TL ICAO LDS-PACE/EAC Security Target LITE

Emission Date : 12-Nov.-2013
Document Type : Technical report
Ref./Version : PU-2012-RT-767-1.0-LITE
Number of pages : 88 (including two cover pages)

LEGAL NOTICE

COPYRIGHT NOTICE

DISCLAIMER OF WARRANTY

Table of contents

Table of figures

Table of tables

1 Introduction

This document is the Security Target LITE of TL ICAO LDS - PACE/EAC, 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 open platform) and the application is TL ICAO LDS – PACE/EAC (a Java Card applet) in addition to an API implemented in jTOP related to Logical Data Structure File System (LDS FS) and PACE for the use of identity applications. The Java Card platform has been evaluated according to the Security Target [PFASE].

1.1 ST Identification

Title	TL ICAO LDS - PACE/EAC Security Target
Reference	PU-2012-RT-767
Version	1.0-LITE
Author	Trusted Logic SA
Address	6 rue de la Verrerie, 92197 Meudon – France

1.2 Identification of the TOE

Commercial name	SLJ 52 Gxx yyy zL
jTOP Platform version	jTOP INFv#46
TOE version	5.7
IC identifiers	SLE78CLX1600PM-m7820-M11 SLE78CLX800P SLE78CLX360PM

The Infineon Commercial name for this product is: SLJ 52 Gxx yyy zL, where xx may take different values:

- CA: Contact Based (No Mifare)
- LA: Contactless no Mifare
- DA: Dual Interface no Mifare
- LL: Contactless with Mifare
- DL: Dual Interface with Mifare

Where yyy is the NVM size for the Customer (may take following values: 036, 080, 128, 160)

And where z is the Market segment:

- A: ePassport
- B: eDriving License
- C: National eID Open Platform
- D: National eID with Applets

1.3 Revisions and Comments

Version	Issue date	Comments
1.0-LITE	November 12th, 2013	Final version

1.4 CC Conformance

This Security Target 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 3, July 2009.
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, CCMB-2007-09-002, Version 3.1, Revision 3, July 2009.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2007-09-003, Version 3.1, Revision 3, July 2009.
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2007-09-004, Version 3.1, Revision 3, July 2009.

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

- Part 1: conformant
- Part 2: extended with the following families defined in [PPEAC] and [PPPACE]: FAU_SAS, FCS_RND, FIA_API, FMT_LIM, and 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.

1.5 PP Claims and Rationale

This security target is compliant with the following protection profiles:

1. "Common Criteria PP Machine Readable Travel Document with ICAO Application, Extended Access Control, V1.10-2009" [PPEAC].

2. "Common Criteria PP Machine Readable Travel Document using Standard Inspection Procedure with PACE, V2-2011" [PPPACE].

The conformance mode is the following:

PP	**Conformance**
PP EAC	Strict
PP PACE	Strict

Additionally, the Active Authentication Mechanism and Active Authentication keys on the TOE are included in the TOE. This implies the below augmentations.

Extension of existing SFRs for the TOE to include the Active Authentication private key:

- FIA_API.1/AA
- FMT_MTD.1/AAK_LOAD
- FMT_MTD.1/AAK_READ
- FMT_MTD.1/AARESP_READ
- FPT_EMSEC.1/AA

The TOE uses APIs from the jTOP platform related to Logical Data Structure File System (LDS FS) and PACE for the use of identity applications. This API is implemented and included in the evaluation scope.

The document [COMP] shall be used in addition to the CC part 3 [CC] and to the CEM [CEM]. This document specifies the additional information to be provided by a developer, and the additional checks to be performed by the ITSEF (Information Technology Security Evaluation Facility) when performing a "composite evaluation". This is the case for the current TOE as the underlying jTOP v46 Platform [PFASE].

This security target is compliant with the SPD of [PPEAC] and [PPPACE] as shown in the following table:

OSP	*PP EAC*	*PP PACE*	*PFASE*	*Included in this ST*
OSP.Manufact	×	×		×
OSP.Sensitive_Data	×			×
OSP.Personalization	×			×
OSP.BAC-PP	×			×
OSP.Pre-Operational		×		×
OSP.Card_PKI		×		×
OSP.Trustworthy_PKI		×		×
OSP.Terminal		×		×
OSP.APPLET-INSTALL				×
OSP.Travel_Document_TRACEABILITY				×
OSP.FILE-ORIGIN			×	×
OSP.VERIFICATION			×	×

Assumptions	*PP EAC*	*PP PACE*	*PFASE*	*Included in this ST*
A.Passive_Auth	×	×		×
A.MRTD_Manufact	×			×
A.MRTD_Delivery	×			×

Assumptions	*PP EAC*	*PP PACE*	*PFASE*	*Included in this ST*
A.Pers_Agent	×			×
A.Insp_Sys	×			×
A.Auth_PKI	×			×
A.NATIVE			×	×
A.APPLET			×	×
A.VERIFICATION			×	×

Threats	*PP EAC*	*PP PACE*	*Included in this ST*
T.Information_Leakage	×	×	×
T.Malfunction	×	×	×
T.Phys-Tamper	×	×	×
T.Forgery	×	×	×
T.Abuse-Func	×	×	×
T.Read_Sensitive_Data	×		×
T.Counterfeit	×		×
T.Eavesdropping		×	×
T.Tracing		×	×
T.Skimming		×	×

Table 1 PPs SPD vs. ST

This security target is compliant with the security objectives of **[PPEAC]** and **[PPPACE]** as shown in the following table:

Security Objectives	*PP EAC*	*PP PACE*	*PFASE*	*Included in this ST*
O.Prot_Inf_Leak	×	×		×
O.Prot_Malfunction	×	×		×
O.Data_Integrity	×	×		×
O.Prot_Abuse-Func	×	×		×
O.Prot_Phys-Tamper	×	×		×
O.Identification	×	×		×
O.AC_Pers	×	×		×
O.Sens_Data_Conf	×			×
O.Chip_Auth_Proof	×			×
O.Data_Confidentiality		×		×
O.Data_Authenticity		×		×
O.Tracing		×		×
O.FIREWALL			×	×

Security Objectives for the Operational Environment	PP EAC	PP PACE	PFASE	Included in this ST
OE.Passive_Auth_Sign	×	×		×
OE.Personalization	×	×		×
OE.Terminal		×		×
OE.Exam_MRTD	×			×
OE.Passive_Auth_Verif	×			×
OE.Prot_Logical_MRTD	×			×
OE.Authoriz_Sens_Data	×			×
OE.Ext_Insp_Systems	×			×
OE.Auth_Key_MRTD	×			×
OE.BAC_PP	×			×
OE.MRTD_ Delivery	×			×
OE.MRTD_Manufact	×			×
OE.Legislative_Compliance		×		×
OE.Travel_Document_Holder		×		×
OE.PRE-PERSONALIZATION				×
OE.PLATFORM-IDENTIFICATION				×
OE.APPLETS-IDENTIFICATION				×
OE.NATIVE			×	×
OE.SECRETS			×	×
OE.APPLET			×	×
OE.VERIFICATION			×	×

Table 2 PPs Security Objectives vs. ST

This security target is compliant with the security functional requirements of [PPEAC] and [PPPACE] as shown in the following table:

SFR	PP EAC	PP PACE	Included in ST IC or Platform	Included in this ST
FAU_SAS.1	×	×	FAU_SAS.1-IC	FAU_SAS.1/EAC_PACE
FCS_CKM.1	×	× (FCS_CKM1/DH_PACE)	FCS_CKM.1-key_generation	FCS_CKM.1/LDS
FCS_CKM.4	×	×		FCS_CKM.4
FCS_COP.1/SHA	×		FCS_COP.1-APP-SHA	FCS_COP.1/LDS
FCS_COP.1/SYM	×			FCS_COP.1/LDS

SFR	PP EAC	PP PACE	Included in ST IC or Platform	Included in this ST
FCS_COP.1/MAC	×			FCS_COP.1/LDS
FCS_COP.1/SIG_VER	×		FCS_COP.1-Asymetric	FCS_COP.1/LDS
FCS_COP.1/PACE_ENC		×		FCS_COP.1/LDS
FCS_COP.1/PACE_MAC		×		FCS_COP.1/LDS
FCS_RND.1	×	×	FCS_RND.1-APP	FCS_RND.1/EAC_PACE
FIA_UID.1	×	× (FIA_UID.1/PACE)		FIA_UID.1/EAC_PACE
FIA_UAU.1	×	× (FIA_UAU.1/PACE)		FIA_UAU.1/EAC_PACE
FIA_UAU.4	×	× (FIA_UAU.4/PACE)		FIA_UAU.4/EAC_PACE
FIA_UAU.5	×	× (FIA_UAU.5/PACE)		FIA_UAU.5/EAC_PACE
FIA_UAU.6	×	× (FIA_UAU.6/PACE)		FIA_UAU.6/EAC_PACE
FIA_API.1	×			FIA_API.1/EAC
FDP_ACC.1	×	× (FDP_ACC.1/TRM)		FDP_ACC.1/EAC_PACE
FDP_ACF.1	×	× (FDP_ACF.1/TRM)		FDP_ACF.1/EAC_PACE
FDP_UCT.1	×	× (FDP_UCT.1/TRM)		FDP_UCT.1/EAC_PACE
FDP_UIT.1	×	× (FDP_UIT.1/TRM)		FDP_UIT.1/EAC_PACE
FMT_SMF.1	×	×		FMT_SMF.1/EAC_PACE
FMT_SMR.1	×	× (FMT_SMR.1/PACE)		FMT_SMR.1/EAC_PACE
FMT_LIM.1	×	×	FMT_LIM.1-IC	FMT_LIM.1/EAC_PACE
FMT_LIM.2	×	×	FMT_LIM.2-IC	FMT_LIM.2/EAC_PACE
FMT_MTD.1/INI_ENA	×	×		FMT_MTD.1/INI_ENA
FMT_MTD.1/INI_DIS	×	×		FMT_MTD.1/INI_DIS
FMT_MTD.1/CVCA_INI	×			FMT_MTD.1/CVCA_INI
FMT_MTD.1/CVCA_UPD	×			FMT_MTD.1/CVCA_UPD
FMT_MTD.1/Date	×			FMT_MTD.1/Date
FMT_MTD.1/KEY_WRITE	×			FMT_MTD.1/KEY_WRITE
FMT_MTD.1/CAPK	×			FMT_MTD.1/CAPK
FMT_MTD.1/KEY_READ	×	×		FMT_MTD.1/KEY_READ
FMT_MTD.1/PA		×		FMT_MTD.1/PA
FMT_MTD.3	×			FMT_MTD.3
FPT_EMSEC.1	×	× (FPT_EMS.1)		FPT_EMSEC.1/EAC_PACE
FPT_FLS.1	×	×		FPT_FLS.1/LDS
FPT_TST.1	×	×	FPT_TST.1	FPT_TST.1/LDS
FPT_PHP.3	×	×	FPT_PHP.3-IC	FPT_PHP.3/EAC_PACE
FIA_AFL.1/PACE		×		FIA_AFL.1/LDS
FDP_RIP.1		×		FDP_RIP.1/LDS
FTP_ITC.1/PACE		×		FTP_ITC.1/PACE_LDS
Additional SFRs for the Active Authentication Mechanism				
				FIA_API.1/AA
				FMT_MTD.1/AAK_LOAD

SFR	PP EAC	PP PACE	Included in ST IC or Platform	Included in this ST
				FMT_MTD.1/AAK_READ
				FMT_MTD.1/AARESP_READ
				FPT_EMSEC.1/AA

