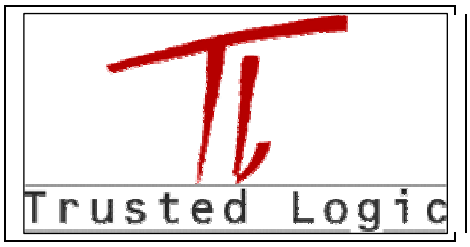

TL ICAO LDS
EAC Security Target Lite

Emission Date	:	July 7th, 2009
Project Name	:	IRIS
Document Type	:	Technical report
Ref./Version	:	PU-2009-RT-356-1.3
Classification	:	**PUBLIC**
Status		**UNDER CC EVALUATION**
Recipients	:	Michael Dulucq (SERMA Technologies)
Number of pages	:	56

Table of figures

Table of tables

1 Introduction

This document is the Security Target Lite of TL ICAO LDS, a Java Card applet which transforms jTOP™ into a Machine Readable Travel Document. It has been conceived to prepare a Common Criteria evaluation following the "compositional approach" described in [COMP]. This approach consists in starting from a *Platform* that has been independently certified, and performing an evaluation of the product resulting from embedding an *Application* into it, which makes use of some of the results issued from the evaluation of the platform. In this case the platform is jTOP (a Java Card platform) and the application is TL ICAO LDS (a Java Card applet). The Java Card platform has been evaluated according to the Security Target [PFASE].

1.1 ST Identification

Title	TL ICAO LDS - EAC Security Target Lite
Sponsor	Trusted Logic SA
Editor	Eduardo Giménez
CC Version	3.1 (Revision 2)
Version Number	1.3

1.2 TOE Identification

Commercial name	TL ICAO LDS
jTOP Platform version	IFXv#27 with patch v1.6
ICAO Application version	22/10/2008 – version 2.0
Integrated Circuit versions	SLE66CLX800PE-m1581-e13/a14 and SLE66CLX360PE-m1587-e13/a14

2 CC Conformance

This Security Target Lite claims conformance to the following documents defining the ISO/IEC 15408:2005 standard:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2006-09-001, Version 3.1, Revision 1, September 2006.
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, CCMB-2007-09-002, Version 3.1, Revision 2, September 2007.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2007-09-003, Version 3.1, Revision 2, September 2007.
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2007-09-004, Version 3.1, Revision 2, September 2007.

Conformance to ISO/IEC 15408:2005 is claimed as follows:

- Part 1: conformant
- Part 2: extended with the following families defined in [PPEAC]: FAU_SAS, FCS_RND, FIA_API, FMT_LIM, FPT_EMSEC. All the other security requirements have been drawn from the catalogue of requirements in CCMB-2007-09-002.
- Part 3: EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3.

2.1 PP Claims

This Security Target Lite is compliant with the following protection profile: "*Machine Readable Travel Document with ICAO Application, Extended Access Control*" [PPEAC]. The compliance is demonstrable in the sense specified in section D.3 of [CC1] because the TOE also comprises an open ID platform, which comes with its own specific assumptions and security objectives for the environment, which are of course not considered in the Protection Profile. Table 1 details the type of conformance for each part of the document.

ST Element	Conformance
Security Problem Definition	Demonstrable
Security Objectives	Demonstrable
Security Functional Requirements	Strict
Security Assurance Measures	Demonstrable

Table 1: Protection Profile Conformance

3 TOE Description

This part of the document describes the TOE as an aid to the understanding of its security requirements. It addresses the general IT features of the TOE.

3.1 TOE Definition

The TOE is a contactless smart card composed of a piece of software embedded into an integrated circuit (IC) which transforms it into a Machine Readable Travel Document with Extended Access Control capabilities. This software is composed of a platform which executes Java Card applications (jTOP) and a particular Java Card applet (TL ICAO LDS) providing the electronic passport services defined in [5] and [20]. The TOE therefore comprises of:

- the circuitry of the MRTD's chip
- the IC Dedicated Software
- the IC Embedded Software (jTOP platform),
- the Java Card applet transforming jTOP into an MRTD (TL ICAO LDS), and
- the associated guidance documentation [USR] and [ADM].

The TOE supports the security mechanisms Basic Access Control and (optional) Active Authentication defined in [5]. It also supports the mechanisms Chip Authentication and Terminal Authentication defined in [20].

The runtime environment on which the TL ICAO LDS is executed is compliant with the version of the Java Card platform specified in [JCVM], [JCRE] and [JCAPI]. The different operations involved in the MRTD management are performed in accordance with VISA GlobalPlatform 2.1.1 specifications, Configuration 2. Management operations include the pre-personalization of the ID platform and the personalization of TL ICAO LDS.

The circuit of the MRTD's chip is any of Infineon's SLE66CLX800PE/SLE66CLX360PE chips, which have been already evaluated according to the Security Target [ICST]. These are bi-mode chips, which may communicate through both the contact-based and the contactless interface.

According to the French Scheme's application note [DCSSIAP09], the TOE does include neither the material that could wrap the chip (passport cover, attached booklet, plastic card, etc) nor the IC antenna.

3.1.1 The TOE as an ID Platform

The TOE can be configured so that other applets apart from the TL ICAO LDS can be downloaded and installed on it, such as a national identity card applet, a driving license applet, etc. Moreover, several instances of TL ICAO LDS can coexist in it, and be used for different identification purposes. The MRTD therefore behaves as an open smart card platform intended for ID applications. A smart card application, however, is usually intended to store highly sensitive information, so the sharing of that information must be carefully limited. Applet isolation is achieved through the Java Card Firewall mechanism defined in [JCRE]. That mechanism confines an applet to its own designated memory area, thus each

applet is prevented from accessing fields and operations of objects owned by other applets, unless the applet that owns it provides a specific interface for that purpose. This access control policy is enforced at runtime by the embedded Java Card Virtual Machine. The challenge of implementing a secure open, multi-application smart card platform has been already addressed in [PFASE]. This Security Target Lite does not focus on that security problem, but on the one described in [PPEAC].

Figure 1 places the different components of the TOE in their environment and schematizes the process for downloading a new applet (different from TL ICAO LDS) on the ID Platform. In order to download a new package on the smart card, its code has to be first approved by the Verification Authority. This Verification Authority is responsible for checking that the Applet Developer has enforced all the security recommendations for programming an application on jTOP, and that the applet code successfully passes the bytecode verification process. Such verifications are performed in a secure physical environment that prevents unauthorized people from modifying the applet's code. If they are successful, the Verification Authority may electronically sign the Executable File containing the applet's code using GlobalPlatform's Data Authentication Pattern mechanism (DAP). This signature attests that the Verification Authority has validated the Executable File, and prevents any further modification on it. The Verification Authority then transmits the signed Executable File to the representative of the Issuing State or Organization in charge of loading new applets on the ID Platform, called hereto the MRTD Administrator. If the Verification Authority does not sign the applet, then it is assumed that there is a secure communication channel between the Verification Authority and the Card Administrator that ensures the origin and the integrity of the received Executable File.

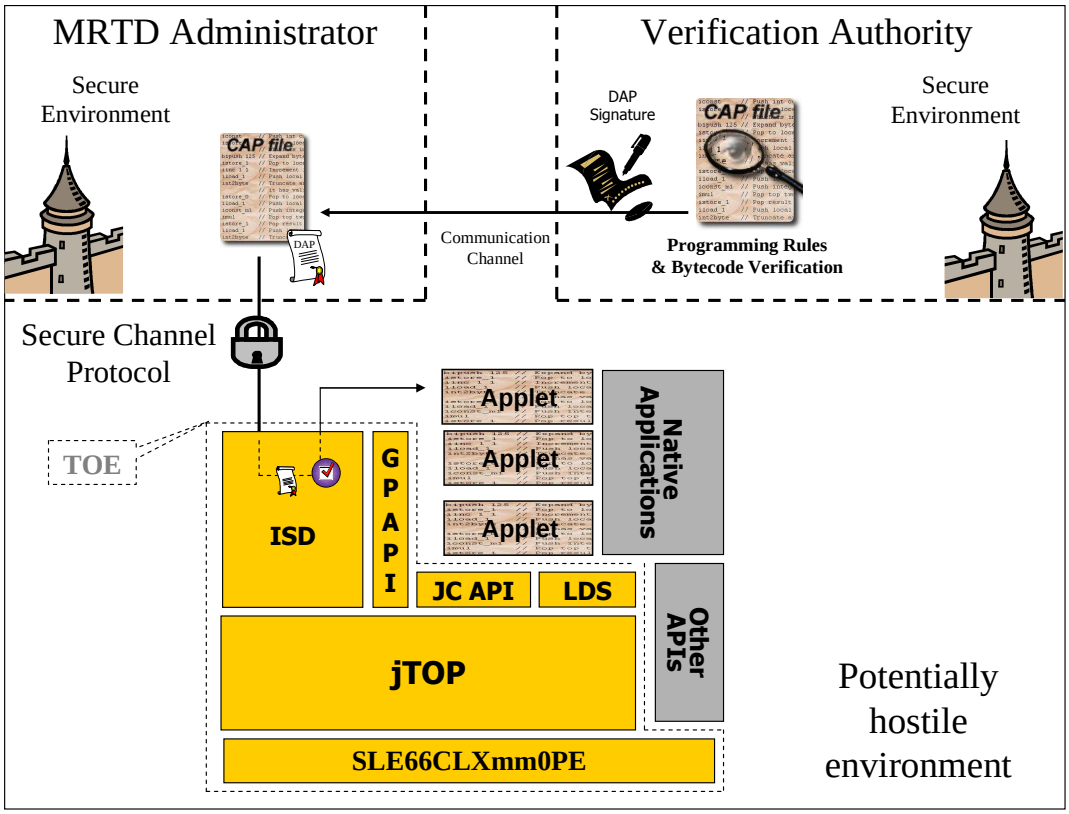

Figure 1: Scope of the TOE

Upon reception of the Executable File, the MRTD Administrator stores it in its secure environment until the file is downloaded into the ID Platform. The ID Platform Administrator transmits the file from its secure environment to the card using GlobalPlatform's secure channel protocol SCP02. This protocol ensures that the file actually comes from a representative of the Issuing State or Organization and that its integrity has been preserved during the transmission step. The file is received by the Issuer Security Domain (ISD), an on-card representative of the Issuing State or Organization in charge of MRTD management. If the ID Platform has been configured to enforce mandatory DAP verification, then the ISD verifies the electronic signature of the Verification Authority upon reception of a new Executable File[1]. If the signature is correct, the package is installed on the ID Platform.

Loading Executable Files requires the TOE to be configured during the IC Manufacturing Phase in order to support this feature. This feature can be disabled during the MRTD Manufacturing Phase, so that the card becomes a *static Java Card Platform*. Once in this configuration, the platform rejects any attempt of downloading new Executable Files. The definite set of available applets is hence the one that can be created from the Java Card packages that have been masked in ROM with the code of the platform and those that have been loaded before moving to the static mode. This operation cannot be undone: once the card becomes static, it cannot rollback to the open configuration again.