Table 3 PPs SFRs vs. ST

2 Overview

2.1 Associated Documents

2.1.1 Protection Profile and Normative Documents

[CC1]	*Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 3. July 2009. CCMB-2009-07-001.*
[CC2]	*Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 3. July 2009. CCMB-2009-07-002.*
[CC3]	*Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 3. July 2009. CCMB-2009-07-003.*
[CEM]	*Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 3. July 2009. CEM-2009-07-004.*
[COMP]	*Composite product evaluation for smart cards and similar devices, CCDB-2012-04-001, April 2012, Version 1.2.*
[DCSSI2791]	*Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse « standard ». DCSSI, version 1.02, November 19th 2004.*
[GPCS]	*GlobalPlatform 2.2.1 Card Specification (January 2011), including Mapping Guidelines v1.0.1 – Implementation for mapping a GlobalPlatform card based on Card Specification 2.1.1 to a GlobalPlatform card compliant with Card Specification v2.2.1 (January 2011).*
[ICST]	*Security Target M7820 M11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox version 1.4, 2011-04-18, Infineon Technologies AG.*
[JCAPI]	*Java Card 3.0.4 Application Programming Interface, Sun Microsystems*
[JCRE]	*Java Card 3.0.4 Runtime Environment Specification, Sun Microsystems*
[JCVM]	*Java Card 3.0.4 Virtual Machine Specification, Sun Microsystems*
[PPEAC]	*Protection Profile Machine Readable Travel Document with ICAO application, Extended Access Control – Common Criteria Protection Profile, BSI-CC-PP-0056, Version 1.10, March 25th, 2009.*

[CC1]	*Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 3. July 2009. CCMB-2009-07-001.*
[PPPACE]	*Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE – Common Criteria Protection Profile, BSI-CC-PP-0068-V2-2011, Version 1.0, November 2011.*
[PFASE]	*jTOP INF#v46 - ARGES Security Target, Trusted Logic, CP-2011-RT-484*
[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.*
[ANSSI]	*Référentiel Général de Sécurité, Annexe B1 : Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse "standard". ANSSI, version 1.20, 26 janvier 2010*
[ETR]	*ETR-lite for composition, Version 1.1, July 2002. Available at the address www.ssi.gouv.fr.*
[ETRSC]	*ETR-lite for composition, Annex A, Composite Smart Card Evaluation: Recommended Best Practice, Version 1.2, March 2002. Available at the address www.ssi.gouv.fr.*
[ICAO Doc]	*ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization, normative appendix 5*
[ICAO TR]	*ICAO TR Supplemental Access Control for Machine Readable Travel Documents version 1.00, march 23, 2010 (PACE)*
[ICPP]	*Security IC Platform Protection Profile, Version 1.0, June 2007, registered at the BSI under the reference BSI-PP-0035*
[ICST]	*Security Target M7820 M11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox version 1.4, 2011-04-18, Infineon Technologies AG*
[MRTD]	*PKI for Machine Readable Travel Documents offering ICC Read-Only Access, International Civil Aviation Organization (ICAO). Version 1.1, October 1st 2004*

[CC1]	*Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 3. July 2009. CCMB-2009-07-001.*
[TR03110]	*Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.1, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)*
[Note 10-ANSSI]	*Application note - Certification of applications on "open and cloisonning platform" », reference ANSSI-CC-NOTE/10.0EN, see www.ssi.gouv.fr.*
[SECGD]	*Infineon SLx 78Controllers Security Guidelines – User Manual. Released, December 2011*

2.1.2 Platform Documents

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

[PFCMC]	*jTOP – Configuration Management Plan, CP-2012-RT-356-1.0.*
[PFPRE]	*jTOP – Preparative Procedure, CP-2011-RT-731-1.0.*
[PFATE]	*jTOP – Test Documentation, CP-2012-RT-347-1.0 to CP-2012-RT-349-1.0..*
[PFDEL]	*jTOP – Delivery and Operation, CP-2007-RT-015.*
[PFDEV]	*SSTP– Development Security, CP-2012-RT-353-1.0.*
[PFFSP]	*jTOP – Functional Specification,CP-2012-RT-348-1.0.*
[PFIGS]	*jTOP – Card Initialization Phase, CP-2003-RT-52-27-1.9-SERMA-v46.*
[PFLCD]	*jTOP – Software Life Cycle, CP-2012-RT-355-1.0.*
[PFTDS]	*jTOP – TOE Design Specification, CP-2012-RT-349-1.0.*
[PFTAT]	*jTOP – Tools and Techniques, CP-2012-RT-354-1.0.*
[PFOPE]	*jTOP – Operational User Guidance, CP-2011-RT-732-46-1.0.*
[PFARC]	*jTOP – Security Architecture, CP-2012-RT-38-1.0.*
[PFCOMP]	*jTOP – Composite Design Compliance, CP-2011-RT-738-1.0.*
[PFINT]	*jTOP – Security Function Internals, CP-2011-RT-729-1.0.*

2.1.3 Assurance Measures Documents

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

[ACM]	*TL ICAO LDS - PACE/EAC – Configuration Management Plan, Trusted Logic, CP-2008-RT-679. TF4C – Configuration Management Plan, Trusted Logic, CP-2008-RT- 680*
[ADM]	*TL ICAO LDS - PACE/EAC – Preparation Guide, Trusted Logic, CP-2008-RT-727.*
[ATE]	*TL ICAO LDS - PACE/EAC – Test Documentation, Trusted Logic, CP-2012-RT-779.*
[DEL]	*TF4C – Delivery and Operation, Trusted Logic, CP-2007-RT-015.*
[DEV]	*TL ICAO LDS - PACE/EAC – Development Security, Trusted Logic, CP-2004-NT-576.*

[ACM]	*TL ICAO LDS - PACE/EAC – Configuration Management Plan, Trusted Logic, CP-2008-RT-679. TF4C – Configuration Management Plan, Trusted Logic, CP-2008-RT- 680*
[FSP]	*TL ICAO LDS - PACE/EAC – Functional Specification, Trusted Logic, CP-2012-RT-773.*
[TDS]	*TL ICAO LDS - PACE/EAC – Design and Architecture, Trusted Logic, CP-2008-RT- 638*
[LCD]	*TF4C – Software Life Cycle, Trusted Logic, CP-2007-RT-016.*
[TAT]	*TL ICAO LDS - PACE/EAC – 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 - PACE/EAC – Security Architecture, Trusted Logic, CP-2012-RT-768.*
[OPE]	*TL ICAO LDS - PACE/EAC – Operation Guide, Trusted Logic, CP-2012-RT-770.*
[PRE]	*TL ICAO LDS - PACE/EAC – Preparation Guide, Trusted Logic, CP-2012-RT-769.*
[ADV_COMP]	*TL ICAO LDS - PACE/EAC – Composite Design Compliance, Trusted Logic, CP-2013-RT-508.*

2.2 Acronyms

The following acronyms are used in this document:

Acronym	Meaning
AA	*Active Authentication*
AES	*Advanced Encryption Standard*
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*
CLA	*Instruction class (of an APDU command)*
CPLC	*Card Production Life Cycle Data*
CVM	*Cardholder Verification Method*
DAP	*Data Authentication Pattern*
DES	*Data Encryption Standard*
DEMA	*Differential Electromagnetic Attack*
DFA	*Differential Fault Analysis*
DPA	*Differential Power Analysis*
EAC	*Extended Access Control*
PACE	*Password Authenticated Connection Establishment*
DV	*Document Verifier*
ECDH	*Elliptic Curve Diffie Hellman*
EEPROM	*Electrically Erasable Programmable Read Only Memory*
EMA	*Electro-Magnetic Analysis*

Acronym	Meaning
EPA	*Emanation Power Analysis*
GP	*GlobalPlatform*
INS	*Instruction code (of an APDU command)*
IS	*Inspection System*
ISD	*Issuer Security Domain*
JAR	*Java Archive file*
JCAPI	*Java Card Application Programming Interface*
JCRE	*Java Card Runtime Environment*
JCSPP	*Java Card System Protection Profile*
JCVM	*Java Card Virtual Machine*
jTOP	*Java Trusted Open Platform*
LDS FS	*LDS File System*
MAC	*Message Authentication Code*
MRTD	*Machine Readable Travel Document*
OPEN	*Open Platform Environment*
OS	*Operating System*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
PP	*Protection Profile*
ROM	*Read Only Memory*
RMI	*Remote Method Invocation*
RSA	*Rivest Shamir Adleman*
RTE	*Run Time Environment*
SAR	*Security Assurance Requirement*
SCP	*Smart Card Platform*
SCP02	*Secure Channel Protocol 02*
SD	*Security Domain*
SF	*Security Function*
SFR	*Security Functional Requirement*
SPA	*Simple Power Analysis*
SSD	*Supplementary Security Domain*
ST	*Security Target*
TA	*Terminal Authentication*
VGP	*VISA GlobalPlatform*
TOE	*Target of Evaluation*
TSF	*TOE Security Functions*

2.3 Glossary

Term	***Definition***
Applet	*An application written in Java Card.*
Application Code 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..*
Application Instance	*Instance of an Executable Module after it has been installed and made selectable.*

Term	***Definition***
Application Protocol Data Unit (APDU)	*Standard communication messaging protocol between a card accepting device and a smart card. See ISO-7816-4.*
Application Provider	*The institution that owns an Application and is responsible for its behavior.*
Application Session	*The link between the Application and the external world during a Card Session starting with the Application selection and ending with Application de-selection or termination of the Card Session.*
Asymmetric Cryptography	*A cryptographic technique that uses two related transformations, a public transformation (defined by the Public Key component) and a private transformation (defined by the Private Key component); these two key components have a property so that it is computationally infeasible to discover the Private Key, even if 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..*
Travel Document's Content	*Code and Application information (but not Application data) contained in the Travel Document that is under the responsibility of the OPEN e.g. Executable Load Files, Application instances, etc.*
Travel Document Session	*The period of time during which the Travel Document receives power supply from the terminal without receiving a Travel Document reset signal.*
Card Administrator	*An organization, representative of the Card Issuer, that has control of the smart card's content and life cycle management. During the platform initialization phase, this role is embodied by the Card Enabler. During the platform usage phase, this role is embodied by the Card Issuer or an Application provider owning a SD with card content management privileges. Depending of its privileges, a Card Administrator can lock, unlock or terminate the smart card, download new applets on it, modify the static keys of its SD or retrieve administration information from the smart card. A Card Administrator always acts on behalf of the Card Issuer.*
Card Content	*Code and Application information (but not Application data) contained in the card that is under the responsibility of the OPEN e.g. Executable Load Files, Application instances, etc.*
Card Enabler	*The organization responsible for moving a manufactured TOE to the operational state.* *The person or organization responsible for transmitting the card to the card Administrator.*
Card Image Number (CIN)	*An identifier for a specific smart card.*

Term	***Definition***
Card Issuer	*The organization that owns the card and is ultimately responsible for its behavior*
Card Manager	*Generic term for the card management entities of a GlobalPlatform card i.e. the Open Platform Environment, the Issuer Security Domain, the Supplementary Security Domains.*
Card Manufacturer	*The organization responsible for integrating the IC containing the embedded software into its carrier, in accordance with the Card Issuer's requirements, to produce a complete card ready for delivery to the Card Enabler.*
Card Production Life Cycle Data	*A record that uniquely identifies the smart card and the actors involved in its manufacturing and personalization.*
Card Session	*The period of time during which the card receives power supply from the terminal without receiving a card reset signal.*
Card Unique Data	*Data that uniquely identifies a card made of the Card Image Number and a code identifying the Card Issuer.*
Cardholder	*The end user of the smart card.*
Cardholder Verification Method (CVM)	*A method to ensure that the person presenting the card is the person to whom the card was issued.*
Chip Manufacturer	*The organization responsible for embedding the software of the OS, RTE and GP in the IC ("masking process").*
Closed Mode	*A mode in which the card restricts card content management operations. When the card is in the Closed Mode it rejects loading more Executable Load Files. There are two possible closed modes: Java Card Static and Native Card.*
Controlling Authority	*A Controlling Authority has the privilege to keep the control over the Card Content through the mandating of DAP Verification*
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 Operating System, the Runtime Environment, the Card Manager and the bytecode of the installed Java Card Packages.*
Executable File	*Actual on-card container of one or more Executable Modules. 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 smart card.*
Executable Module	*The on-card executable code of a single Application present within an Executable Load File.*
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.*

Term	***Definition***
GlobalPlatform Registry	*A container of information related to Card Content management.*
Host	*The back end system that supports the smart card. Hosts perform functions such as authorization and authentication, card administration, download of post-issuance Application code and data and transactional processing*
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 Card Issuer*
Issuing State or Organization	*The state that provides the Travel Document for the user. This role is a particular case of "Card Issuer", as it concerns LDS FS API.*
Java Card Platform	*A collective name for all the components of the Embedded Software (OS, RTE and GP) that transform the IC into a Java Card enabled smart card.*
Java Card Static	*A closed mode in which no more Executable Load Files may be loaded on the card.*
Java Card System	*The term used in [JCSPP] to refer to the Runtime Environment, plus those parts of the Card Manager corresponding to the Installer and the Applet Deletion Manager.*
Masking Process	*The process of embedding the binary code of the Operating System, the Runtime Environment, the Card 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 card is in this mode.*
Object	*An entity on which a Security Policy is enforced.*
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 the basic OS, RTE and GP software.*
Platform Personalization Data	*Any data supplied relative to the Card Issuer that is injected into the non-volatile memory of the smart card by the Card Enabler. These data are for instance used to personalize the platform with the Card Issuer's keys, for traceability purposes, and to secure shipment between phases.*
Post-Issuance	*Phase following the card being issued to the Cardholder.*
Pre-Issuance	*Phase prior to the card being issued to the Cardholder.*

Term	***Definition***
Private Key	*The private component of an asymmetric key pair.*
Public Key	*The public component of an asymmetric key pair.*
Retry Counter	*A counter, used in conjunction with the Retry Limit, to determine when attempts to present a CVM value shall be prohibited.*
Retry Limit	*The maximum number of times an invalid CVM value can be presented prior to the CVM handler prohibiting further attempts to present a CVM value.*
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.*
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 Domain	*On-card entity providing support for the control, security, and communication requirements of the Application Provider.*
Security Policy	*A set of rules that regulate how certain assets are managed, protected and/or distributed.*
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.*
Subject	*The entity within the Platform (e.g. Issuer Security Domain, RTE) that acts on behalf of a User to perform some operation on an Object within the scope of a Security Policy.*
Supplementary Security Domain	*Security Domain other than ISD.*
Symmetric Cryptography	*A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation.*
User	*Either an Application (via GP API or JC API) or an off-card entity (via an APDU command) that makes a request to a Subject to perform some operation on an Object within the scope of a Security Policy.*

2.4 Equivalent Terms

This Security Target relays on several public specifications (GlobalPlatform, Java Card, and 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.

The Term "Travel Document" corresponds to both the meanings "MRTD" in [PPEAC] and "Travel Document" in [PPPACE].

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

3 TOE Description

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

3.1 The Target of Evaluation

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 – PACE/EAC) providing the electronic passport services defined in [ICAO Doc] and [TR03110]. The TOE therefore comprises of:

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

The TOE supports the security mechanism Active Authentication defined in [ICAO Doc]. It also supports the mechanisms Chip Authentication and Terminal Authentication defined in [TR03110].

The runtime environment on which the TL ICAO LDS – PACE/EAC is executed is compliant with the version of the Java Card platform specified in [JCVM], [JCRE] and [JCAPI]. The different operations involved in the Travel Document 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 – PACE/EAC.

The circuit of the Travel Document's chip is any of Infineon's SLE78CLX1600PM-m7820-M11/SLE78CLX800P/SLE78CLX360PM 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, 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 Open Platform

The TOE behaves as an open smart card platform intended for ID applications. It can be configured so that other applets apart from the TL ICAO LDS – PACE/EAC can be downloaded and installed on it, such as a national identity card applet. Moreover, several instances of TL ICAO LDS - PACE/EAC can coexist in it, and be used for different identification purposes. A smart card application, however, is usually intended to store highly sensitive information, so the sharing of that information must be carefully limited.

The Open Platform jTOP follows the certification requirements for "open and Isolating Platform" as defined in ANSSI Note 10 document [Note 10-ANSSI]. This note requires:

1. Applet isolation, which is achieved in jTOP 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.

2. Verification of integrity and authenticity of post-loaded applications, which is achieved in jTOP through the GlobalPlatform Mandated DAP feature.

3. Verification of loaded applications according to the rules stated in the AGD_OPE guide of the jTOP Platform for isolation properties, which is enforced by the OE.VERIFICATION security objective for the environment of the jTOP security target.

4. Availability of an integrity and authenticity evidence for each application, which is enforced through a DAP signature of the application by the OE.CODE-EVIDENCE security objective for the environment of the jTOP security target.

The challenge of implementing a secure open, multi-application smart card platform has been already addressed in [PFASE]. This Security Target does not focus on that security problem, but on the one described in [PPEAC] and [PPPACE].

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 – PACE/EAC) 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 Travel Document 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.

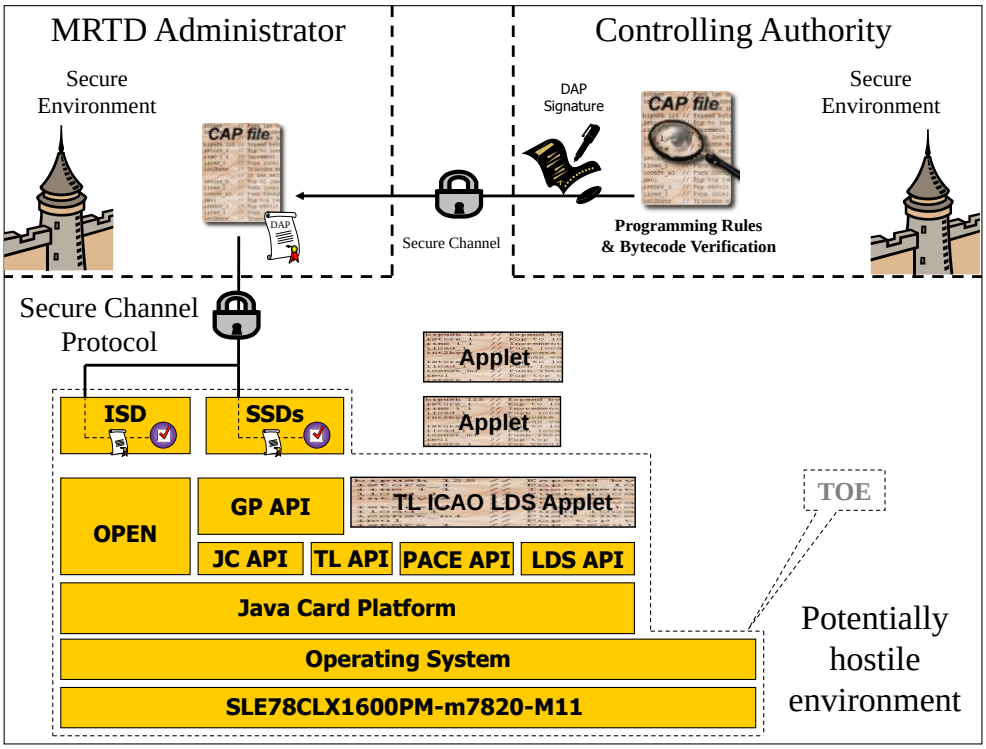

Figure 1: The TOE and its environment

Upon reception of the Executable File, the Travel Document 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 Travel Document 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.

[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.

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 Travel Document 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.

Optionally, the selection of the ISD may be disabled before the Operational Phase, so that the Travel Document behaves as a closed-application native card. In this case, after installing the desired applet instances, the ISD becomes not longer selectable and all the external interfaces available for accessing it are disabled. This operation cannot be undone. Once the Travel Document is closed, the only management command that the ID Platform supports is the SELECT command specified in ISO7816. Other APDU commands are directly forwarded to the selected application.

3.1.2 LDS FS API

The LDS FS API is part of the TOE. This API is implemented as a part of jTOP Platform. The supported services related to this API are:

Secure Messaging using DES and AES session keys

LDS File System with fast file reading

LDS File System with fast file writing for personalization.

Secure storage of biometric and sensitive files.

LDS FS is a file system that contains information like identity, age, name, first name, picture… It may also contain biometric data (fingerprint…). If biometry is present, the EAC configuration is used, and the sensitive files are stored securely. EAC enables protection of sensitive data. If biometry is not present, the PACE configuration is used. The API allowed to manage the file system (add file, read file, set authentication level) and the secure messaging (wrap, unwrap, authentication).

LDS FS is an API at disposal of applications. These applications can be added post-issuance and evaluated by composition over the jTOP platform.

3.1.3 PACE API

The PACE API is part of the TOE and provides the following services:

- SAC PACE authentication (with ECDH and DES/AES algorithms)
- Secure Messaging initialization with session keys issued from the PACE authentication.
- PACE mapping (point generation with ECDH and domain generation)

PACE API is aimed at providing a replacement for the BAC protocol, correcting the entropy weakness with strong session keys. This API provides services as secure messaging and mapping.

This API can be used by applications in the same way as LDS FS API. This API is also a part of the jTOP Platform.

3.2 TOE Life Cycle

Figure 2 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] and [PPPACE]: Development, Manufacturing, Personalization of the Travel Document 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.

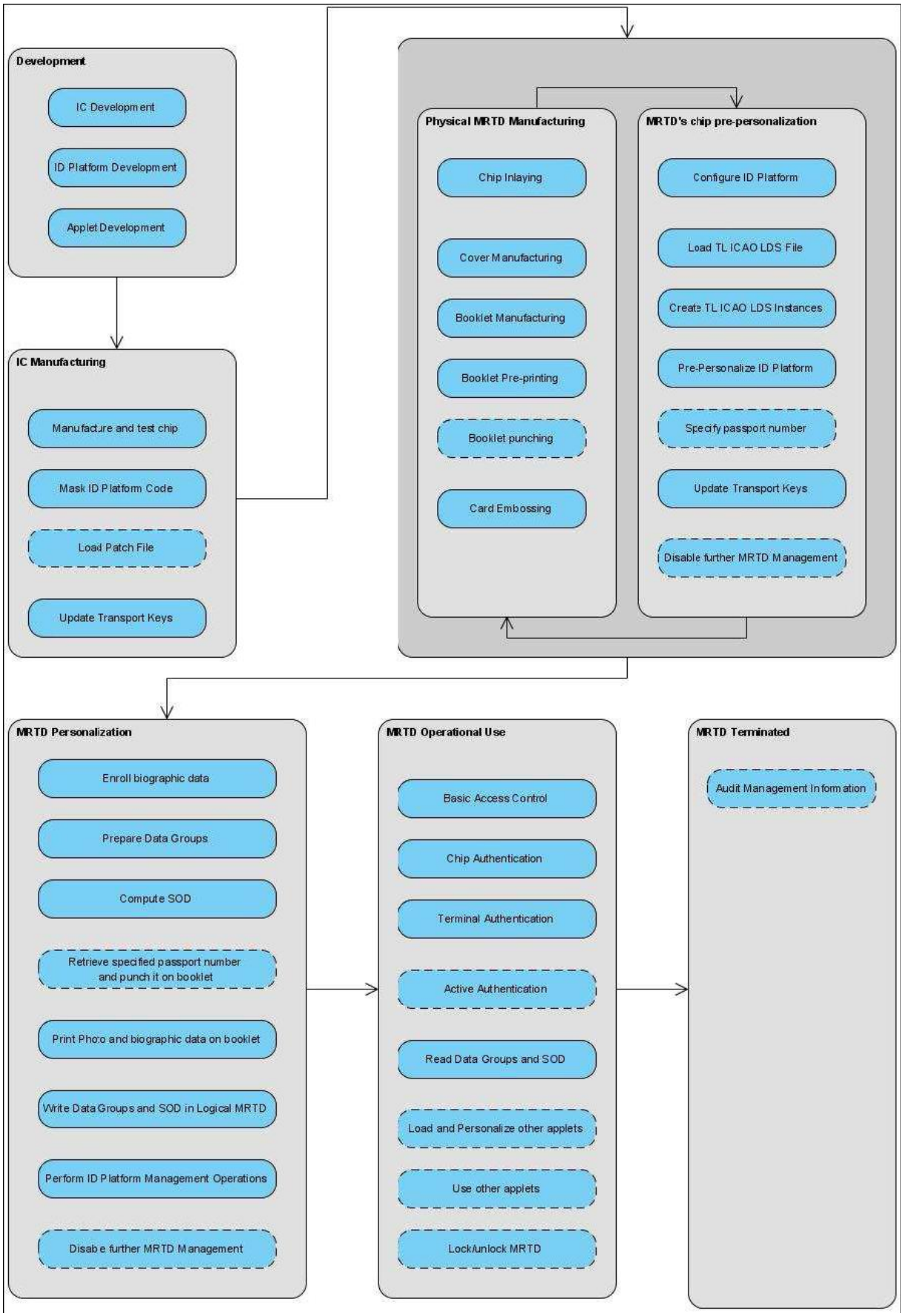

Figure 2: TOE Life Cycle

3.2.1 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 – PACE/EAC 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.