3.2 Users and Roles

The users of the TOE include the people and organizations listed below. Please notice that a given real actor may potentially embody several of the defined roles.

Application Provider

An Application Provider is an organization that develops Java Card applications on demand of the Issuing State or Organization. These applications implement services that the Issuing State proposes to the MRTD Holder. The developer of the TL ICAO LDS embedded in the MRTD is an example of Application Provider.

ID Platform Developer

The ID Platform Developer is the organization responsible for designing and implementing the Embedded Software masked on the IC, namely, the jTOP platform.

IC Manufacturer

The IC Manufacturer fabricates and tests the IC, and integrates the Embedded Software within it. This latter step is usually known as the "masking process". The IC Manufacturer is also responsible for loading any Patch File into the EEPROM of the MRTD's IC chip. This role may also pre-configure some of the ID Platform parameters and options.

Manufacturer

The Manufacturer is a generic role that includes all the actors involved in the fabrication of the MRTD. The role of the Manufacturer is in turn embodied by the Application Provider, the ID Platform Developer, the IC Manufacturer, and the MRTD Manufacturer.

[1] If the card is not configured to verify DAP signatures, it is assumed that there is a secure channel linking the Verification Authority and the Card Administrator that ensures the origin and the integrity of the received Executable File. The description of such secure channel falls beyond the scope of this security target.

MRTD Administrator

The MRTD Administrator is the representative of the Issuing State or Organization that has ultimate control of the MRTD's content. The MRTD Administrator can download new applets on the MRTD, temporarily or definitely disable access them, remove applets other than the TL ICAO LDS, replace the ISD's keys or retrieve administrative information from the MRTD. During the Manufacturing phase, this role is embodied by the MRTD's Chip Pre-personalizer and the Personalization Agent. The TOE can be configured so that the MRTD does not recognize this role in the Operational Phase.

MRTD Manufacturer

According to [PPEAC], "*the MRTD Manufacturer (i) adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary, (ii) creates the MRTD application, (iii) equips MRTD's chip with pre-personalization data, and (iv) combines the IC with hardware for the contactless interface in the passport book.*" In practice, this process may be actually split into several steps, which may be potentially performed by different actors. In order to cope with such complex scenarios, this Security Target Lite introduces two sub-roles regarding MRTD fabrication: the MRTD's Chip Pre-Personalizer and the Physical MRTD Manufacturer (see below). While the first does interact and modifies part of the TOE, the second does not perform any security relevant action on it, but just wraps up the TOE with additional physical material.

MRTD's Chip Pre-personalizer

The MRTD's Chip Pre-personalizer is responsible for further tuning the ID Platform options and parameters (e.g.: the particular communication protocol to be used), loading the TL ICAO LDS in EEPROM when the applet is not masked in ROM, creating an instance of it, configuring the created instance, preventing its removal, and replacing the static ISD keys to be used for authenticating the Personalization Agent. This role may optionally add non-biographical data to the logical MRTD, such as the passport number.

Physical MRTD Manufacturer

The Physical MRTD Manufacturer integrates the masked IC with the carrier (a plastic card, a passport booklet, etc) in accordance with the Issuing State requirements, to produce a complete MRTD ready for starting the electronic personalization. This role could be embodied in turn by several actors, such as, for example:

- The Chip Inlay Manufacturer, who enables communications with the chip by physically connecting it to the antenna and placing the whole on an intermediate carrier (for example, a piece of paper).
- The Cover Manufacturer, who embeds the chip inlay into a passport hard cover;
- The Booklet Manufacturer, who bounds the passport cover containing the chip to the passport booklet.
- The Booklet Pre-printer, who prints non-personal data on the passport booklet, such as draws, Issuing State's blazon, etc.
- The Card Embosser, who prints symbols in relief on the surface of plastic card carriers..

None of the above mentioned roles introduce any security relevant action on the TOE, so this Security Target Lite does not introduce any difference between them. Nevertheless, [ADM] provides generic guidance about the organizational measures that shall be enforced when exchanging any asset containing the IC chip.

Personalization Agent

The Personalization Agent acts on behalf of the Issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographical data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [5].

Verification Authority

The Verification Authority is in charge of ensuring that the Java Card applets to be installed on the ID Platform do not violate any of the security policies defined by the Issuing State or Organization. In particular, the Verification Authority is responsible for the bytecode verification of the downloaded applets, as well as for checking that the Application Developer develop them respecting all the security recommendations specified in [PFUSR].

MRTD Holder

The MRTD Holder is the rightful holder of the MRTD for whom the Issuing State or Organization has delivered it.

Traveler

A Traveler is any person presenting the MRTD to an Inspection System and claiming the identity of the MRTD Holder.

3.3 TOE Life Cycle

Figure 2 in page 14 specifies the TOE life cycle. The life cycle states are displayed in gray. Each state includes a collection of actions to be performed when the TOE is in that state. Actions in dotted lines correspond to optional actions, which depend on the TOE configuration and on how actors and roles are mapped in the use case. Arrows specify allowed life cycle transitions. Any other life cycle transition that is not explicitly specified in the diagram is forbidden.

The TOE life cycle includes the four main phases described in [PPEAC]: Development, Manufacturing, Personalization of the MRTD and Operational Use. In addition to this, it refines that life cycle by the introduction of additional states and the specification of sub-phases detailing the actions performed in the main phases.

3.3.1 Development

During the Development Phase, the IC Manufacturer designs the chip, the ID Platform Developer designs the code of the ID Platform, and the Applet Providers designs the code of TL ICAO LDS and potentially of other applets to be embedded with the platform's code.

The role of the IC Manufacturer is embodied by Infineon Technologies AG.

The role of the ID Platform Developer and the Applet Provider developing TL ICAO LDS is embodied by Trusted Logic SA.

The IC Manufacturer provides the ID Platform Developer with the chip's databook and programmers guidelines. The Application Provider applies the programming rules specified in [PFUSR] to develop the applets. The ID Platform Developer also provides the Verification Authority with this latter document, so that it can check that the applet does satisfy all the expected constraints before signing it.

3.3.2 Manufacturing

The Manufacturing phase introduced in [PPEAC] is refined into two sequential sub-phases: IC Manufacturing and MRTD Manufacturing.

3.3.2.1 IC Manufacturing

During this sub-phase, the IC Manufacturer fabricates and tests the IC, masks the IC with the code of the ID Platform and configures the ID Platform. This latter action consists in loading any Patch File that could be required for the ID Platform code and setting the Card Parameters and the Card Configuration File. The ID Platform configuration determines the behavior of some of the TSF.

The ID Platform Developer provides the IC Manufacturer with the code to be masked and the values to be written in EEPROM: Patch File (if any) Card Parameters and Card Configuration File. It also provides the IC Manufacturer with the guidance [PFIGS] and the keys required for testing the masked IC and updating the transport keys required for performing further management operations on the ID Platform.

3.3.2.2 MRTD Manufacturing

This sub-phase consists in transforming the chip masked with the ID Platform into an MRTD ready for being personalized. This process is made of two different kinds of actions: manufacturing the physical MRTD and pre-personalizing the MRTD's chip.

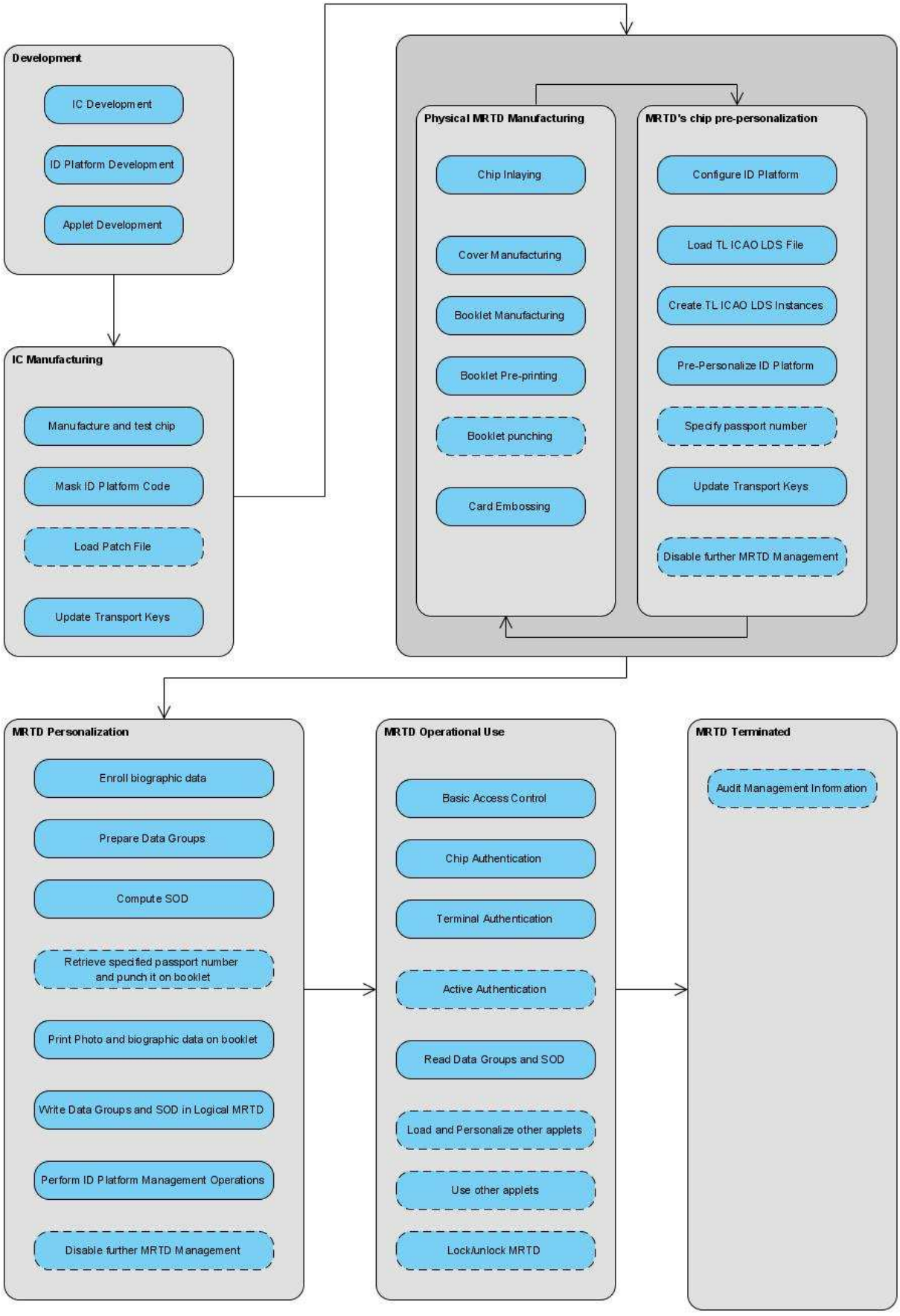

Figure 2: TOE Life Cycle

Manufacturing the physical MRTD consists in connecting the integrated circuit with its communication interface (contact-based, contactless, or both) and wrapping it with different types of materials (paper, plastic, etc). In the case of a typical contactless MRTD to be used as an e-passport, the IC is first connected with the antenna and placed inside a paper sheet or a passport hard cover. The resulting inlay is then linked to a passport booklet. Moreover, the booklet may be furthermore modified by different transformations, such as pre-printing its pages, punching on the passport number on it, etc. If the MRTD is intended to communicate through the contact-based interface, manufacturing the physical MRTD rather consists in connecting the chip with its metallic contact interface and embedding it onto a plastic card carrier, which may be later embossed, printed or physically modified in other ways. Independently from the specific carrier for the MRTD and the process to fabricate it, all these operations have in common that they run the MRTD Embedded Software only for identifying and tracing the TOE, and that this action does not require any particular authentication procedure from the TOE. This is what characterizes the manufacturing of the physical MRTD.

Pre-personalizing the MRTD's chip involves (1) loading the code of the TL ICAO LDS in EEPROM if it is not already present in the mask; (2) creating an instance of the applet and preventing its removal; (3) performing other content management operations on the ID Platform, such as loading other applets, restricting MRTD content management, writing CPLC audit logs, stepping forward the TOE life cycle state; etc. These operations have in common that they interact with the MRTD's chip and request mandatory authentication from the TOE. Some of the TSF are enabled during the creation of the applet instance.

Although the Physical MRTD Manufacturing and the pre-personalization of the MRTD's chip correspond to two processes that are very different in nature, in practice their steps may be highly interleaved and performed by several different actors. For example, a possible MRTD Manufacturing scenario could involve three different actors:

1. Actor A1, in charge of manufacturing the inlays, pre-personalizing the platform, and delivering the resulting inlays to a second actor.
2. Actor A2, in charge of loading TL ICAO LDS, creating the instance of it, preventing its removal and the loading of any other applet, putting the resulting inlays into a passport cover, and delivering the covers to a third actor.
3. Actor A3, in charge of attaching the cover to a pre-printed booklet, assigning passport numbers to the booklets and punching each booklet with the corresponding number, and finally storing this number into the Logical MRTD.

In this example, all the three actors embody in turn both the role of MRTD's Chip Pre-Personalizer and Physical MRTD Manufacturer.

The reference [DEL] provides generic guidelines which explain how the TOE shall be managed and delivered during MRTD Manufacturing.

3.3.3 MRTD Personalization

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

If the passport number was already punched on the booklet during the MRTD Manufacturing Phase, its number may be retrieved from the Logical MRTD, checked and included in the enrolment information database in order to simplify the personalization process. If the booklet has not been punched yet, then it is done in this step

The signing of the Document security object by the Document signer is a key part of the personalization of the genuine MRTD for the MRTD holder. This signature attests that all the loaded data is correct and does match the MRTD holder.

TL ICAO LDS is personalized following the EMV Command Personalization process, which is based on GlobalPlatform specifications. Before issuing the passport, the Personalization Agent may optionally perform some other management operations on the ID Platform, such as replacing transport key by diversified ones, updating audit information records, disabling the downloading of further applets on the ID Platform, updating its life cycle state, etc. Furthermore, if the ID Platform is used just as the runtime for a fixed set of ID applications, the Personalization Agent may optionally disable any further card management action at this point by shifting the ID Platform to the native mode, in which the Issuer Security Domain cannot be selected anymore.

The Applet Developer provides the Personalization Agent with the administration guidance [ADM], which provides security recommendations regarding the personalization of TL ICAO LDS.

Once the personalization process is completed, the personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

3.3.4 MRTD Operational Use

The TOE is used as MRTD chip by the traveler and the inspection systems in the Operational Use phase. The data validated by the Document Signer can be read according to the security policy of the Issuing State or Organization but they can never be modified. Only CVCA certificates can be updated, using the EAC mechanism.

No actor, including the Personalization Agent, is allowed to add more data on the Data Groups of the MRTD during the operational phase or to delete the personalized instance of the TL ICAO LDS.

If other applets apart from the TL ICAO LDS are installed on the ID Platform, the TOE may provide additional services through them, such as electronic driving licenses, electronic signature, access control badges, etc.

If ID Platform management has not been disabled in a previous phase of the MRTD's life cycle, the MRTD Administrator is allowed to perform the management operations defined in [VGP] on it. The TOE also includes means to restrain some of these operations, such as definitely disabling the downloading of additional applets, restricting the number of instances of some applets, etc.

The Platform Developer provides the MRTD Administrator with the administration guidance [PFADM], which contains security recommendations regarding ID Platform management. The Applet Developer provides the Issuing State and Organization with the user guidance [USR], which contains security recommendations regarding the inspection of an MRTD, and particularly how to securely access to the biometric data stored in it. Potentially, any Receiving States could be also interested in a (light) public version of this document that should be taken into consideration when inspecting a passport from the Issuing State and Organization.

3.3.5 MRTD Termination

Upon special events such as expiration of passport validity period, the MRTD Administrator may shift the TOE to a terminated state, in which it cannot longer be used as an MRTD. In this state, only read access on the audit records of the ID Platform is allowed.

In order to terminate the MRTD, the MRTD Administrator applies the guidelines defined in [ADM].

3.4 Limits of the TOE

This section specifies the components of the smart card that form the Target of Evaluation, and the phases of its life cycle that fall under the scope of the evaluation.

3.4.1 Evaluated life cycles

The following table shows which TOE life cycle states fall into the scope of this evaluation, and what are the assurance families that apply to each of them:

TOE Life Cycle	Assurance Measure
Development	ACM, ALC, COMP
IC Manufacturing	AGD_PRE
Physical MRTD Manufacturing	AGD_PREL
MRTD's chip Pre-Personalization	AGD_PRE
MRTD Personalization	AGD_PRE
MRTD Operational Use	AGD_OPE
MRTD Termination	AGD_OPE

Table 1: Evaluated TOE life cycles

The MRTD's chip, especially with regard to AVA_VLA, is evaluated in the Operational Phase.

3.4.1.1 ID Platform Configuration

The ID Platform underlying TL ICAO LDS has several optional features that may be configured during the IC Manufacturing Phase. The optional features that shall be mandatory fixed to a specific value are the ones detailed in the so-called "CC configuration" defined in [PFIGS]. All the platform configurations resulting from assigning any of the possible values to the other optional features do fall into the evaluation scope.

The optional features of TL ICAO LDS that shall be fixed to a specific value are listed in [ADM]. All the configurations resulting from assigning any of the possible values to the other TL ICAO LDS optional features do fall into the evaluation scope.

3.4.2 Features excluded from the evaluation

The scope of the TOE is defined in §3.1. This section provides further details and precision on what is not included in the TOE.

3.4.2.1 Applications

Any Java Card applet different from TL ICAO LDS is excluded from the scope of the TOE, and considered as data managed by the ID Platform. This means that any application-specific TSF not included in [PPEAC] is out of the scope of this Security Target Lite. Moreover, the requirements in this Security Target Lite do not span (actually, they do not need to span) all the stages in the development cycle of a Java Card application. Applets installed in the ID Platform are only considered in their CAP format, and the process of compiling the source code of an application and converting it into the CAP format does not concern the TOE or its environment. On the other hand, the processes of verifying CAP files and loading them on the card are a crucial part of the TOE environment and play an important role as a complement to some of the on-card security functions. For this reason, this Security Target

Lite requires the enforcement of organizational security policies regarding those activities, and imposes security functional requirements on the implementation of the bytecode verifier.

Any native application (that is, not written in Java Card) that could be embedded in ROM with the code of jTOP chip is also out of the scope of the TOE. Native applications are considered as being part of the TOE IT environment. This Security Target Lite assumes that they are harmless with respect to all the security policies of the platform.

3.4.2.2 Supplementary logical channels and Remote Method Invocation

The Java Card platform underlying the TL ICAO LDS has been designed to support a configurable number of logical channels, which can be set up during the initialization phase of its manufacturing process. For the sake of the evaluation, it is assumed that the MRTD Manufacturer initializes the TOE so that one single logical channel can be opened at most. Similarly, although the underlying Java Card platform does support Remote Method Invocation from the terminal, this mechanism is excluded from the scope of evaluation. This means that the Verification Authority is expected to deny the loading of any applet relying on this mechanism.

4 Security Problem Definition

This section describes the threats, assumptions and organizational security policies that define the security problem to be addressed.

4.1 Assets

The TOE assets to be protected are those defined in [PPEAC].

Asset	Operation
Logical MRTD Data	None
Logical MRTD standard User Data	None
Logical MRTD sensitive User Data	None
Authenticity of MRTD's chip	None

Table 2: Operations on the assets introduced in the PP

4.2 Subjects

The TOE is an open platform compliant with GlobalPlatform, which may host several applet instances. Consequently, the following subjects are added in this Security Target Lite to the ones defined in [PPEAC]:

Issuer Security Domain. The ISD is a distinguished applet that acts as the on-card representative of the MRTD Administrator. When the MRTD Administrator has to perform a management operation such as loading a new applet, performing an MRTD life cycle transition, etc., it selects this applet and sends GlobalPlatform commands to it.

Applet Instances: Other applet instances different from the TL ICAO LDS and the ISD that the MRTD Administrator could have created on the ID Platform. These applets act on behalf of the Application Provider that developed them. Even though the installation of new applets and the creation of new applet instances require the authentication of the external user through a cryptographic protocol, the attacker could try to defeat such protocol, in order to install malicious code on the ID Platform. For this reason other applet instances should be considered as potentially hostile with respect to TL ICAO LDS.

4.3 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used. They come either from [PPEAC] or from the platform's security target [PFASE].

4.3.1 Assumptions from the Protection Profile

All the assumptions made in [PPEAC] are also supposed in this Security Target Lite without any modification.

Assumption	Operation
A.Pers_Agent	None
A.Insp_Sys	None
A.Signature_PKI	None
A.Auth_PKI	None

Table 3: Operations on the assumptions introduced in the PP

4.3.2 Assumptions from the Platform's Security Target

The following assumptions were made for evaluating jTOP. They are assumed for any other applet installed on the MRTD's chip:

A.NATIVE: Any native application (that is, not written in Java Card) masked in the MRTD's chip is assumed to be compliant with TL ICAO LDS so as to ensure that security policies and objectives described herein are not violated.

A.VERIFICATION: Any Executable File different from TL ICAO LDS that is masked on the MRTD's chip has successfully passed the Bytecode Verification process and has not been modified after being verified. Moreover, such files only contain applets that follow the security recommendations stated in [PFUSR].

A.APPLET: Any Executable File loaded in the MRTD's chip does not contain native code.

Application note: The above mentioned assumptions aim to exclude from the security problem definition the case in which an unevaluated piece of native code not included in the TOE could be used to bypass the applet isolation enforced by the Java Card Firewall.

Application note: The A.MANUFACTURING assumption introduced in [PFASE] is covered by the P.Manufact Organizational Security Policy in [PPEAC], and is therefore not repeated.

4.4 Threats

All the threats menacing the TOE are the ones introduced in [PPEAC]. Table 4 specifies the operations performed on them (no modification). No additional threats are introduced for the TOE in this Security Target Lite.