3.2.2 Manufacturing

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

3.2.2.1 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.

3.2.2.2 Travel Document Manufacturing

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

Manufacturing the physical Travel Document 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 Travel Document 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 Travel Document is intended to communicate through the contact-based interface, manufacturing the physical Travel Document 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 Travel Document and the process to fabricate it, all these operations have in common that they run the Travel Document 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 Travel Document.

Pre-personalizing the Travel Document's chip involves (1) loading the code of the TL ICAO LDS – PACE/EAC 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 Travel Document content management, writing CPLC audit logs, stepping forward the TOE life cycle state; etc. These operations have in common that they interact with the Travel Document'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 Travel Document Manufacturing and the pre-personalization of the Travel Document'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 Travel Document 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 – PACE/EAC, 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 Travel Document.

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

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

3.2.3 Travel Document Personalization

The personalization of the Travel Document includes (i) the survey of the Travel Document holder's biographical data, (ii) the enrolment of the Travel Document 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 Travel Document, (iv) the writing of the TOE User Data and TSF Data into the logical Travel Document and (v) the writing of the TSF Data into the logical Travel Document 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 Travel Document Manufacturing Phase, its number may be retrieved from the Logical Travel Document, 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 Travel Document for the Travel Document holder. This signature attests that all the loaded data is correct and does match the Travel Document holder.

TL ICAO LDS – PACE/EAC 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 – PACE/EAC.

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

3.2.4 Travel Document Operational Use

The TOE is used as Travel Document 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 Travel Document during the operational phase or to delete the personalized instance of the TL ICAO LDS – PACE/EAC.

If other applets apart from the TL ICAO LDS – PACE/EAC 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 Travel Document's life cycle, the Travel Document 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 Travel Document 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 Travel Document, 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.

3.2.5 Travel Document Termination

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

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

3.3 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.

3.3.1 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	*ALC*
IC Manufacturing	*AGD_PRE*
Physical Travel Document Manufacturing	*AGD_PRE*
Travel Document's chip Pre-Personalization	*AGD_PRE*
Travel Document Personalization	*AGD_PRE*
Travel Document Operational Use	*AGD_OPE*
Travel Document Termination	*AGD_OPE*

Table 4 Evaluated TOE life cycles

The Travel Document's chip, especially with regard to AVA_VAN, is evaluated in the Operational Phase.

As required by [PPEAC] and [PPPACE], the TOE life cycle perimeter includes all the design phases as well as the IC and Travel Document manufacturing phases up to the Travel Document personalization and usage. However, several TOE life cycle phases, that would be quite unrealistic to cover by ALC class, can be covered by AGD class without decreasing significantly the obtained assurance.

By following the interpretation of French Scheme's application, the following issues have been solved:

- The "creation of the Travel Document application" is covered by guidance and analyzed through AGD tasks because the procedures describe exactly how to configure the application and that this configuration process cannot decrease the security level of the product (see AGD_PRE, chapter 3.2),

- The product's self-protection mechanism from the delivery until its use by the personalization agent is based on SCP.02 secure channel protocol evaluated during OURANOS and considered as strong enough to protect the TOE integrity during intermediate deliveries during these phases.

These interpretations allow covering the Travel Document manufacturing and pre-personalization life cycle phases only by AGD class instead of the whole ALC class (see fully detailed recommendations in [PFUSR]). Therefore, the TOE delivery is operated at the end of IC manufacturing, with a reasonable loss of assurance. After this point, the TOE is mature enough to be considered as self-protected and using the same mechanisms as those considered in the scope of evaluation (namely, Mutual Authentication based on secure DES.

3.3.1.1 ID Platform Configuration

The ID Platform underlying TL ICAO LDS – PACE/EAC 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 – PACE/EAC 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 – PACE/EAC optional features do fall into the evaluation scope.

3.3.2 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.

3.3.2.1 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] and [PPPACE] is out of the scope of this Security Target. Moreover, the requirements in this Security Target 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 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 assumes that they are harmless with respect to all the security policies of the platform.

3.3.2.2 Supplementary logical channels and Remote Method Invocation

The Java Card platform underlying the TL ICAO LDS – PACE/EAC 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 Travel Document 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

4.1 Assets

4.1.1 Assets from PPs EAC and PACE

The TOE assets to be protected are those defined in [PPEAC] and [PPPACE]. This Security Target does not introduce new assets to be protected.

User data stored on the TOE

All data (being not authentication data) stored in the context of the ePassport application of the travel document and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. This asset covers Logical Travel Document sensitive User Data in [PPEAC].

Property to be maintained by the current security policy: Confidentiality, Integrity and Authenticity.

Application Note:

User Data consisting of sensitive biometric data of the Travel Document holder such as fingerprints and iris image, contained in the EF.DG3 and EF.DG4 elementary files.

User data transferred between the TOE and the terminal connected

All data (being not authentication data) being transferred in the context of the ePassport application of the travel document between the TOE and an authenticated terminal acting as Basic Inspection System. User data can be received and sent (exchange <--> [receive, send]).

Property to be maintained by the current security policy: Confidentiality, Integrity and Authenticity.

Application Note:

User Data consisting of sensitive biometric data of the Travel Document holder such as fingerprints and iris image, contained in the EF.DG3 and EF.DG4 elementary files.

Travel document tracing data

Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognising the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.

Property to be maintained by the current security policy: Unavailability

Accessibility to the TOE functions and data only for authorised subjects

Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.

Property to be maintained by the current security policy: Availability.

Genuineness of the TOE

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. The authenticity of the Travel Document's chip personalized by the issuing

State or Organization for the Travel Document holder is used by the traveler to prove his possession of a genuine Travel Document. This asset also covers "Authenticity of the Travel Document's chip" in [PPEAC].

Property to be maintained by the current security policy: Availability.

TOE internal secret cryptographic keys

Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

Property to be maintained by the current security policy: Confidentiality, Integrity.

TOE internal non-secret cryptographic material

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.

Property to be maintained by the current security policy: Integrity, Authenticity.

Travel document communication establishment authorisation data

Restricted-revealable authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.

Property to be maintained by the current security policy: Confidentiality, Integrity.

Application Note:

The travel document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy.

4.2 Users / Subjects

4.2.1 Subjects from PPs EAC and PACE

The following Subjects come either from [PPEAC] and [PPPACE]:

Manufacturer

Generic term for the IC Manufacturer producing integrated circuit and the Travel Document Manufacturer completing the IC to the Travel Document's chip. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and Travel Document Manufacturer using this role Manufacturer. This entity is commensurate with "Manufacturer" in [PPEAC].

Personalization Agent

The Personalization Agent is acting on behalf of the issuing State or Organization to personalize the Travel Document for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the Travel Document, (ii) enrolling the biometric reference data of the Travel Document 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 Travel Document for the holder as defined for global, international

and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object. Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the Travel Document Issuer. This entity is commensurate with 'Personalisation agent' in [PPEAC].

Terminal

A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role "Terminal" is the default role for any terminal being recognised by the TOE as not being PACE authenticated ("Terminal" is used by the travel document presenter).

This entity is commensurate with 'Terminal' in [PPEAC].

Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an Travel Document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as Travel Document holder.

The Basic Inspection System (BIS) (i) contains a terminal for the contactless communication with the Travel Document's chip. The General Inspection System (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

Application Note:

The support of (i) the Passive Authentication mechanism is mandatory, and (ii) the Basic Access Control is optional. In the context of the protection profile [PP PACE], the Primary Inspection System does not implement the terminal part of the Basic Access Control. It is therefore not able to read the logicalTravel Document because the logical Travel Document of the TOE is protected by Basic Access Control. Therefore the protection profile [PP PACE] will not consider the use of Primary Inspection System by the receiving State or Organization. The TOE of the current security target does not allow the Personalization Agent to disable the Basic Access Control for use with Primary Inspection Systems as described in the BSI-PP-0017 Machine Readable Travel Document with 'ICAO Application", Basic Access Control.

Travel document holder

A person for whom the travel document Issuer has personalised the travel document (Travel Document). Please note that a travel document holder can also be an attacker.

This entity is commensurate with 'Travel Document Holder' in [PPEAC].

Travel document presenter

A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This entity is commensurate with 'Traveller' in [PPEAC].

Please note that a traveler can also be an attacker.

Attacker

A threat agent trying (i) to identify and to trace the movement of the Travel Document's chip remotely (i.e. without knowing or optically reading the physical Travel Document), (ii) to read or to manipulate the logical Travel Document without authorization, or (iii) to forge a genuine Travel Document. The attacker is assumed to possess an at most high attack potential. Please note that the attacker might "capture" any subject role recognised by the TOE. This external entity is commensurate with "Attacker" in [PPEAC].

Application Note:

An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged Travel Document. Therefore the impostor may use results of successful attacks against the TOE but his or her attack itself is not relevant for the TOE.

BIS-PACE

A technical system being used by an inspecting authority and verifying the Travel Document presenter as the Travel Document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder).BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the Travel Document using a shared password (PACE password) and supports Passive Authentication.

Document Signer (DS)

An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the Travel Document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS). This role is usually delegated to a Personalisation Agent.

Document Verifier

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

Country Verifying Certification Authority (CVCA)

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

Country Signing Certification Authority (CSCA)

An organisation enforcing the policy of the Travel Document Issuer with respect to confirming correctness of user and TSF data stored in the Travel Document. The CSCA represents the country specific root of the PKI for the Travel Document and creates the

Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means.

4.2.2 Specified Subjects for LDS Applet

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 to the ones defined in [PPEAC] and [PPPACE]:

Issuer Security Domain

The ISD is a distinguished applet that acts as the on-card representative of the Travel Document Administrator. When the Travel Document Administrator has to perform a management operation such as loading a new applet, performing an Travel Document 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-PACE/EAC and the ISD that the Travel Document 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-PACE/EAC.

4.3 Threats

4.3.1 Threats from PPs EAC and PACE

All the threats menacing the TOE are the ones introduced in [PPEAC] and [PPPACE].

T.Leak-Inherent and T.Leak-Forced from [ICST] cover the threat T.Information_Leakage from [PP EAC] and [PP PACE].

T.Skimming

An attacker imitates the inspection system to read the logical Travel Document or parts of it via the contactless communication channel of the TOE. The attacker cannot read and does not know in advance the physical Travel Document.