Threat	Operation
T.Chip_ID	None
T.Skimming	None
T.Read_Sensitive_Data	None
T.Forgery	None
T.Counterfait	None
T.Abuse_Func	None
T.Information_Leakage	None
T.Phys_Tamper	None
T.Malfunction	None

Table 4: Operations on the threats introduced in the PP

4.5 Organizational Security Policies

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

4.5.1 Policies from the Protection Profile

The TOE environment shall enforce all the Organizational Security Policies defined in [PPEAC].

Organization Security Policy	Operation
P.Manufact	None
P.Personalization	None
P.Personal_Data	None
P.Sensitive_Data	None

Table 5: Operations on the OSP introduced in the PP

4.5.2 Policies from the Platform's Security Target

The following Organizational Security Policies introduced in [PFASE] also apply to this Security Target Lite. For the sake of readability, the policies in [PFASE] have been slightly rephrased in order to use the terminology introduced in [PPEAC]. Please refer to §12 for the correspondence between the roles used in that document and the ones introduced in this Security Target Lite.

P.VERIFICATION Bytecode verification.

Before loading an Executable Load File on the MRTD, the Verification Authority checks that the Executable File successfully passes bytecode verification using Export Files that match the Executable Files that are already installed on the MRTD. Upon successful verification of an Executable Load File, all the roles involved in MRTD content management immediately activate all the IT and organizational measures required for preventing any modification of it until it is downloaded into the MRTD. If the MRTD Manufacturer has configured the ID Platform to verify DAP signatures, then the Verification Authority electronically signs the file immediately after successful verification.

If this feature has not been activated, the Verification Authority transmits the Executable Load File to the MRTD Administrator through a secure communication channel ensuring the origin and the integrity of transmitted files. Upon reception, the MRTD Administrator stores the Executable File in its secure environment until the file is downloaded into the MRTD.

Application note: Bytecode verification ensures that MRTD security will not be endangered by the installation of other, potentially malicious applets on the ID Platform. New applets may be downloaded on the MRTD at any time, even during the MRTD Operational Phase. The Verification Authority is the role in charge of performing bytecode verification. The MRTD Administrator is in charge of transmitting the applet code to the MRTD. When the applet is loaded during the MRTD Manufacturing Phase, this latter role is embodied by the MRTD's Chip Pre-Personalizer

P.FILE-ORIGIN Applet Loading on the ID Platform

The MRTD's Chip Pre-Personalizer and the MRTD Administrator are the only roles that have access to the keys required for securely transmitting Executable Files to the ID Platform. If the TOE has not been configured to enforce DAP verification, the Executable Files that these roles transmit to the MRTD have been previously validated by the Verification Authority, and not modified afterwards.

P.PREPARATION MRTD Preparation

Before reaching the Operational Phase, the MRTD is under the physical control of the MRTD Manufacturer and the Personalization Agent, and is only used in a secure environment. Once the MRTD reaches the Operational Phase, it is placed under the administrative control of the MRTD Administrator, who is the only role responsible for modifying its content. The MRTD is issued to the MRTD Holder only after reaching the SECURED life cycle state described in GlobalPlatform's specifications.

Application note: This policy corresponds to OSP.PERSONALIZATION in [PFASE].

As the scope of this TOE includes TL ICAO LDS, the OSP.SECRETS and OSP.KEY-LENGTH policies defined in [PFASE] become security functional requirements for the TOE in this Security Target Lite. The OSP.PROCESS-TOE policy in [PFASE] is covered by P.Personalization in [PPEAC].

4.5.3 Policies Required for the Composition

The following Organizational Security Policies are specific to this Security Target Lite:

P.APPLET-INSTALL Installation of TL ICAO LDS.

When creating an instance of TL ICAO LDS, the MRTD's Chip Pre-Personalizer sets the installation parameters required to activate at least the following security features: (1) Basic Access Control, (2) Active Authentication, (3) Extended Access Control, (4) mandatory authentication of the Personalization Agent during personalization and (5) load key values encrypted. In addition to this, No Access Control (NAC) shall be disabled. The MRTD's Chip Pre-Personalizer also performs some MRTD management operations that prevent the other actors from intentionally or accidentally deleting the TL ICAO LDS instance to be used as an electronic passport.

P.MRTD-TRACEABILITY Disabling traceability information

The Personalization Agent definitely disables the access to any unique data used for management purposes that the MRTD's chip could return in clear text, including the key

diversification data enabling the Personalization Agent to derive the MRTD's Personalization Keys from a master key. After having successfully personalized the MRTD chip, the Personalization Agent ensures that the transport keys that the MRTD Manufacturer placed in the MRTD's chip have been replaced by new secret ones, which shall only be known by the MRTD Administrator. Before allowing the installation of other applets on the ID Platform, the Verification Authority launches an evaluation procedure in order to determine that they do not transmit information through the contactless interface that could be used to uniquely identify the MRTD.

Application note: In a fully open MRTD, the information that is released before authentication is a global property which does not only concern the sole e-passport application. Indeed, it is not enough that TL ICAO LDS or the underlying ID Platform do not leak unique identifiers: all the applets installed on the MRTD which communicate through the contactless interface should also comply with this specific requirement. The Verification Authority is responsible for ensuring that applets that fall out of the scope of the TOE cannot be used to realize the T.Chip_ID threat. In order to cope with this property in a fully open MRTD, the Verification Authority shall launch an evaluation procedure which analyzes the code of any additional applet before loading it on the MRTD, in order to check whether it satisfies the expected privacy constraints. In particular, the Verification Authority shall ensure that the applets installed in the MRTD satisfy the requirements FIA_UID.1 and FIA_UAU.1 in [PPEAC]

Defining which precise institution should embody the Verification Authority role and how this institution should organize the analysis of the privacy requirements is up to each Issuing State, and exceeds the scope of this document. Even though no mandatory recommendations is provided on the way of organizing such procedure, this Security Target Lite strongly advocates for implementing it in the framework of the Common Criteria standard. Further details on how this can be achieved are provided in chapter 5 of [ADM].

5 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

5.1 Security Objectives for the TOE

5.1.1 Security objectives from the Protection Profile

All the security objectives for the TOE defined in [PPEAC] are part of this Security Target Lite.

Threat	Operation
OT.AC_Pers	None
OT.Data_Int	None
OT.Data_Conf	None
OT.Sens_Data_Conf	None
OT.Identification	None
OT.Chip_Auth_Proof	None
OT.Prot_Abuse-Func	None
OT.Prot_Inf_Leak	None
OT.Prot_Phys-Tamper	None
OT.Prot_Malfunction	None

Table 6: Operations on the TOE security objectives introduced in the PP

Application note: Notice that the OT. Prot_Inf_Leak and OT.Prot_Phys-Tamper security objectives correspond to the homonym security objectives introduced in [PFASE].

5.1.2 Security objectives from the Platform

The following security objectives introduced in [PFASE] also support the objectives defined in [PPEAC]:

OT.FIREWALL: Applet isolation .
The other applet instances installed on the ID Platform shall not be able to read or write the logical MRTD data or the TSF data used by TL ICAO LDS.

Application note: This security objective supports OT.Data_Integ and completes OT.Data_Conf. TL ICAO LDS runs on an open ID Platform that could embed other applets designed to provide completely different services. The ID Platform shall therefore have been designed so that there is no possible interaction between the TL ICAO LDS instances and instances of other applets that could result in the disclosure or the corruption of the logical MRTD data, or any other data that supports the TSF described in this Security Target Lite. The security objective above is just a refinement for the TL ICAO LDS of the generic objective O.FIREWALL introduced in [PFASE].

5.2 Security Objectives for the TOE Environment

5.2.1 Security objectives from the Protection Profile

All the security objectives for the environment defined in [PPEAC] applies to the environment of the TOE.

Security Objective	Operation
OD.Assurance	None
OD.Material	None
OE.Personalization	None
OE.Pass_Auth_Sign	None
OE.Auth_Key_MRTD	None
OE.Authoriz_Sens_Data	None
OE.Exam_MRTD	None
OE.Passive_Auth_Verif	None
OE.Prot_Logical_MRTD	None
OE.Ext_Insp_Systems	None

Table 7: Operations on the SO for the TOE environment introduced in the PP

5.2.2 Security objectives from the Platform

The following security objectives for jTOP's environment introduced in [PFASE] are also objectives for the environment of the TOE:

- OE.VERIFICATION
- OD.NATIVE
- OE.APPLETS
- OD.NO-RMI-APPLETS
- OD.MANUFACTURING

Application note: Following recommendations from the French Certification Scheme, the OE.KEY-LENGTH objective introduced in [PFASE] request the Verification Authority to check that the applets installed on the platform do not use key lengths that could be too short for the current state of the art in cryptography. The evaluated configuration of TL ICAO LDS does meet the key lengths recommended in OE.KEY-LENGTH. Other applets fall out of the scope of this Security Target Lite. Therefore, OE.KEY-LENGTH is not necessary as an objective for the TOE environment.

OD.SECRETS-DAP When the TOE is configured to enforce DAP verification, the TOE IT Environment shall protect the secrecy of the private DAP Verification Key.

Application note: The objective above refines OD.SECRETS in [PFASE]. The other platform's keys and secrets mentioned in OD.SECRETS are subsumed by the objectives OD.Assurance and OE.Pass_Auth_Sign in [PPEAC].

5.2.3 Security objectives required for the composition

The TOE environment shall satisfy the following security objectives for the soundness of the evaluation by composition:

OD.PRE-PERSONALIZATION Installation of TL ICAO LDS.

The MRTD's Chip Pre-Personalizer shall configure TL ICAO LDS's optional features to support Basic Access Control, Chip Authentication and Terminal Authentication. This role shall also perform the MRTD management operations required to disable the replacement of the genuine LDSApplet by another one.

OD.PLATFORM-IDENTIFICATION Disabling platform traceability

The Personalization Agent shall restrict read access to any unique data used for management purposes that the MRTD's chip could return in clear text and replace the MRTD transport keys by new secret ones, which shall only be known by the MRTD Administrator. The MRTD Administrator shall not re-enable access to such data during the Operational Phase of the MRTD.

OE.APPLETS-IDENTIFICATION Identification through other applets.

Any other applet installed on the ID Platform shall identify itself through the contactless interface only to a successful authenticated Inspection System .

6 Security Functional Requirements for the TOE

6.1 Security Functional Requirements from the Protection Profile

Table 8 specifies the Common Criteria operations performed on the security functional requirements coming from [PPEAC]. All the requirements which are not drawn from CC Part 2 are marked in italics and introduced in [PPEAC].

Security Functional Requirement	Operation
FAU_SAS.1	None
FCS_CKM.1/KDF_MRTD	None
FCS_CKM.1/DH_MRTD	Iteration / Assignment
FCS_CKM.4/MRTD	Assignment
FCS_COP.1/SHA_MRTD	Iteration / Assignment
FCS_COP.1/TDES_MRTD	None
FCS_COP.1/MAC_MRTD	None
FCS_COP.1/SIG_VER	Assignment
FCS_RND.1/MRTD	Assignment
FIA_UID.1	None
FIA_UAU.1	None
FIA_UAU.4/MRTD	None
FIA_UAU.5/MRTD	Refinement
FIA_UAU.6/MRTD	None
FIA_AFL.1	Assignment
FIA_API/CAP	None
FDP_ACC.1	None
FDP_ACF.1	None
FDP_UCT.1/MRTD	None
FDP_UIT.1/MRTD	None
FMT_SMF.1/MRTD	None
FMT_SMR.1	None
FMT_LIM.1	None
FMT_LIM.2	None
FMT_MTD.1/INI_ENA	None
FMT_MTD.1/INI_DIS	None
FMT_MTD.1/CVCA_INI	Assignment
FMT_MTD.1/CVCA_UPD	None
FMT_MTD.1/DATE	None
FMT_MTD.1/KEY_WRITE	None
FMT_MTD.1/CAPK	Assigned
FMT_MTD.1/KEY_READ	None
FMT_MTD.3	None
FPT_EMSEC.1	Assignment
FPT_TST.1	Assignment
FPT_PHP.3	None

Table 8: Operations on the SFR introduced in the PP

Application note: The FIA_UID.1 and FIA_UAU.1 requirements list the actions that can be performed before identifying and authenticating a TOE external user. One of these actions

concerns establishing a communication channel with the MRTD. In the TOE, the MRTD is a multi-application device, so establishing a communication channel with it does not only involve receiving the ATS or ATR (as mentioned in the §154 of [PPEAC]), but also selecting the LDSApplet instance containing the logical MRTD among all the applets installed in the ID Platform. Hence, the action "*selecting an applet instance on the card*" specified in FIA_UID.1-SC of [PFASE] shall be understood as being part of the action "*to establish a communication channel*" specified in [PPEAC].

Application note: The requirements FPT_SEP.1 and FPT_RVM.1 in [PPEAC] have been removed from the version v3.1 of the Common Criteria standard. They are therefore not considered in this Security Target Lite. The depency on ADV_SPM.1 does neither apply, as there is no security policy model for EAL4 evaluations in version 3.1 of Common Criteria. The rules in FDP_ACF.1 already provide a detailed access control policy that stand for an informal SPM.

The rest of this section describes the security functional requirements resulting from the operations specified in Table 8.

6.1.1 Cryptographic Support

All the security functional requirements for the TOE regarding the FCS class just rephrase the corresponding ones introduced in [PFASE] for jTOP.

FCS_CKM.1/DH_MRTD/PKCS#3 Diffie-Hellman Keys by the MRTD

FCS_CKM.1/DH_MRTD/ECDSA. The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant with ISO 15496 and specified cryptographic key sizes (192, 224 and 256 bits) that meet the following: [20], Annex A.1 8.

Application note: The TOE shall use the certified key agreement algorithms provided by jTOP. In [PFASE], the requirements regarding key agreement algorithms are specified through instances of the FCS_CKM.2 family, as they are considered as a means for distributing a key to the terminal. The above mentioned requirement corresponds to FCS_CKM.2-APP-DH-EC in [PFASE].

FCS_CKM.4/MRTD Cryptographic key destruction by the MRTD

FCS_CKM.4.1-MRTD The TSF shall destroy cryptographic keys in accordance with the cryptographic key destruction method specified below that meets the following: none.

1. The TOE shall destroy the Document Basic Access Keys of the MRTD and the Triple DES encryption key and the Retail-MAC message authentication keys for secure messaging upon closing the secure channel with the Inspection System.
2. The TOE shall destroy the Triple DES session keys S-ENC, S-MAC and S-DEK specified in §E of [GPCS] upon closing a secure channel with the Personalization Agent.
3. When destroying a key, the TOE shall reset the internal state of the key to a "not initialized" state that prevents its use, and update the key value with a randomly chosen number.

Application note: The point (3) above corresponds to the FCS_CKM.4.1-KD security functional requirement key in [PFASE], which specifies the key destruction method enforced by jTOP

FCS_COP.1/SHA_MRTD Hash for Key Derivation by MRTD

FCS_COP.1/SHA_MRTD/BAC_CA The TSF shall perform hashing in accordance with a specified cryptographic algorithm (SHA-1) and cryptographic key sizes (none) that meet the following: FIPS 180-2.

Application Note: This hashing algorithm is used for deriving the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism. The mechanism for deriving Chip Authentication session keys also uses SHA-1.

FCS_COP.1/SHA_MRTD/TAP The TSF shall perform hashing in accordance with a specified cryptographic algorithm (SHA-224 or SHA-256) and cryptographic key sizes (none) that meet the following: FIPS 180-2.

Application Note: This hashing algorithm is used for implementing the Terminal Authentication Protocol. For this protocol, the TOE shall use the certified message digest primitive provided by jTOP. The requirement above is a rephrasing of the FCS_COP.1-APP-SHA security functional requirement introduced in [PFASE].

FCS_COP.1/SIG_VER Signature Verification by MRTD

FCS_COP.1/SIG_VER/RSA The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm (Rivest-Shamir-Adleman algorithm) and cryptographic key sizes (1536 to 2048 bits) that meet the following: PKCS#1 v1.5.

Application note: The TOE shall use the certified RSA signature verification algorithm provided by jTOP. The requirement above is a rephrasing of the FCS_COP.1-APP-RSA security functional requirement introduced in [PFASE].

FCS_COP.1/SIG_VER/ECDSA The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm (Elliptic Curves Digital Signature Algorithm) and cryptographic key sizes (192, 224 and 256 bits) that meet the following: ISO-15946-1 and ISO-15946-2.

Application note: The TOE shall use the certified ECDSA signature verification algorithm provided by jTOP. The requirement above is a rephrasing of the FCS_COP.1-APP-EC security functional requirement introduced in [PFASE].

FCS_RND.1/MRTD Quality metric for random numbers

FCS_RND.1/MRTD The TSF shall provide a mechanism to generate random numbers that meets the STANDARD security level specified in [DCSSI2791].

Application note: The TOE shall use the certified random number generator provided by jTOP. The requirement above is a rephrasing of the FCS_RND.1-APP security functional requirement introduced in [PFASE].

6.1.2 Multiple Authentication Mechanisms

FIA_UAU.5/MRTD Multiple authentication mechanisms

FIA_UAU.5.1/MRTD The TSF shall provide Basic Access Control Authentication Mechanism, Terminal Authentication Protocol, Secure messaging in MAC-ENC mode, Symmetric Authentication Mechanism based on Triple-DES to support user authentication.

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

1. The TOE accepts the authentication attempt as Personalization Agent only by means of the Symmetric Authentication Mechanism with Personalization Agent Key,

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

3. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging with the key agreed upon with the authenticated terminal by means of the Basic Access Control Authentication Mechanism.

4. After run of the Chip Authentication Mechanism the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.

5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism.

6.1.3 Authentication Failure Handling

FIA_AFL.1/SGN Authentication Failure Handling

FIA_AFL.1/SGN The TSF shall detect when an administrator configurable positive integer within 1 and 255 unsuccessful authentication attempts occur related to signature verification.

FIA_AFL.2/SGN When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall increase the response time by an administrator configurable positive delay in milliseconds before returning any answer to the terminal.

6.1.4 Security Management

FMT_MTD.1/CVCA_INI Initialization of CVCA Certificate and Current Date

FMT_MTD.1/CVCA_INI The TSF shall restrict the ability to write the initial Country Verifying Certification Authority Public Key, the initial Country Verifier Certification Authority Certificate and the initial Current date to the Personalization Agent.

FMT_MTD.1/CAPK Chip Authentication Private Key

FMT_MTD.1/CAPK The TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent.

FPT_EMSEC.1/ TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit electromagnetic emissions or variations in the time or power consumption required to process an APDU command in excess of levels that could be measured or analyzed in the current state of the art enabling access to Personalization Agent Authentication Key and Chip Authentication Private Key and none.

FPT_EMSEC.1.2 The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Authentication Key and Chip Authentication Private Key and none.

FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

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

6.2 Security Functional Requirements for additional features

This section specifies requirements regarding other security mechanisms that are not specified in [PPEAC] but which are also supported by the TOE.

FIA_API.1/AAP Authentication Proof of Identity using Active Authentication

FIA_API.1.1/AAP The TSF shall provide an Active Authentication Protocol according to [5] to prove the identity of the TOE.

Application note: In addition to the Chip Authentication mechanism required in [PPEAC] to prevent from cloning the MRTD, the TOE also supports the standard Active Authentication mechanism specified by ICAO in [5]. This mechanism may be optionally activated during the MRTD's Chip Pre-Personalization phase.

FCS_COP.1/AA Cryptographic Operation for Active Authentication

FCS_COP.1/AA The TSF shall perform digital signature generation in accordance with a specified cryptographic algorithm (Rivest-Shamir-Adleman algorithm) and cryptographic key sizes (1536 to 2048 bits) that meet the following: ISO9796-2, scheme 1.

Application note: For Active Authentication, the TOE shall use the RSA certified signature generation algorithm provided by jTOP. This requirement is a refinement of the FCS_COP.1-APP-RSA security functional requirement introduced in [PFASE].

6.3 Security Functional Requirements from the Platform

This section specifies the Security Functional Requirements from [PFASE] that contribute to support the security objectives for the TOE.

6.3.1 Cryptographic requirements regarding MRTD Personalization

The following Security Functional Requirements from [PFASE] contribute to support the objective regarding access control for the personalization of the logical MRTD:

- FCS_CKM.1-SCP-SESSION-KEYS
- FCS_CKM.2-SCP-SESSION-KEYS
- FCS_COP.1-SCP/FULL
- FCS_COP.1-SCP02/FINAL
- FCS_COP.1-SCP02/ECB
- FCS_MSA.2-KEYS

Application note: The Personalization Agent uses GlobalPlatform's SCP02 protocol provided by jTOP to open a secure channel with the MRTD's chip. The above mentioned requirements specify the cryptographic algorithms that the MRTD shall use for (1) generating the SCP02 session keys that satisfy FIA_UAU.4/MRTD, (2) implicitly communicating these keys to the Personalization Terminal, (3) authenticating the external user as the Personalization Agent, (4) ensuring the origin and integrity of the APDU messages received from the Personalization Terminal and (5) ensuring the confidentiality of the loaded keys. The FCS_MSA.2-KEYS requirement satisfies the dependencies for the previous ones.

Application note: As it is obvious from its name and from the application notes in [PFASE], the FMT_MSA.2-KEYS requirement in that Security Target Lite shall be understood as the following instantiation of the text specified for FMT_MSA.2 in version v3.1 of Common Criteria: "*The TSF shall ensure that only secure values are accepted for key's attributes*". The attributes of a key are its length, type, associated algorithm and value. They are considered sure when the sender has been authenticated as the Personalization Agent. The statement of the other security functional requirements listed above is the same both in versions v2.3 and v3.1 of Common Criteria.