T.Eavesdropping

An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.

Asset: confidentiality of "User data stored on the TOE".

T.Tracing

An attacker tries to gather TOE tracing data (i.e. to trace the movement of the Travel Document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE.

Asset:privacy of the travel document holder

T.Counterfeit

An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine chip to be used as part of a counterfeit product. This violates the authenticity of the chip used for authentication of a traveler. The attacker may generate a new data set or extract completely or partially the data from a genuine chip and copy them on another appropriate chip to imitate this genuine chip.

Asset: authenticity of "User data stored on the TOE".

T.Forgery

An attacker alters fraudulently the complete stored logical Travel Document or any part of it including its security related data in order to impose on an inspection system by means of the changed holder's identity or biometric reference data. An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS-PACE by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one. This threat comprises several attack scenarios of forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical Travel Documents to create a new forged Travel Document, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical Travel Document of a traveler into an other Travel Document's chip leaving their digital MRZ unchanged to claim the identity of the holder this Travel Document. The attacker may also copy the complete unchanged logical Travel Document in another contactless chip.

Asset: authenticity and integrity of "User data transferred between the TOE and the terminal connected" and "User data stored on the TOE".

T.Phys_Tamper

An attacker may perform physical probing of the chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the chip Embedded Software. An attacker may physically modify the chip in order to (i) modify security features or functions of the chip, (ii) modify security functions of the chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The

modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

Application Note:

This threat refines threats described in [ICST]:

- o T.Phys-Manipulation
- o T.Phys-Probing

It is described specifically for LDS/PACE API because of the presence of biometric data.

T.Read_Sensitive_Data

An attacker with high attack potential knowing the Document Basic Access Keys is trying to gain the sensitive biometric reference data through the communication interface of the chip. The attack T.Read_Sensitive_Data is similar to the threats T.Skimming in respect of the attack path (communication interface) and the motivation (to get data stored on the chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the Travel Document's chip as private sensitive personal data whereas the MRZ data and the portrait are visual readable on the physical Travel Document as well.

Asset: confidentiality of "User data stored on the TOE".

T.Abuse_Func

Abuse of Functionality An attacker may use functions of the TOE which shall not be used in "Operational Use" phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to Travel Document holder.

Asset: confidentiality and authenticity of logical Travel Document and TSF data, correctness of TSF

Application Note:

This threat refines T.Abuse_Func described in [ICST].

It is described specifically for LDS/PACE API because of the presence of biometric data.

T.Information_Leakage

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

Asset:confidentiality of User Data and TSF-data of the travel document

Application Note:

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to

the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Malfunction

An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE's hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Asset:integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.

4.4 Organisational Security Policies

All Organizational Security Policies introduced in [PFASE] are also apply to this Security Target. For the sake of readability, the following policies in [PFASE] have been slightly rephrased in order to use the terminology introduced in [PPEAC] and [PPPACE]:

- OSP.FILE-ORIGIN
- OSP.VERIFICATION

4.4.1 Embedded Software OSP

OSP.FILE-ORIGIN

The Travel Document's Chip Pre-Personalizer and the Travel Document 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 Travel Document have been previously validated by the Verification Authority, and not modified afterwards.

Application Note:

If the TOE does not enforce DAP verification, it is up to the Travel Document's Chip Pre-personalizer and/or the Travel Document Administrator to ensure that only bytecode verified applets are installed on the ID Platform. The Policy above is just a refinement for the TL ICAO LDS-PACE/EAC of the generic Policy OSP.FILE-ORIGIN introduced in [PFASE].

4.4.2 Java Card System Protection Profile - Open Configuration

OSP.VERIFICATION

Before loading an Executable Load File on the Travel Document, 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 Travel Document. Upon successful verification of an Executable Load File, all the roles involved in Travel Document content management immediately activate all the IT and organizational measures required for preventing any modification of it until it is downloaded into the Travel Document. If the Travel Document 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 Travel Document Administrator through a secure communication channel ensuring the origin and the integrity of transmitted files. Upon reception, the Travel Document Administrator stores the Executable File in its secure environment until the file is downloaded into the Travel Document.

Application Note:

Bytecode verification ensures that Travel Document security will not be endangered by the installation of other, potentially malicious applets on the ID Platform. New applets may be downloaded on the Travel Document at any time, even during the Travel Document Operational Phase. The Verification Authority is the role in charge of performing bytecode verification. The Travel Document Administrator is in charge of transmitting the applet code to the Travel Document. When the applet is loaded during the Travel Document Manufacturing Phase, this latter role is embodied by the Travel Document's Chip Pre-Personalizer. The Policy above is just a refinement for the TL ICAO LDS-PACE/EAC of the generic Policy OSP.VERIFICATION introduced in [PFASE].

4.4.3 OSPs from PPs EAC and PACE

The TOE environment shall enforce all the Organizational Security Policies defined in [PPEAC] and [PPPACE]:

OSP.Pre-Operational

1)Travel Document Issuer issues the Travel Document and approves it using the terminals complying with all applicable laws and regulations. 2)The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF data permanently stored in the TOE. 3)The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase. 4)If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

OSP.Card_PKI

1)The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (CCSCA). 2)The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer. 3)A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

OSP.Manufact

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The Travel Document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

OSP.Trustworthy_PKI

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

OSP.Terminal

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows: 1)The related terminals shall be used by terminal operators and by travel document holders. 2)They shall implement the terminal parts of the PACE protocol, of the Passive Authentication and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann). 3)The related terminals need not to use any own credentials. 4)They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document). 5)The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

OSP.BAC-PP

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

OSP.Sensitive_Data

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

OSP.MRTD_Personalization

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

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

4.4.4 Specified OSPs for LDS Applet

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

OSP.APPLET-INSTALL

Installation of TL ICAO LDS-PACE/EAC

When creating an instance of TL ICAO LDS-PACE/EAC, the Travel Document's Chip Pre-Personalizer sets the installation parameters required to activate at least the following security features: (1) 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 Travel Document's Chip Pre-Personalizer also performs some Travel Document management operations that prevent the other actors from intentionally or accidentally deleting the TL ICAO LDS-PACE/EAC instance to be used as an electronic passport.

Application Note:

Some of the security mechanisms required in this Security Target are optional features of TL ICAO LDS-PACE/EAC. The parameters passed during the creation of the applet instance determine whether they are activated or not. All other optional features that are not explicitly listed in the OSP above are considered as being free, all values for the option falling into the scope of evaluation. Disabling the possibility of removing the applet instance provides in-depth security, as the attacker could try to replace the code of the genuine TL ICAO LDS (including the Chip Authentication key pair) by a fake applet under his control.

OSP.Travel_Document_TRACEABILITY

Disabling traceability information

The Personalization Agent definitely disables the access to any unique data used for management purposes that the Travel Document's chip could return in clear text, including the key diversification data enabling the Personalization Agent to derive the Travel Document's Personalization Keys from a master key. After having successfully personalized the Travel Document chip, the Personalization Agent ensures that the transport keys that the Travel Document Manufacturer placed in the Travel Document's chip have been replaced by new secret ones, which shall only be known by the Travel Document 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 Travel Document.

Application Note:

Beyond the information stored in the CPLC audit records, the Travel Document's chip could also return other unique data that the attacker could use to trace the Travel Document Holder. An example of such unique data is the Key Diversification Data that GlobalPlatform's INITIALIZE UPDATE command returns. This data is usually used to

derive the secret key stored in the Travel Document's chip from a unique master key stored by the Personalization Agent, so simplifying the key infrastructure. This feature, introduced by GlobalPlatform's specifications and hence supported by the Issuer Security Domain, shall not be used to manage an Travel Document. The Personalization Agent is also expected to replace the transport keys that the Travel Document Manufacturer used to securely delivering the Travel Document to the Personalization Agent. Otherwise, the Travel Document Manufacturer would be in position of accessing the CPLC audit records identifying a given Travel Document chip.

In a fully open Travel Document, 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-PACE/EAC or the underlying ID Platform do not leak unique identifiers: all the applets installed on the Travel Document 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 Travel Document, the Verification Authority shall launch an evaluation procedure which analyzes the code of any additional applet before loading it on the Travel Document, in order to check whether it satisfies the expected privacy constraints. In particular, the Verification Authority shall ensure that the applets installed in the Travel Document satisfy the requirements FIA_UID.1 and FIA_UAU.1 in [PPEAC] and [PPPACE]. 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 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].

4.5 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used. They come either from [PPEAC], [PPPACE] or from the platform's security target [PFASE]. All assumptions introduced in [PFASE] are also apply to this Security Target. For the sake of readability, the following Assumptions in [PFASE] have been slightly rephrased in order to use the terminology introduced in [PPEAC] and [PPPACE]:

- A.NATIVE
- A.VERIFICATION
- A.APPLET

4.5.1 Assumptions on the Embedded Software

A.NATIVE

Any native application (that is, not written in Java Card) masked in the Travel Document's chip is assumed to be compliant with TL ICAO LDS-PACE/EAC so as to ensure that security policies and objectives described herein are not violated.

Application Note:

The Assumption above is just a refinement for the TL ICAO LDS-PACE/EAC of the generic Assumption A.NATIVE introduced in [PFASE].

4.5.2 Java Card System Protection Profile - Open Configuration

A.APPLET

Any Executable File loaded in the Travel Document's chip does not contain native code.

Application Note:

The Assumption above is just a refinement for the TL ICAO LDS-PACE/EAC of the generic Assumption A.APPLET introduced in [PFASE].

A.VERIFICATION

Any Executable File different from TL ICAO LDS-PACE/EAC that is masked on the Travel Document'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].

Application Note:

The Assumption above is just a refinement for the TL ICAO LDS-PACE/EAC of the generic Assumption A.VERIFICATION introduced in [PFASE].

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.

4.5.3 Assumptions from PPs EAC and PACE

The assumptions describe the security aspects of the environment in which the TOE will be used. They come either from [PPEAC] and [PPPACE]:

A.MRTD_Manufact

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

A.MRTD_Delivery

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

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Auth_PKI

The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control

rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their Travel Document's chip.

A.Passive_Auth

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical Travel Document. The issuing State or Organization runs a Certification Authority (CA) which (i) securely generates, stores and uses the Country Signing CA Key pair, and (ii) manages the Travel Document's Chip Authentication Key Pairs. The CA keeps the Country Signing CA Private Key secret and distributes the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the Travel Documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and Organizations.

Application Note:

Similar to A.Signature_PKI in [PP EAC]

A.Insp_Sys

The Inspection System is used by the border control officer of the receiving State (i) examining an Travel Document presented by the traveler and verifying its authenticity and (ii) verifying the traveler as Travel Document holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the PACE v2 Access Control. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the Travel Document's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

A.Pers_Agent

The Personalization Agent ensures the correctness of (i) the logical Travel Document with respect to the Travel Document holder, (ii) the Document Basic Access Keys or the document PACE v2 Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the Travel Document's chip, and (iv) the Document Signer Public Key Certificate (if stored on the Travel Document's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

5 Security Objectives

5.1 Security Objectives for the TOE

All security objectives introduced in [PFASE] are also apply to this Security Target. For the sake of readability, the following security objective in [PFASE] have been slightly rephrased in order to use the terminology introduced in [PPEAC] and [PPPACE]:

- O.FIREWALL

5.1.1 Java Card System Protection Profile - Open Configuration

5.1.1.1 EXECUTION

O.FIREWALL

The other applet instances installed on the ID Platform shall not be able to read or write the logical Travel Document data or the TSF data used by TL ICAO LDS-PACE/EAC.

Application Note:

This security objective supports O.Data_Integ and completes O.Data_Confidentiality. TL ICAO LDS-PACE/EAC 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-PACE/EAC instances and instances of other applets that could result in the disclosure or the corruption of the logical Travel Document data, or any other data that supports the TSF described in this Security Target. The security objective above is just a refinement for the TL ICAO LDS-PACE/EAC of the generic objective O.FIREWALL introduced in [PFASE].