6.3.2 Requirements regarding a multi-application MRTD

The following Security Functional Requirements from [PFASE] contribute to support the objective regarding the protection of the logical MRTD from any malicious applet that the attacker could fraudulently download on the ID Platform:

- FDP_ACC.2-FIREWALL,
- FDP_ACF.1-FIREWALL,
- FDP_IFC.1-JCVM,
- FDP_IFF.1-JCVM,
- FMT_MSA.2-JCRE,
- FMT_MSA.3-FIREWALL,
- FMT_SMR.1-JCRE,

- FMT_MTD.1-JCRE,
- FMT_MSA.1-JCRE,
- FMT_SMF.1-FIREWALL

Application note: The security functional requirements listed above specify the access and information flow control policies of the Java Card Firewall. These policies contribute to enforce the isolation between the data spaces of TL ICAO LDS and the other applets installed on the ID Platform.

Application note: According to the rationale between SFR and TSS provided in [PFASE], the FMT_MSA.2-JCRE requirement in that Security Target Lite shall be understood as the following instantiation of the text specified for FMT_MSA.2 in version v3.1 of Common Criteria: "*The TSF shall ensure that only secure values are accepted for the Firewall security attribute Selected Applet Instance*". The statement of the other security functional requirements listed above is the same both in versions v2.3 and v3.1 of Common Criteria.

7 TOE Summary Specification

This section introduces the TOE Security Functions (TSF) and relate them to the Security Functional Requirements defined in §6.

7.1 Secure Messaging with a Personalization Terminal

This TSF enforces the origin, integrity and confidentiality of the data received from a Personalization Terminal during the MRTD Personalization Phase.

This TSF may be configured in two different modes during the instantiation of the TL ICAO LDS. In the first mode, which is intended for personalization under secure premises, the TOE leaves the Personalization Terminal to negotiate what cryptographic protections shall be attached to personalization data transmitted to the MRTD chip among three possible increasing options: (1) confidentiality protections only for the private keys loaded on the MRTD; (2) additional integrity protections for all transmitted data, and (3) both integrity and encryption protections for all transmitted data. In the second mode, which is intended for personalization within an insecure environment, the TOE enforces the option (3): all personalization commands shall include cryptographic protections against both data corruption and disclosure.

Opposite to secure messaging with an Inspection System, secure messaging with a Personalization Terminal does not attach any cryptographic protection to the APDU responses sent by the MRTD's chip.

7.2 Secure Messaging with an Inspection System

This TSF enforces the origin, integrity and confidentiality of the data exchanged between the MRTD and an Inspection System during the Operational Phase.

Data origin and the integrity is ensured by attaching a MAC computed on the whole APDU using a Triple DES session key. The algorithm used to compute this MAC is the Algorithm 3 with sequence message counter and padding mode 2 specified in the ISO 9797 standard. In order to prevent command repetitions, suppressions or permutations inside a given session, the MAC computation uses a value of a sequence counter as initialization chaining vector. This counter is increased each time a new MAC is computed and initialized to a value depending on the random numbers exchanged during the Basic Access Control Authentication of the Inspection System.

Data confidentiality is ensured through the encryption of the APDU data field using Triple DES in CBC mode specified in FIPS 46-3 and in the reference [5], normative appendix 5, A.5.3.

In both cases, the key used is a 112 bits Triple DES session key derived as part of the authentication procedure (Basic Access Control Protocol or Chip Authentication Protocol). Different keys are used for computing the MAC and for encrypting the data field. These keys are different for each secure channel session. If the Inspection System supports Chip Authentication, they are replaced during the session upon successful re-authentication of the Basic Inspection System using this latter protocol.

The secure channel is closed upon any of the following events:

- The MRTD is reset.
- TL ICAO LDS is deselected (even because of a re-selection operation).
- TL ICAO LDS receives a new BAC Authentication request.
- TL ICAO LDS detects an error on the cryptographic protections attached to an APDU command received through the secure channel.

7.3 Basic Access Control Authentication Protocol

This TSF enables to authenticate a terminal as a Basic Inspection System in order to gain access to the logical MRTD.

The BAC Protocol is detailed in §E.2 of [20]. It relies on the symmetric Document Basic Access Keys (K_ENC, K_MAC) shared with the Basic Inspection System once the MRTD Holder has willingly offered his passport to the Boarder Officer. This security function prevents an attacker from skimming the information contained in the passport without the MRTD Holder authorization, as the authentication protocol requires to optically reading the MRZ information that is physically printed on the passport booklet. If BAC Authentication succeeds, the Inspection System endorses the Basic Inspection System role with regard to the File Access Control TSF defined in §7.8.

As a side effect, the protocol provides two session keys KS_ENC and KS_MAC that are subsequently used for establishing a secure channel with the Basic Inspection System; see §7.2. If the Basic Inspection System supports the Chip Authentication mechanism, these session keys are only used to protect the Chip Authentication public key. Once the Basic Inspection System has successfully re-authenticated itself using Chip Authentication, they are replaced by the (stronger) session keys resulting from this latter protocol. If the Basic Inspection System of the receiving State does not support Chip Authentication, it is assumed that its operating environment is equipped with sufficient measures against eavesdropping.

BAC Authentication is available only during the Operational Use phase of the TOE's life cycle. It is mandatory to use it before accessing the logical information contained in the MRTD's chip and before performing Chip Authentication.

7.4 Chip Authentication Protocol

This TSF enables to authenticate a Basic Inspection System as a General Inspection System in order to gain access to the logical MRTD in a potential hostile environment. It also enables to recognize the MRTD as a genuine one, issued by the Personalization Agent.

The Chip Authentication Protocol is detailed in §3.2 of [20]. Chip Authentication is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and implicit unilateral authentication of the MRTD chip. It relies on the Chip Authentication Key Pair stored in the MRTD's chip. This security function prevents an attacker from cloning the MRTD's chip by proving that it actually contains the private Chip Authentication key that the Personalization Agent stored during the Personalization Phase. This private key is stored in the MRTD secure memory and protected by both hardware and software memory encryption and checksum integrity protections, and no external interface enables to retrieve it

As the public Chip Authentication key that the MRTD returns as part of the protocol is signed in the SOD, the authenticity of the private Chip Authentication key is ensured only when the terminal performs Passive Authentication (verification of the SOD signature). If Chip Authentication succeeds, the Basic Inspection System endorses the General Inspection System role with regard to the File Access Control TSF defined in §7.8.

7.5 Active Authentication Protocol

This TSF provides an alternative method to Chip Authentication for recognizing the MRTD as a genuine one, issued by the Personalization Agent.

The Active Authentication Protocol is detailed in §D.2 of [5]. It is a challenge-response protocol which provides explicit authentication of the MRTD. It relies on the private Active Authentication key stored in the MRTD's chip. This security function prevents an attacker from cloning the MRTD's chip by proving that it actually contains the private Active Authentication key that the Personalization Agent stored during the Personalization Phase. This private key is stored in the MRTD secure memory and protected by both hardware and software memory encryption and checksum integrity protections, and no external interface enables to retrieve it.

As the public Active Authentication key that the MRTD returns as part of the protocol is signed in the SOD, the authenticity of the private Active Authentication key is ensured only when the terminal performs Passive Authentication (verification of the SOD signature).

The commands involved in the Active Authentication protocol are accepted only if they include the Secure Messaging protections requires exchanging information with a Basic Inspection System. In other words, the Basic Access Control Authentication Protocol shall be run before running the Active Authentication Protocol.

7.6 Terminal Authentication Protocol

This TSF enables to authenticate a General Inspection System as an Extended Inspection System in order to gain access to the optional biometric reference data stored in the MRTD.

The Terminal Protocol is detailed in §3.3 of [20]. It is a two move challenge-response protocol that provides explicit unilateral authentication of the inspection system. If Terminal Authentication succeeds, the General Inspection System endorses the Extended Inspection System role with regard to the File Access Control TSF defined in §7.8. The protocol makes use of data generated during the Chip Authentication Protocol, so this protocol shall be run and succeed before engaging Terminal Authentication.

The fist step of the Terminal Authentication Protocol involves transmitting to the MRTD's chip a chain of Certificate Holder Authorizations based on the PKI infrastructure specified in §2.2 of [20]. Each element of this chain specifies what are the Data Groups containing biometric data that the actor is authorized to read, and a certificate with the public key of the actor signed by the previous one. The MRTD's chip verifies that all the signatures in the chain are valid.

Each certificate also contains a validity period, defined by an effective and an expiration date. The MRTD keeps an internal current date and verifies during Terminal Authentication,

that the received certificates are still valid. As the MRTD does not have an internal clock, it approximates the current date by the most recent effective date received so far.

Terminal Authentication may be also used to update the root CVCA certificate. New root certificates are accepted only if the whole chain of signatures is correct. At most two CVCA certificates may be stored in the MRTD. The hash algorithm and/or the key length used for Terminal Authentication may be modified when during certificate update.

Current date and certificate updates are both performed atomically.

All messages are transmitted with secure messaging in encrypt-then-authenticate mode using session keys derived from Chip Authentication. Secure messaging is not affected by Terminal Authentication. The MRTD chip retains secure messaging even if Terminal Authentication fails (unless a secure messaging error occurs).

7.7 Personalization Authentication Protocol

This TSF enables to authenticate a terminal as a Personalization Terminal in order to gain write access to all the data groups of the logical MRTD.

The Personalization Authentication Protocol is GlobalPlatform's SCP02 protocol in Explicit Mode, option i=55, specified in §E of [GPCS]. If Personalization Authentication succeeds, the terminal endorses the Personalization Agent role with regard to the File Access Control TSF defined in §7.8.

7.8 Files Access Control

This TSF controls the read and write access to the information contained in the logical MRTD.

The subjects under the control of this TSF are the terminals requesting access a given file of the logical MRTD. Such terminals may endorse different roles using one of the authentication protocols described in §7.2 to §7.7. Table 9 summarizes the access control rules enforced by this TSF. It specifies the operations that are allowed for each file and role: read (r), conditional read (cr), write (w) or write only once (wo). An empty cell means that no operation is allowed at all for that role and file. Access for all the operations specified in the cell may be restricted to a given MRTD life cycle state.

Inspection System		**Life Cycle Restrictions**	**DG1**	**DG2**	**DG.3-DG.4**	**DG5 - DG16**	**SOD**
Passive	IS	Operational Phase					
BAC	IS	Operational Phase	r	r		r	r
General	IS	Operational Phase	r	r		r	r
Extended	IS	Operational Phase	r	r	cr	r	r
Personalization	IS	Personalization Phase	r/wo	r/wo	wo	r/wo	r/w
		Operational Phase					

Table 9: File Access Control TSF

The only case in which read access is conditional is when an Extended Inspection System accesses the sensitive biometric data in Data Groups 3 and 4. In this case access is

conditioned by the verification of the chain of Certificate Holder Authorizations transmitted by the terminal during the Terminal Authentication Protocol. Access to a given Data Group is granted only if all the actors of the chain have read access to it.

During the Personalization Phase, a Personalization Inspection System is allowed to write the SOD as many times as necessary. This may be used by the MRTD Manufacturer in order to store temporary information in the logical MRTD before its personalization (such as, for instance, the passport number to be used during the Personalization Phase, which is usually punched on the booklet during MRTD Manufacturing Phase). Any type of access is definitely disabled for the Personalization Agent when the MRTD shifts to the Operational Phase.