5.1.2 OTs from PPs EAC and PACE

All the security objectives for the TOE defined in [PPEAC] and [PPPACE] are part of this Security Target:

O.AC_Pers

Access Control for Personalization of logical Travel Document

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

O.Data_Int

Integrity of Data

The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected after:

- o the Chip Authentication
- o the PACE Authentication (The Terminal must be represented by PACE authenticated BIS-PACE).

O.Data_Confidentiality

Confidentiality of Data

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated BIS-PACE connected.The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

O.Sens_Data_Conf

Confidentiality of sensitive biometric reference data

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

O.Identification

Identification and Authentication of the TOE

The TOE must provide means to store Initialisation and Pre-Personalisation Data in its non volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s). In Phase "Operational Use", the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

Application Note:

This Security Objective refines the Objective described in [ICST]:

- o O.Identification

O.Chip_Auth_Proof

Proof of Travel Document's chip authenticity

The TOE must support the General Inspection Systems to verify the identity and authenticity of the travel documents chip as issued by the identified issuing State or Organization by means of the Chip Authentication. The authenticity proof provided by travel documents chip shall be protected against attacks with high attack potential.

Application Note:

The OT.Chip_Auth_Proof implies the Travel Document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the

authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

O.Prot_Phys-Tamper

Protection against Physical Tampering

The TOE must provide protection of confidentiality and integrity of the User Data (e.g. the biometric reference data for the inspection system), the TSF-data (e.g. authentication key of the chip) and the travel document's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security functionality, as well as
- controlled manipulation of memory contents (User Data, TSF-data)with a prior
- reverse-engineering to understand the design and its properties and functionality.

Application Note:

This Security Objective refines Objectives described in [ICST]:

- O.Phys-Manipulation
- O.Phys-Probing

It is described specifically for LDS/PACE API because of the presence of biometric data.

O.Data_Authenticity

Authenticity of Data

The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal side.The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

O.Tracing

Tracing travel document

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

O.Prot_Inf_Leak

Protection against Information Leakage

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document

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

Application Note:

This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

O.Prot_Malfunction

Protection against Malfunctions

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

Application Note:

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

O.Prot_Abuse_Func

Protection against Abuse of Functionality After delivery of the TOE to the Travel Document Holder, the TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

5.2 Security Objectives for the Operational Environment

All security objectives for jTOP's environment introduced in [PFASE] are also objectives for the environment of the TOE. More specifically, the plaform being open, the following ones relate to applets loaded on the platform:

- OE.VERIFICATION
- OE.NATIVE
- OE.APPLET
- OE.NO-RMI-APPLETS
- OE.SECRETS

5.2.1 Java Card System Protection Profile - Open Configuration

OE.APPLET

No applet loaded post-issuance shall contain native methods.

OE.VERIFICATION

The Card Administrator transmits an Executable Load File to the card only if the application code complies with the security recommendations in [USR], has successfully passed the Bytecode Verification process and has not been modified afterwards.

Bytecode verification shall include:

- well-formedness of the CAP file structure and verification of the typing constraints on its bytecodes,
- binary compatibility with installed Executable Files and the assurance that the export files used to check the Executable Load File match the CAP files that will be present on the card when loading occurs. All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. See #.VERIFICATION for details. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform.

Application Note:

Constraints to maintain the isolation property of the platform are provided by the platform developer in application development guidance. The constraints apply to all application code loaded in the platform.

5.2.2 OEs from PPs EAC and PACE

All the security objectives for the environment defined in [PPEAC] and [PPPACE] applies to the environment of the TOE:

OE.Authoriz_Sens_Data

Authorization for Use of Sensitive Biometric Reference Data

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

Application Note:

This security objective for the operational environment is needed additionally to those from [PP PACE] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy OSP.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in this Protection Profile and not in [PP PACE].

OE.Ext_Insp_Systems

Authorization of Extended Inspection Systems

The Document Verifier of receiving States or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive

biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

Application Note:

This security objective for the operational environment is needed additionally to those from [PP PACE] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy OSP.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

OE.Auth_Key_MRTD

Travel document Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

Application Note:

This security objective for the operational environment is needed additionally to those from [PP PACE] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in this Protection Profile and not in [PP PACE].

OE.BAC_PP

It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the travel document data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

OE.MRTD_ Delivery

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

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

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

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

OE.MRTD_Manufact

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

OE.Legislative_Compliance

The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.

OE.Travel_Document_Holder

The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

OE.Passive_Auth_Sign

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained.A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

OE.Terminal

The terminal operators must operate their terminals as follows:

- The related terminals are used by terminal operators and by travel document holders.
- The related terminals implement the terminal parts of the PACE protocol, of the Passive Authentication (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost)for Diffie-Hellmann).
- The related terminals need not to use any own credentials.
- The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document).

- The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

Application Note:

OE.Terminal completely covers and extends 'OE.Exam_MRTD', 'OE.Passive_Auth_Verif' and 'OE.Prot_Logical_MRTD' from [PP EAC].

OE.Personalization

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enroll the biometric reference data of the travel document holder, (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data, (iv) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO Doc], (v) write the document details data, (vi) write the initial TSF data, (vii) sign the Document Security Object defined in [ICAO Doc](in the role of a DS).

OE.Exam_MRTD

Examination of the physical part of the travel document

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

Application Note:

This security objective for the operational environment is needed additionally to those from [PP PACE] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_MRTD also repeats partly the requirements from OE.Terminal in [PP PACE] and therefore also counters T.Forgery and A.Passive_Auth from [PP PACE].

OE.Prot_Logical_MRTD

Protection of data from the logical travel document

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.

Application Note:

This security objective for the operational environment is needed additionally to those from [PP PACE] in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

OE.Passive_Auth_Verif

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

5.2.3 Specified OEs for LDS Applet

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

OE.PRE-PERSONALIZATION

Installation of TL ICAO LDS-PACE/EAC

The Travel Document's Chip Pre-Personalizer shall configure TL ICAO LDS-PACE/EAC's optional features to support Chip Authentication and Terminal Authentication. This role shall also perform the Travel Document management operations required to disable the replacement of the genuine LDSApplet by another one.

OE.PLATFORM-IDENTIFICATION

Disabling platform traceability

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

Application Note:

The Personalization Agent may restrict access to unique information either by clearing it inside the Travel Document's chip (e.g., replacing key derivation data used during Travel Document Manufacturing by zeroes) or by the activation of a security mechanism that requires previous authentication as the Travel Document Administrator before accessing such data, and protects its transmission through secure messaging. Obviously, the Travel Document Administrator is not expected to restore the cleared data further on.

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.

Application Note:

Even if TL ICAO LDS-PACE/EAC does not leak any information that could be used to identify and trace the Travel Document Holder, the attacker could try to select and execute other applet instances installed on the ID Platform with the aim of obtaining data that uniquely identifies the Travel Document. The Verification Authority shall carefully inspect the design of other applets installed on the ID Platform and reject the installation of those that do not satisfy the objective OT.Identification stated for TL ICAO LDS-PACE/EAC.

5.2.4 Miscellaneous

OE.NATIVE

The Platform Developper shall ensure that all pre-issuance native applications masked with the code of the platform enforce the security policies and objectives described in this Security Target.

In particular, native applications that handle Java Card objects must respect the Java Card Firewall policy.Those parts of the APIs written in native code as well as any pre-issuance native application on the card shall be conformant with the TOE so as to ensure that security policies and objectives described herein are not violated.

Application Note:

In [JCSPP], this security objective also requires that parts of the API that are implemented as native methods enforce the security policies defined for the platform. That part of the objective has been discharged in this Security Target, as the native libraries of the Operating System that support API implementation are also in the scope of this TOE.

OE.SECRETS

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

5.2.5 Conclusion

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-PACE/EAC does meet the key lengths recommended in OE.KEY-LENGTH. Other applets fall out of the scope of this Security Target. Therefore, OE.KEY-LENGTH is not necessary as an objective for the TOE environment.

6 Extended Requirements

6.1 Extended Families

6.1.1 Extended Family FAU_SAS - Audit data storage

6.1.1.1 Description

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

6.1.1.2 Extended Components

Extended Component FAU_SAS.1

Description

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

There are no management activities foreseen.

There are no actions defined to be auditable.

Definition

FAU_SAS.1 Audit storage

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

Dependencies: No dependencies.

6.1.2 Extended Family FCS_RND - Generation of random numbers

6.1.2.1 Description

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

6.1.2.2 Extended Components

Extended Component FCS_RND.1

Description

The generation of random numbers requires that random numbers meet a defined quality metric.

There are no management activities foreseen for this component.

There are no actions defined to be auditable for this component.

Definition

FCS_RND.1 Quality metric for random numbers

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

Dependencies: No dependencies.

Rationale

It was chosen to define FCS_RND.1 explicitly, because Part 2 of the Common Criteria do not contain generic security functional requirements for Random Number generation. Note tha there are security functional requirements in Part 2 of the Common Criteria, which refer to random numbers. However, they define requirements only for the authentication context, which is only one of the possible applications of random numbers.

6.1.2.3 Rationale

This family has been introduced in [SSVG]. An attacker may predict or obtain information about random numbers generated by the TOE for instance because of a lack of entropy of the random numbers provided. Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE without specific knowledge about the TOE's generator. Malfunctions or premature aging are also considered which may assist in getting information about random numbers. To counter this kind of attacks, the TOE must ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy. The introduction of this new class enables to specify the quality metric that must be used.

6.1.3 Extended Family FIA_API - Authentication Proof of Identity

6.1.3.1 Description

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Application note: The other families of the Class FIA describe only the authentication verification of users identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 3 (cf. [CC3], chapter Explicitly stated IT security requirements(APE_SRE)) from a TOE point of view.

6.1.3.2 Extended Components

Extended Component FIA_API.1

Description

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

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

There are no actions defined to be auditable.

Definition

FIA_API.1 Authentication Proof of Identity

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

Dependencies: No dependencies.

6.1.4 Extended Family FMT_LIM - Limited Capabilities and Availability

6.1.4.1 Description

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

Application note: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that (i)the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced or conversely (ii)the TSF is designed with high functionality, but is removed or disabled in the product in its user environment. The combination of both the requirements shall enforce the related policy.

6.1.4.2 Extended Components

Extended Component FMT_LIM.1

Description

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

Definition

FMT_LIM.1 Limited Capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: Limited capability and availability policy]

Dependencies: (FMT_LIM.2)

Extended Component FMT_LIM.2

Description

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

Definition

FMT_LIM.2 Limited Availability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: Limited capability and availability policy]

Dependencies: (FMT_LIM.1)

6.1.4.3 Rationale

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

6.1.5 Extended Family FPT_EMS - TOE Emanation

6.1.5.1 Description

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [CC2]. This family defines requirements to mitigate intelligible emanations.

6.1.5.2 Extended Components

Extended Component FPT_EMSEC.1

Description

TOE emanation has two constituents: **FPT_EMSEC.1.1:** Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data. **FPT_EMSEC.1.2:** Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

There are no management activities foreseen.

There are no actions defined to be auditable.

Definition

FPT_EMSEC.1 TOE Emanation

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

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

Dependencies: No dependencies.

7 Security Requirements

7.1 Security Functional Requirements

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

All Security Functional Requirements introduced in [PFASE] are also SFRs for the TOE and contribute to support security objectives. More specifically:

Cryptographic requirements regarding Travel Document Personalization The following Security Functional Requirements from [PFASE] contribute to support the objective regarding access control for the personalization of the logical Travel Document:

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

Application note: The Personalization Agent uses GlobalPlatform's SCP02 protocol provided by jTOP to open a secure channel with the Travel Document's chip. The above mentioned requirements specify the cryptographic algorithms that the Travel Document shall use for (1) generating the SCP02 session keys, (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 FMT_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 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.

Requirements regarding a multi-application Travel Document The following Security Functional Requirements from [PFASE] contribute to support the objective regarding the protection of the logical Travel Document 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.3-FIREWALL,
- FMT_SMR.1,

- 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-EAC/PACE and the other applets installed on the ID Platform.

Application note: According to the rationale between SFR and TSF provided in [PFASE], the FMT_MSA.2-JCRE requirement in that Security Target 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.

7.1.1 SFRs from PPs EAC and PACE - LDS FS and PACE APIs

This section describes the security functional requirements for the LDS FS API of the platform. These SFRs are instanciations from the corresponding SFR of PACE Protection Profile [PPPACE] and EAC PP [PPEAC].

7.1.1.1 Class Cryptographic Support (FCS)

FCS_CKM.1/LDS Cryptographic key generation

FCS_CKM.1.1/LDS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following:

Key Generation Algorithm	Key sizes	Standard
-Document PACE V2 Access Key (PACE)	128,192 or 256 bits (for AES)	[ICAO TR]
-Diffie-Hellman-Protocol ECDH (PACE)	224 to 521 bits	BSI's TR-03111
-Diffie-Hellman-Protocol ECDH or DH (Chip Authentication)	224 to 521 bits for ECDH, 1536 to 2048 bits for DH	BSI's TR-03110

.

Application Note:

The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [TR03110], sec. 3.1 and Annex A.1. The shared secret value is used to derive the AES or Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [ICAODoc], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/LDS.

The third row from the table above corresponds to FCS_CKM.1-key_generation in [PFASE].

FCS_COP.1/LDS Cryptographic operation

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

Iteration	Operation	Algorithm	Key Size	Standard
-SHA	**hashing**	**SHA-1, SHA 256**	**none**	**FIPS 180-2**
-SYM	**symetric authentication - encryption and decryption**	**Triple DES, AES**	**112, 128, 168, 192, 256 bits**	**FIPS 46-3 for Triple DES, FIPS 197 and ISO 10116 for AES**
-SIG_VER_RSA	**digital signature verification**	**RSA**	**1536 to 2048 bits**	**PKCS#1 v1.5**
-SIG_VER_ECDSA	**digital signature verification**	**ECDSA**	**192, 224 and 256 bits**	**ISO-15946-1 and ISO-15946-2**
-SIG_AA	**digital signature generation**	**RSA CRT**	**1536 to 2048 bits**	**ISO-9796-2, scheme 1**
-ENC	**secure messaging (PACE v2) - encryption and decryption**	**Triple DES in CBC mode and AES**	**112 bits for TDES and 128, 192 or 256 bits for AES**	**FIPS 46-3 for Triple DES, FIPS 197 and ISO 10116 for AES**
-MAC	**secure messaging - Message Authentication Code**	**Retail MAC with Triple DES, AES**	**112 bits, 128 bits, 192 bits 256 bits**	**ISO 9797 (MAC Algorithm 3 block cipher DES, Sequence Message Counter, padding mode 2) for Triple DES, NIST-838B for AES**

.

Application Note:

The first Iteration "SHA" from the table above corresponds to FCS_COP.1-APP-SHA in [PFASE]. The Iterations "SIG_VER_RSA, SIG_VER_ECDSA, SIG_AA" correspond to FCS_COP.1-Asymetric in [PFASE].

7.1.1.2 Class FIA Identification and Authentication

FIA_AFL.1/LDS Authentication failure handling

FIA_AFL.1.1/LDS The TSF shall detect when **an administrator configurable positive integer within 1 and 255** unsuccessful authentication attempts occur related to **signature verification**.

FIA_AFL.1.2/LDS When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **increase the response time by an administrator configurable positive delay in milliseconds before returning any answer to the terminal**.

7.1.1.3 Class FDP User Data Protection

FDP_RIP.1/LDS Subset residual information protection

FDP_RIP.1.1/LDS The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to and deallocation of the resource from** the following objects:

- **Session Keys (immediately after closing related communication session),**
- **the ephemeral private key ephem-SK_PICC-PACE (by having generated a DH shared secret K)**.

Application Note:

Applied to cryptographic keys, FDP_RIP.1/LDS requires a certain quality metric (any previous information content of a resource is made unavailable) for key's destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

7.1.1.4 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE_LDS Inter-TSF trusted channel

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

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

FTP_ITC.1.3/PACE_LDS [Editorially Refined] The TSF shall **enforce** communication via the trusted channel for **any data exchange between the TOE and the Terminal**.

Application Note:

The trusted IT product is the terminal. In FTP_ITC.1.3-PACE_LDS, the word 'initiate' is changed to 'enforce', as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/EAC_PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-KMAC, PACE-KEnc): this secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/LDS. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/LDS.

7.1.1.5 Class FMT Security Management

7.1.1.6 Class FPT Protection of the Security Functions

FPT_TST.1/LDS TSF testing

FPT_TST.1.1/LDS The TSF shall run a suite of self tests **at the conditions**

Tested Property	**Event**
Applet bytecode integrity	**Applet instance creation or selection**
Patch file integrity	**Travel Document Boot**
Cryptographic key integrity	**Before each static key access**
Chip sensors	**Travel Document Boot**

to demonstrate the correct operation of **the stored TSF executable code**.

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

FPT_TST.1.3/LDS The TSF shall provide authorised users with the capability to verify the integrity of **TSF**.

Application Note:

The requirement above is a rephrasing of the FCS_TST.1 security functional requirement introduced in [PFASE].

FPT_FLS.1/LDS Failure with preservation of secure state

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

- **Exposure to operating conditions where therefore a malfunction could occur,**
- **Failure detected by TSF according to FPT_TST.1/LDS**.

7.1.2 SFRs from PPs EAC and PACE - LDS Applet

This section states the security functional requirements for the PACE [PPPACE] and EAC [PPEAC] Protection Profiles.

As the LDS applet is built upon the LDS FS API of the platform and that this security target is built on composition on the platform security target, conformance to the PACE PP can be claimed by the union of the SFRs of the platform SFRs for the LDS FS API and of the SFR from this security target

7.1.2.1 Class FAU Security Audit

FAU_SAS.1/EAC_PACE Audit storage

FAU_SAS.1.1/EAC_PACE The TSF shall provide **the Manufacturer** with the capability to store **the Initialisation and Pre-Personalisation Data** in the audit records.

Application Note:

The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase "manufacturing". The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

This SFR is covered by the following TSF from the ST 7820 M11 [ICST]:

- SF_DPM Device Phase Management

7.1.2.2 Class Cryptographic Support (FCS)

FCS_CKM.4 Cryptographic key destruction

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

FCS_RND.1/EAC_PACE Quality metric for random numbers

FCS_RND.1.1/EAC_PACE The TSF shall provide a mechanism to generate random numbers that meet **the *STANDARD* level specified in [ANSSI]**.

Application Note:

The requirement above is a rephrasing of the FCS_RND.1-APP security functional requirement introduced in [PFASE]. This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE and EAC) as required by FIA_UAU.4/EAC_PACE.

7.1.2.3 Class FIA Identification and Authentication

FIA_UID.1/EAC_PACE Timing of identification

FIA_UID.1.1/EAC_PACE The TSF shall allow

- **carrying out the Terminal Authentication Protocol**
- **carrying out the Chip Authentication Protocol**
- **to establish a communication channel**
- **carrying out the PACE Protocol**
- **to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_LDS**

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

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

Application Note:

User identified after a successfully performed PACE protocol is a PACE authenticated BIS-PACE. Please note that neither CAN nor MRZ effectively represent secrets (but other PACE passwords may do so), but are restricted-revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE).In the Phase 2 'Manufacturing of the TOE' the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The Travel Document manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 'Personalization of the Travel Document'. The users in

role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the Document Basic Access Keys, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to run the BAC Authentication Protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or (ii) if necessary and available by symmetric authentication as Personalization Agent (using the Personalization Agent Key).

FIA_UAU.1/EAC_PACE Timing of authentication

FIA_UAU.1.1/EAC_PACE The TSF shall allow

- **carrying out the Terminal Authentication Protocol**
- **to carry out the Chip Authentication Protocol**
- **to establish the communication channel,**
- **carrying out the PACE Protocol,**
- **to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_LDS,**
- **to identify themselves by selection of the authentication key**

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

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

Application Note:

The user authenticated after a successfully performed PACE protocol is a PACE authenticated BIS-PACE. Please note that neither CAN nor MRZ effectively represent secrets (but other PACE passwords may do so), but are restricted-revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-KMAC, PACE-KEnc), cf. FTP_ITC.1/PACE_LDS.

FIA_UAU.4/EAC_PACE Single-use authentication mechanisms

FIA_UAU.4.1/EAC_PACE The TSF shall prevent reuse of authentication data related to

- **Terminal Authentication Protocol**
- **Authentication Mechanism based on Triple-DES or AES**
- **PACE V2 Access Control Authentication Mechanism**.

Application Note:

The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful

authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

For the PACE protocol, the TOE randomly selects a nonce s of 128 bits length being (almost) uniformly distributed.

FIA_UAU.5/EAC_PACE Multiple authentication mechanisms

FIA_UAU.5.1/EAC_PACE The TSF shall provide

- **Passive Authentication**
- **Terminal Authentication Protocol (EAC)**
- **PACE V2 Access Control Authentication Mechanism**
- **Secure messaging in MAC-ENC mode**
- **Symmetric Authentication Mechanism based on Triple-DES or AES for PACE**

to support user authentication.

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

- **The TOE accepts the authentication attempt as Personalization Agent by means of the Symmetric Authentication Mechanism with Personalization Agent Key, the Terminal Authentication Protocol with Personalization Agent Keys.**
- **After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.**
- **The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism.**
- **The TOE accepts the authentication attempt as Supplemental Inspection only by means of the PACE V2 Access Control Authentication Mechanism with the Document PACE V2 Access Keys.**
- **Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol**.

Application Note:

Depending on the authentication methods used the Personalization Agent holds (i) a key for the Symmetric Authentication Mechanism or (ii) an asymmetric key pair for the Terminal Authentication Protocol (e.g. provided by the Extended Access Control PKI in a valid card verifiable certificate with appropriate encoded access rights). The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE

and personalization terminal. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of ePassport application.

FIA_UAU.6/EAC_PACE Re-authenticating

FIA_UAU.6.1/EAC_PACE The TSF shall re-authenticate the user under the conditions

- **Each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.**
- **Each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.**
- **Failure of MAC verification in a command received by the TOE**.

Application Note:

The Chip Authentication Protocol include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on CMAC, Retail-MAC or EMAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/LDS for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE reauthenticates the user for each received command and accepts only those commands received from the previously authenticated user.

The PACE protocol starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/LDS for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

FIA_API.1/EAC Authentication Proof of Identity

FIA_API.1.1/EAC The TSF shall provide a **Chip Authentication Protocol** to prove the identity of the **TOE**.

Application Note:

This SFR requires the TOE to implement the Chip Authentication Mechanism. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or ECDH) and two session keys for secure messaging in ENC_MAC mode. The terminal verifies by means of secure messaging whether the Travel Document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

7.1.2.4 Class FDP User Data Protection

FDP_ACC.1/EAC_PACE Subset access control

FDP_ACC.1.1/EAC_PACE The TSF shall enforce the **Access Control SFP (except Secure messaging and Read Binary commands)** on **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical Travel Document**.

FDP_ACF.1/EAC_PACE Security attribute based access control

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

- **Subjects:**
  - **Personalization Agent**
  - **Extended Inspection System (EAC)**
  - **Terminal**
  - **Supplemental Inspection System (PACE)**
  - **BIS-PACE,**
- **Objects:**
  - **data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document**
  - **data in EF.DG3 of the logical travel document**
  - **data in EF.DG4 of the logical travel document**
- **Security attributes:**
  - **authentication status of terminals,**
  - **Terminal Authorization**.