7.9 MRTD Anonymity

This TSF prevents information leakages that could be used by an attacker during the Operational Phase in order to remotely identify or trace the MRTD Holder when it carries its MRTD.

This TSF controls that the MRTD's chip does not return any data that uniquely identifies its MRTD, such as the MRTD's chip serial number or any other almost unique information stored in the audit records of the MRTD's chip, anti-collision information used for contactless protocols, key derivation data used to diversify the MRTD Administration keys from a master key, etc.

Traceability of the MRTD's chip is allowed during IC Manufacturing, MRTD Manufacturing and MRTD Personalization. Writing the CPLC audit records requires prior authentication through GlobalPlatform's SCP02 protocol using the secret keys of the Issuer Security Domain. This TSF prevents the information written in the CPLC audit records from being updated.

7.10 Bytecode Integrity

This TSF enables any MRTD user to check the integrity of TL ICAO LDS upon request.

7.11 Supporting Security Functions from the platform

The following TSF provided by the platform support the ones introduced in the previous sections of this chapter:

- Host Authentication
- Session Key Generation
- Message Confidentiality
- Message Integrity and Authentication
- ISD Key Loading and Replacement.
- Java Card Firewall
- Key Integrity
- Key Confidentiality
- Signature Generation and Verification
- Message Digest Generation
- Encryption and Decryption
- Key Agreement
- Random Number Generation
- Booting Tests

- Operating state checking
- Phase management with test mode lock-out
- Protection against snooping
- Notification of physical attack

These TSF are detailed either in §7 of [PFASE] (jTOP TSF) or in section §6 of [ICST] (integrated circuit TSF).

8 Rationales

8.1 Security Objectives Rationale

The security objectives defined in this document may be classified into three classes:

1. Security objectives from the Protection Profile [PPEAC]. These security objectives are introduced in §5.1.1 and §5.2.1;
2. Security objectives from jTOP's security target [PFASE] that contribute to counter the menaces defined in [PPEAC]. These security objectives are introduced in §5.1.2 and §5.2.2;
3. Additional security objectives for the TOE Environment for consistently composing jTOP with TL ICAO LDS. These security objectives are introduced in §5.2.3.

As this Security Target Lite does not introduce any new threat for the TOE, the security objectives coming from the evaluated Protection Profile already cover all of them. The associated rational is provided in §7.1 of [PPEAC] and is not repeated here.

This section concentrates on the coverage provided by the supporting security objectives for the TOE taken from jTOP's Security Target and the additional security objectives required for the composition of jTOP and TL ICAO LDS. Table 10 summarizes this coverage, which is detailed in the paragraphs below.

The threat **T.Chip_ID** addresses the trace of the MRTD movement by identifying remotely the MRTD chip through the contactless communication interface. The objective OD.PLATFORM-IDENTIFICATION requires the Personalization Agent to disable or restrict read access to some information provided by the ID Platform that could be used to uniquely identify the MRTD, such as GlobalPlatform's key derivation data (disabling) or the contents of the CPLC audit records (restriction to MRTD Administrator through key replacement). As the ID Platform underlying the MRTD could also provide other identification services (electronic signature applets, driver licence applets, etc), the objective OE.APPLETS-IDENTIFICATION states that the applets providing those services shall also satisfy the OT.IDENTIFICATION security objective stated for TL ICAO LDS. Finally, the OD.NO-RMI-APPLETS states that no applet on the ID Platform shall make use of RMI mechanism, as it has not been included in the evaluation scope of the platform, and could therefore include unknown means for uniquely identifying the applets that use it.

The threat **T.Read_Sensitive_Data** addresses the unauthorized access to sensitive biometric data stored in the MRTD's chip. The objective OT.FIREWALL contributes to counter that threat by preventing an attacker to access to biometric data stored by TL ICAO LDS using another applet that would be fraudulently installed on the ID Platform. The objectives OE.VERIFICATION, OE.NATIVE and OE.NATIVE support O.FIREWALL, as the Java Card Firewall is effective only against applets written in Java Card that comply with all the well-formedness rules checked during bytecode verification. Finally, the OD.NO-RMI-APPLETS states that no applet on the ID Platform shall make use of RMI mechanism, as the Firewall rules it enforces were not included in the platform's evaluation scope.

The same arguments developed for T.Read_Sensitive_Data also apply to the protection of the logical MRTD against the threat **T.Forgery**. In this case, OT.FIRWALL contributes to prevent that a malicious applet installed on the ID Platform could corrupt the logical MRTD. The objective OD.PRE-PERSONALIZATION prevents that the data groups created by the

genuine TL ICAO LDS applet could be deleted and replaced by other ones through the deletion and re-installation of this applet.

The threat **T.Counterfeit** addresses the unauthorized copy or reproduction of the genuine MRTD's chip. In an open ID platform, the code of the genuine TL ICAO LDS applet could be deleted and replaced by a fake applet. The objective OD.PRE-PERSONALIZATION prevents that by requesting the MRTD Manufacturer to disable the deletion of TL ICAO LDS. In addition to this, the TOE may be configured to accept only those applets that have been signed by the Verification Authority. The security objective OD.SECRETS-DAP supports this security mechanism by requesting the Verification Authority to protect the secrecy of the DAP private key.

The OSP **P.Manufact** requires the quality and integrity of the manufacturing process. The objective OD.MANUFACTURING refines such global requirement, introducing constraints with respect to the transport and default secret keys used during the MRTD Manufacturing and the integrity and confidentiality of the ID Platform's code.

The OSP **P.APPLET-INSTALL** requires the MRTD's Chip Pre-Personalizer to activate the security mechanisms that satisfy some of the security objectives for the TOE, and to prevent the deletion of the genuine LDSApplet. These requirements are re-stated as requirements for the TOE IT Environment in the objective OD.PRE-PERSONALIZATION.

The OSP **P.MRTD-Traceability** requires the Personalization Agent to disable those generic mechanisms present in the ID Platform that could be used to uniquely identify the MRTD. This requirement is re-stated as a requirement for the TOE IT Environment in the objective OD.PLATFORM-IDENTIFICATION, which states that other applets in the TOE IT Environment shall not enable to uniquely identify the MRTD.

	OT.FIREWALL	OE.VERIFICATION	OE.NATIVE	OE.APPLET	OD.SECRETS-DAP	OD.NO-RMI-APPLETS	OD.MANUFACTURING	OD.PRE-PERSONALIZATION	OD.PLATFORM-IDENTIFICATION	OE.APPLETS-IDENTIFICATION
T.Chip_ID						×			×	×
T.Skimming										
T.Read_Sensitive_Data	×	×	×	×		×				
T.Forgery	×	×	×	×		×		×		
T.Counterfait					×			×		
T.Abuse_Func[24]										
T.Information_Leakage4										
T.Phys_Tamper4										
T.Malfunction4										
P.Manufact							×			
P.Personalization4										
P.Personal_Data4										
P.Sensitive_Data4										
P.APPLET-INSTALL								×		
P.MRTD-TRACEABILITY									×	
A.Pers_Agent4										

[2] See the rational for this element in [PPEAC].

A.Insp_Sys4										
A.Signature_PKI4										
A.Auth_PKI4										

Table 10: Security Objectives Rationale: objectives from the Platform

8.2 Security Functional Requirements Rationale

The security functional requirements for the TOE may be classified into the following classes:

1. Security functional requirements coming from the Protection Profile [PPEAC]. These requirements are introduced in §6.1.
2. Security functional requirements corresponding to additional security features not required by the Protection Profile [PPEAC], but which are nevertheless provided by the TOE to support the security objectives defined in that Protection Profile.
3. Security functional requirements from jTOP's Security Target that support the security objectives defined in [PPEAC]. These requirements are introduced in §**Erreur ! Source du renvoi introuvable.**.

The first class of security functional requirements cover the security objectives for the TOE defined in [PPEAC] and listed in §5.1.1. The associated rational is provided in §7.2 of [PPEAC] and is not repeated here.

This section therefore concentrates only on the coverage provided by the additional security requirements and the supporting security functional requirements taken from jTOP's Security Target. Table 11 summarizes this coverage, which is detailed in the paragraphs below.

Threat	Security Functional Requirements
OT.AC_Pers	FCS_CKM.1-SCP-SESSION-KEY, FCS_CKM.2-SCP-SESSION-KEY, FCS_COP.1-SCP/FULL, FCS_COP.1-SCP02/FINAL, FCS_COP.1-SCP02/ECB, FMT_MSA.2-KEYS
OT.Data_Int[3]	
OT.Data_Conf5	
OT.Sens_Data_Conf5	
OT.Identification5	
OT.Chip_Auth_Proof	FIA_API.1/AA, FCS_COP.1/AA,
OT.Prot_Abuse-Func5	
OT.Prot_Inf_Leak5	
OT.Prot_Phys-Tamper5	
OT.Prot_Phys-Tamper5	
OT.FIREWALL	FDP_ACC.2-FIREWALL, FDP_ACF.1-FIREWALL, FDP_IFC.1-JCVM, FDP_IFF.1-JCVM, FMT_MSA.2-JCRE, FMT_MSA.3-FIREWALL, FMT_SMR.1-JCRE, FMT_MTD.1-JCRE, FMT_MSA.1-JCRE, FPT_SEP.1-FIREWALL, FMT_SMF.1-FIREWALL

Table 11: Security Functional Requirements Rationale (TOE)

The objective **OT.AC_Pers** requires the TOE to authenticate the Personalization Agent during the Personalization Phase. The cryptographic mechanisms using for authenticating such role are specified in FCS_COP.1-SCP/FULL (user authentication) and FCS_COP.1-SCP02/FINAL (message authentication). FCS_CKM.1-SCP-SESSION-KEY specifies the

[3] See the rational for this security objective in [PPEAC].

algorithm that the TOE shall use for deriving the personalization session keys. FCS_CKM.2-SESSION-KEYS specify the protocol that the Personalization Terminal and the MRTD shall use for agreeing on the same session keys. FCS_COP.1-SCP02/ECB specifies the cryptographic algorithm to be used for encrypting secret keys during the Personalization Phase. The FMT_MSA.2-KEYS is included to satisfy the dependencies on the previously mentioned requirements. It specifies that cryptographic functions shall only use security attributes (key lengths, key types, algorithms) that are appropriate for the intended operation.

The objective OT.Chip_Auth_Proof may be ensured by the Active Authentication Protocol provided by FIA_API.1/AA, which proves the identity of the TOE. The Active Authentication Protocol is based on the cryptographic algorithms specified in FCS_COP.1/AA. [PPEAC]

The objective **OT.FIREWALL** requires the TOE to prevent that other applets installed in the ID Platform could access to the logical MRTD. The access control and information flow policies listed in Table 11 are introduced in [PFASE] for controlling what applet instances are allowed to access which Java Card object (FDP_ACC.2-FIREWALL, FDP_ACF.1-FIREWALL), and how the references to shared data containers such as the APDU buffer can be transmitted between applets (FDP_IFC.1-JCVM, FDP_IFF.1-JCVM). Other security functional requirements associated to this security objective define how the security attributes and roles involved in these policies shall be managed. They are introduced for satisfying the SFR dependencies on the security policies.