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

- **the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical Travel Document.**
- **the successfully authenticated Extended Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG14, EF.DG16 of the logical Travel Document.**
- **the successfully authenticated Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical Travel Document.**
- **the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical Travel Document.**

- **A BIS-PACE is allowed to read data objects from FDP_ACF.1/EAC_PACE after a successful PACE authentication as required by FIA_UAU.1/EAC_PACE.**
- **the successfully authenticated BIS-PACE is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG14, EF.DG16 of the logical Travel Document.**
- **the successfully authenticated Supplemental Inspection System is allowed to read the data of the EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG5 to EF.DG16 of the logical Travel Document**.

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

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

- **A terminal authenticated as CVCA is not allowed to read data in the EF.DG3**
- **A terminal authenticated as CVCA is not allowed to read data in the EF.DG4**
- **A terminal authenticated as DV is not allowed to read data in the EF.DG3**
- **A terminal authenticated as DV is not allowed to read data in the EF.DG4**
- **Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical Travel Document**
- **Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical Travel Document**
- **Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document**
- **Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document**
- **the Supplemental Inspection System is not allowed to read data in EF.DG3 and EF.DG4**.

Application Note:

Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE_LDS.The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

FDP_UCT.1/EAC_PACE Basic data exchange confidentiality

FDP_UCT.1.1/EAC_PACE [Editorially Refined] The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/EAC_PACE Data exchange integrity

FDP_UIT.1.1/EAC_PACE [Editorially Refined] The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.

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

Application Note:

FDP_UCT.1/EAC_PACE and FDP_UIT.1/EAC_PACE require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication to the General Inspection System. The authentication mechanism as part of the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

7.1.2.5 Class FMT Security Management

FMT_SMR.1/EAC_PACE Security roles

FMT_SMR.1.1/EAC_PACE The TSF shall maintain the roles

- **Terminal (EAC)**
- **Personalization Agent**
- **Country Verifying Certification Authority (EAC)**
- **Document Verifier (EAC)**
- **domestic Extended Inspection System (EAC)**
- **foreign Extended Inspection System (EAC)**
- **Manufacturer**
- **Terminal (PACE)**
- **Basic Inspection System (EAC)**
- **PACE authenticated BIS-PACE (PACE)**.

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

FMT_MTD.1/CVCA_INI Management of TSF data

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to **write** the

- **initial Country Verifying Certification Authority Public Key**
- **initial Country Verifying Certification Authority Certificate**
- **initial Current Date**

to

- **the Manufacturer**
- **the Personalization Agent**.

Application Note:

The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

FMT_MTD.1/CVCA_UPD Management of TSF data

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to **update** the

- **Country Verifying Certification Authority Public Key**
- **Country Verifying Certification Authority Certificate**

to **Country Verifying Certification Authority**.

Application Note:

The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates. The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal.

FMT_MTD.1/Date Management of TSF data

FMT_MTD.1.1/Date The TSF shall restrict the ability to **modify** the **Current date** to

- **Country Verifying Certification Authority**
- **Document Verifier**
- **domestic Extended Inspection System**.

Application Note:

The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [26], annex A.3.3, for details).

FMT_MTD.1/KEY_WRITE Management of TSF data

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to **write** the **Document Basic Access Keys** to **the Personalization Agent**.

Application Note:

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

FMT_MTD.1/CAPK Management of TSF data

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **create, load** the **Chip Authentication Private Key** to **the Personalization Agent**.

Application Note:

The verb 'load' means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb 'create' means here that the Chip Authentication Private Key is generated by the TOE itself. In the later case the ST writer shall include an appropriate instantiation of the component FCS_CKM.1 as SFR for this key generation.

FMT_MTD.1/PA Management of TSF data

FMT_MTD.1.1/PA The TSF shall restrict the ability to **write** the **Document Security Object (SOD)** to **the Personalisation Agent**.

Application Note:

By writing SOD into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 [Editorially Refined] The TSF shall ensure that only secure values **of the certificate chain** are accepted for **TSF data of the Terminal Authentication Protocol and the Access Control**.

Refinement:

Refinement: The certificate chain is valid if and only if

- the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,
- the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority

and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

- the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying of the Country Verifying Certification Authority is not before the Current Date of the TOE.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

FMT_SMF.1/EAC_PACE Specification of Management Functions

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

- **Initialization,**
- **Pre-personalisation,**
- **Personalisation,**
- **Configuration**.

FMT_MTD.1/INI_ENA Management of TSF data

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to **write** the **Initialisation Data and Pre-personalisation Data** to **the Manufacturer**.

FMT_MTD.1/KEY_READ Management of TSF data

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the

- **Document PACE V2 password - Chip Authentication Private Key (EAC)**
- **Personalisation Agent Keys**

to **none**.

FMT_MTD.1/INI_DIS Management of TSF data

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to **read out** the **Initialisation Data and the Pre-personalisation Data** to **the Personalisation Agent**.

Application Note:

The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

FMT_LIM.1/EAC_PACE Limited Capabilities

FMT_LIM.1.1/EAC_PACE The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced **Deploying Test Features after TOE Delivery does not allow:**

- **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed**
- **User Data to be manipulated or disclosed**
- **TSF data to be disclosed or manipulated**
- **software to be reconstructed and**
- **substantial information about construction of TSF to be gathered which may enable other attacks**

Application Note:

This SFR is covered by the following TSF from the ST 7820 M11 [ICST]:

- SF_DPM Device Phase Management

FMT_LIM.2/EAC_PACE Limited Availability

FMT_LIM.2.1/EAC_PACE The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced **Deploying Test Features after TOE Delivery does not allow:**

- **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed**
- **User Data to be manipulated and disclosed**
- **TSF data to be manipulated or disclosed**
- **software to be reconstructed**
- **substantial information about construction of TSF to be gathered which may enable other attacks**

Application Note:

Note that the term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

This SFR is covered by the following TSF from the ST 7820 M11 [ICST]:

- SF_DPM Device Phase Management

7.1.2.6 Class FPT Protection of the Security Functions

FPT_EMSEC.1/EAC_PACE TOE Emanation

FPT_EMSEC.1.1/EAC_PACE The TOE shall not emit **information of power consumption, side channel during command execution** in excess of **levels that could be measured or analyzed in the current state of the art** enabling access to **Personalization Agent Authentication Key, Chip Authentication Private Key** and **PACE session keys (PACE-K MAC, PACE-KEnc), the ephemeral private key ephem-SKPICC-PACE**.

FPT_EMSEC.1.2/EAC_PACE 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, Chip Authentication Private Key** and **PACE session keys (PACE-K MAC, PACE-KEnc), the ephemeral private key ephem-SKPICC-PACE**.

Application Note:

The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

This sfr for the TOE corresponds to

- FPT_EMSEC from [PP EAC] and
- FPT_EMS from [PP PACE].

This SFR is covered by the Security Feature SF_PS "Protection against Snooping" from the ST 7820 M11 [ICST] incldluing several security mechanisms working against data leakage, side channel attacks and Power consumption.

All recommendations provided by the the security guideline [SECGD] of the IC are followed by the jTOP Platform [PFCOMP] and more specifically the security feature "CPU higher order side channel protection". In order to exclude the possibility for differential analysis and advanced statistics, the following countermeasures have been implemented:

- All keys and secret values (DES, AES, PIN) are masked during manipulation. All values are Xored with a random number. This random number is changed within each APDU. -Random order execution only for sensitive pieces of code. This method can make differential analysis and advanced statistics more complicated.
- Variable clock speed.
- Some of the Jitters in code execution time.

FPT_PHP.3/EAC_PACE Resistance to physical attack

FPT_PHP.3.1/EAC_PACE The TSF shall resist **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

Application Note:

The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

This SFR is covered by the following TSFs from the ST 7820 M11 [ICST]:

- SF_DPM Device Phase Management
- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks
- SF_PLA Protection against Logical Attacks
- SF_CS Cryptographic Support

7.1.3 SFRs for Active Authentication Mechanisme

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

7.1.3.1 Class FIA Identification and Authentication

FIA_API.1/AA Authentication Proof of Identity

FIA_API.1.1/AA The TSF shall provide a **Active Authentication Protocol** to prove the identity of the **TOE**.

Application Note:

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

7.1.3.2 Class FMT Security Management

FMT_MTD.1/AAK_LOAD Management of TSF data

FMT_MTD.1.1/AAK_LOAD The TSF shall restrict the ability to **load** the **Active Authentication Private Key** to **the Personalisation Agent**.

FMT_MTD.1/AAK_READ Management of TSF data

FMT_MTD.1.1/AAK_READ The TSF shall restrict the ability to **read** the **Active Authentication Private Key** to **none**.

FMT_MTD.1/AARESP_READ Management of TSF data

FMT_MTD.1.1/AARESP_READ The TSF shall restrict the ability to **read** the **signed challenge returned to the Inspection System during the Active Authentication Protocol** to **Basic Inspection Systems**.

Application Note:

In order to prevent the identification of the Travel Document through the response sent to a given challenge, the Active Authentication Protocol shall be executed only within a BAC secure channel session.

7.1.3.3 Class FPT Protection of the Security Functions

FPT_EMSEC.1/AA TOE Emanation

FPT_EMSEC.1.1/AA The TOE shall not emit **information of power consumption, side channel during command execution** in excess of **levels that could be measured or analyzed in the current state of the art** enabling access to **Active Authentication Key** and **none**.

FPT_EMSEC.1.2/AA The TSF shall ensure **any users** are unable to use the following interface **smart card circuit contacts** to gain access to **Active Authentication Key** and **none**.

Application Note:

This SFR is covered by the Security Feature SF_PS "Protection against Snooping" from the ST 7820 M11 [ICST] incldluing several security mechanisms working against data leakage, side channel attacks and Power consumption. The Security Feature SF_PS covers the following SFRs from the [ICST]: FPT_PHP.3, FPT_ITT.1, FDP_ITT.1 and FDP_IFC.1.

7.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

8 TOE Summary Specification

8.1 TOE Summary Specification

This section describes the security functionalities of the TOE.

The security functionalities concerning the Platform are described in [PFASE] and are not redefined in this security target, although they must be considered for the TOE. The security functionalities from [PFASE] are reminded below:

- 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

FPT_TST.1/LDS is covered by the TSF "Key Integrity" from [PFASE].

FCS_RND.1/EAC_PACE is covered by the TSF "Random Number Generation" from [PFASE].

FAU_SAS.1/EAC_PACE is covered by the SF "Device Phase Management" from [ICST].

FPT_PHP.3/EAC_PACE is covered by SFs: "Device Phase Management", "Protection against Snooping", "Protection against Modifying Attacks", "Protection against Logical Attacks" and "Cryptographic Support" from [ICST].

FPT_EMSEC.1/EAC_PACE and FPT_EMSEC.1/AA are covered by the Security Feature SF_PS "Protection against Snooping" from [ICST].

8.1.1 Specified TSFs for LDS API

Files Access Control

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

[information removed]

PACE Authentication Protocol

This TSF provides an alternative method to Basic Access Control in order to gain access to the logical Travel Document.

Secure Messaging with an Inspection System

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

[information removed]

8.1.2 Specified TSFs for LDS Applet

Secure Messaging with a Personalization Terminal

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

[information removed]

Active Authentication Protocol

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

[information removed]

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 Travel Document.

[information removed]

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 Travel Document in a potential hostile environment. It also enables to recognize the Travel Document as a genuine one, issued by the Personalization Agent.

[information removed]

Travel Document 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 Travel Document Holder when it carries its Travel Document.

[information removed]

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 Travel Document.

[information removed]

Index

P

S

T

U