9 References

9.1.1 Protection Profile Documents

The references introduced in [PPEAC] are not repeated in this Security Target Lite. Such references are noted using numbers instead of letters. For example, reference number 20 in chapter §9 of [PPEAC] is written in this Security Target Lite like this: [20].

9.1.2 Normative Documents

[CC1] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2006-09-001, Version 3.1, Revision 1, September 2006.

[CC2] *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements*, CCMB-2007-09-002, Version 3.1, Revision 2, September 2007.

[CC3] *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements*, CCMB-2007-09-003, Version 3.1, Revision2, September 2007.

[CEM] *Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology*, CEM-2007-09-004, Version 3.1, Revision 2, September 2007.

[COMP] *Composite product evaluation for smart cards and similar devices,* CCDB-2007-09-001, September 2007, Version 1.0, Revision 1*.*

[DCSSIAP09] *E-passport, understanding the EAC Protection Profile, DCSSI, Application Note 09, Version 0.3, January 22snd, 2008.*

[DCSSI2791] *Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionement des mécanismes cryptographiques de niveau de robustesse « standard »*. DCSSI, version 1.02, November 19th 2004.

[GPCS] *GlobalPlatform 2.1.1 Card Specification (March 2003), including Amandment A and Errata Precision List 1.3 (december 2004).*

[ICST] *SLE66CLX800PE-m1581-e13/a14 & SLE66CLX360PE-m1587-e13/a14 Security Target with optional libraries RSA2048 V1.5 and ECC v1.1, Version 1.2, January 9th, 2008..*

[JCAPI] *Java Card 2.2.1 Application Programming Interface, Sun Microsystems , October 2003.*

[JCRE] *Java Card 2.2.1 Runtime Environment Specification, Sun Microsystems,, October 2003.*

[JCVM] *Java Card 2.2.1 Virtual Machine Specification, Sun Microsystems, October 2003.*

[PPEAC] *Machine Readable Travel Document with ICAO application, Extended Access Control – Common Criteria Protection Profile*, BSI-PP-0026, Version 1.2, November 19th, 2008.

[PROFILE] *jTOP Platform -- Profile, Trusted Logic, CP-2007-RT-246-27/0.9/SERMA.*

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

[VCPG] *VISA GlobalPlatform 2.1.1 Card Production Guide, Version 1.01, March 2005*.

[VGP] *Visa GlobalPlatform 2.1.1 Card Implementation Requirements, Version 2.0, July 2007*.

9.1.3 Platform Documents

The following Trusted Logic's technical reports describe jTOP's assurance measures:

[PFACM]	*JCLX80jTOP20ID – Configuration Management Plan,* Trusted Logic, CP-2007-RT-017.
[PFADM]	*JCLX80jTOP20ID – Administration Guide,* Trusted Logic, CP-2007-RT-165.
[PFASE]	*JCLX80jTOP20ID – Security Target,* Trusted Logic, CP-2006-RT-389.
[PFATE]	*JCLX80jTOP20ID – Test Documentation,* Trusted Logic, CP-2007-RT-113 to -120.
[PFDEL]	*JCLX80jTOP20ID – Delivery and Operation*, Trusted Logic, CP-2007-RT-015.
[PFFSP]	*JCLX80jTOP20ID – Functional Specification*, Trusted Logic, CP-2006-RT-551 and -093.
[PFIGS]	*JCLX80jTOP20ID – Card Initialization Phase*, Trusted Logic, CP-2003-RT-52-27-1.9.
[PFUSR]	*JCLX80jTOP20ID – User Guide,* Trusted Logic, CP-2007-RT-166.
[PFVLA]	*JCLX80jTOP20ID – Vulnerability Analysis*, Trusted Logic, CP-2007-RT-121.

9.1.4 Assurance Measures Documents

The following Trusted Logic's technical reports describe the assurance measures of the TOE:

[ACM]	TL ICAO LDS – Configuration Management Plan, Trusted Logic, CP-2008-RT- 679. TF4C – Configuration Management Plan, Trusted Logic, CP-2008-RT- 680
[ADM]	TL ICAO LDS – Preparation Guide, Trusted Logic, CP-2008-RT-727.
[ATE]	TL ICAO LDS – Test Documentation, Trusted Logic, CP-2008-RT-610.
[DEL]	TF4C – Delivery and Operation, Trusted Logic, CP-2007-RT-015.
[DEV]	TL ICAO LDS – Development Security, Trusted Logic, CP-2004-NT-576.
[FSP]	TL ICAO LDS – Functional Specification, Trusted Logic, CP-2005-RT-076.
[TDS]	TL ICAO LDS – Design and Architecture, Trusted Logic, CP-2008-RT- 638
[LCD]	TF4C – Software Life Cycle, Trusted Logic, CP-2007-RT-016.
[TAT]	TL ICAO LDS – Tools and Techniques, Trusted Logic, CP-2008-RT-668.
[USR]	TL ICAO LDS – User Guide, Trusted Logic, CP-2008-RT-740.
[ARC]	TL ICAO LDS – Security Architecture, Trusted Logic, CP-2008-RT-670.

10 Acronyms

The following acronyms are used in this document:

Acronym	Meaning
AA	Active Authentication
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset
BAC	Basic Access Control
CA	Chip Authentication
CAD	Card Acceptance Device
CC	Common Criteria
CCM	Card Content Management
CPLC	Card Production Life Cycle Data
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAC	Extended Access Control
EEPROM	Electrically Erasable Programmable Read Only Memory
EMA	Electro-Magnetic Analysis
EPA	Emanation Power Analysis
GP	GlobalPlatform
ISD	Issuer Security Domain
JCAPI	Java Card Application Programming Interface
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine
jTOP	Java Trusted Open Platform
MAC	Message Authentication Code
OPEN	Open Platform Environment
OS	Operating System
PP	Protection Profile
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RTE	Run Time Environment
SCP	Smart Card Platform
SCP02	Secure Channel Protocol 02
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SPA	Simple Power Analysis
ST	Security Target
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE Security Functions
VGP	VISA GlobalPlatform

11 Glossary

Term	Definition
Applet	An application written in Java Card.
Application instance	Instance of an Executable Module after it has been installed and made selectable.
Application Protocol Data Unit (APDU)	Standard communication messaging protocol between the MRTD's chip and a Inspection System or Personalization Terminal. See ISO-7816-4.
Application Provider	The organization that owns an Application and is responsible for its behavior.
Application Session	The link between the Application and the external world during a MRTD's chip Session starting with the Application selection and ending with Application de-selection or MRTD's chip reset.
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 the Public Key is known.
Bytecode Verification	A static analysis of an Executable Module to determine whether it respects the CAP format and satisfies some essential security properties, such as the absence of pointer arithmetic, uncontrolled control jumps, data-structure overflows, etc..
MRTD's Content	Code and Application information (but not Application data) contained in the MRTD that is under the responsibility of the OPEN e.g. Executable Load Files, Application instances, etc.
MRTD Session	The period of time during which the MRTD receives power supply from the terminal without receiving a MRTD reset signal.
Card Production Life Cycle Data	A record that uniquely identifies the MRTD and the actors involved in its manufacturing and personalization.
Closed Mode	A mode in which the card restricts MRTD content management operations. When the MRTD is in the Closed Mode it rejects loading more Executable Load Files. There are two possible closed modes: Java Card Static and Native Card.
Embedded Software	The piece of executable code that is masked on the ROM and written in the EEPROM memories of the integrated circuit. It comprises the ICAO LDS

	applet and the code of jTOP.
Executable File	Actual on-card container of one or more Applets. It may reside in immutable persistent memory or may be created in mutable persistent memory as the resulting image of an Executable Load File.
Executable Load File	An Executable File that is in transit to the MRTD's chip.
Export File	A binary representation of the type and access modifiers of an Executable File in the CAP format. If B is a CAP file that imports methods or fields of a CAP file A, then the Export File of *A* contains all the information required to perform the bytecode verification of *B*.
Initialization Data	Any data supplied by the Platform Developer that is injected into the non-volatile memory of the IC by the IC Manufacturer. These data are for instance used for initializing the platform, and to enforce traceability and secure shipment between phases.
Issuer Security Domain	On-card entity providing support for the control, security, and communication requirements of the Issuer State or Organization
Java Card Platform	A collective name for all the components of the Embedded Software that transform the IC into a runtime environment for running Java Card applets.
Java Card Static	A closed mode in which no more Executable Load Files may be loaded on the MRTD's chip.
Masking Process	The process of embedding the binary code of the Operating System, the Runtime Environment, the MRTD Manager and a collection of applets into the IC chip.
Message Authentication Code (MAC)	A symmetric cryptographic transformation of data that provides data origin authentication and data integrity.
Mutable Persistent Memory	Memory that can be modified.
Native Card Mode	A closed mode in which the card behaves as a native card. GlobalPlatform commands are rejected when the MRTD is in this mode.
Open Platform Environment (OPEN)	The on-card piece of software that manages the GlobalPlatform Registry.
Platform Developer	The organization responsible for developing the code of jTOP.
Platform Personalization Data	Any data supplied relative to the Issuer State or Organization that is injected into the non-volatile memory of the MRTD's chip. These data are for instance used to personalize the platform with the Issuer State or Organization's keys, for traceability purposes, and to secure shipment between phases.

Pre-Issuance	Phase prior to the card being issued to the MRTD Holder.
Private Key	The private component of an asymmetric key pair.
Public key	The public component of an asymmetric key pair.
Secret key	A private key. In GlobalPlatform specification, this term refers to a key used to generate a Session Keys during the initiation of a Secure Channel.
Session key	A key whose lifetime is a card session. In GlobalPlatform specifications, this term refers to the key associated to a Secure Channel and which is used for a secure communication session.
Secure Channel	A communication mechanism between an off-card entity and a card that provides a level of assurance, to one or both entities.
Secure Channel Session	A session, during an Application Session, starting with the Secure Channel Initiation and ending with a Secure Channel Termination or termination of either the Application Session or Card Session.
Security Attribute	A logical entity used by a Security Policy to determine whether the outcome of a requested operation may succeed.
Security Policy	A set of rules that regulate how certain assets are managed, protected and/or distributed.
Symmetric Cryptography	A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation.

12 Equivalent Terms

This Security Target Lite relays on several public specifications (GlobalPlatform, Java Card, ICAO LDS) which sometimes uses different terms for the same concept. The following table maps the names of the terms used in this document onto the ones used in other specifications. Terms on the same line shall be considered as synonymous and may be undistinguishable used all along the Common Criteria documentation of the TOE.

This Security Target Lite	**Platform's Security Target**
MRTD	smart card (or just card)
Issuing State or Organization	Card Issuer
MRTD's Chip Pre-Personalizer	Card Enabler
Traveler	Card User
MRTD Holder	Card holder
Card Administrator	MRTD Administrator

13 Index