REF: 2011-14-INF-1095 v1	Created by: CERT8
Target: Expediente	Revised by: CALIDAD
Date: 17.12.2012	Approved by: TECNICO

CERTIFICATION REPORT

File: 2011-14 POLYMNIE LDS EAC applet

Applicant: B340709534 OBERTHUR TECHNOLOGIES

References:

[EXT-1368] Certification request of LDS EAC Java Applet in EAC configuration with AA v2.2

[EXT-1918] Evaluation Technical Report of LDS EAC Java Applet in EAC configuration with AA v2.2, version M4.

The product documentation referenced in the above documents.

Certification report of the product LDS EAC Java Applet in EAC configuration with AA v2.2, as requested in [EXT-1368] dated 10-06-2011, and evaluated by the laboratory Applus LGAI Technological Center S.A., as detailed in the Evaluation Technical Report [EXT-1918] received on 26/10/2012.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product LDS EAC Java Applet in EAC configuration with AA v2.2.

The TOE is composed of both an Integrated Circuit (IC), JavaCard platform and a loaded applet providing secure data management following ePassport EAC specifications [PP-EAC] and Active Authentication. The Target of Evaluation is therefore a composite TOE.

Developer/manufacturer: Oberthur Technologies.

Sponsor: Oberthur Technologies.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus LGAI Technological Center S.A..

Protection Profile: Common Criteria Protection Profile Machine Readable Travel Documents with "ICAO Application", Extended Access Control. BSI-CC-PP-0056. Version 1.10. March 2009.

Evaluation Level: Common Criteria version 3.1 revision 3, EAL4 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 09/10/2012.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_DVS.2 *Sufficiency of security measures* and AVA_VAN.5 *Advanced methodical vulnerability analysis*) have been assigned a "PASS" verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria version 3.1 revision 3 and the Common Methodology for Information Technology Security Evaluation version 3.1 revision 3.

Considering the obtained evidences during the instruction of the certification request of the product LDS EAC Java Applet in EAC configuration with AA v2.2, a positive resolution is proposed.

TOE SUMMARY

The Target of Evaluation (TOE) is a smartcard composed of the following components:

- An ID One Cosmo v7.0.1-n JavaCard platform including Global Platform support and a cryptographic libary,
- LDS EAC Java Applet in EAC configuration with AA v2.2

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

The Logical Data Structure (LDS) application is a generic filesystem that can be configured to match especially ICAO specifications for ePassports BAC and EAC and ISO specifications for IDL BAP and EAP. The configuration in the scope of this certification report is the EAC specification of this application according to [PP-EAC].

The main features provided by the LDS EAC Java Applet in EAC configuration with AA v2.2 and present in the evaluation scope are summarized in the following table:

Feature	Embedded in the product	In the Certificate scope
BAC	Yes	Yes [1]
EAC	Yes	Yes
Active Authentication (DES, AES, RSA CRT and ECC)	Yes	Yes
Cryptosystem migration (Algorithm change during certificate verification transaction)	Yes	Yes
BAP	Yes	No
EAP	Yes	No

The TOE in the scope of this Certification Report provides and Basic Access Control[1] and Extended Access Control according to the 'ICAO Doc 9303' [ICAO_P1] and [PP-EAC] and Active Authentication mechanisms.

The Basic Access Control (BAC) is a security feature that is supported by the TOE. The inspection system

- reads the printed data in the MRZ (for ePassport),
- authenticates itself as inspection system by means of keys derived from MRZ data.

After successful 3DES based authentication, the TOE provides read access to data requiring BAC rights by means of a private communication (secure messaging) with the inspection system.

The Active Authentication of the TOE is an optional feature that may be implemented. It ensures that the TOE has not been substituted, by means of a challenge-response protocol between the inspection system and the TOE. For this purpose the chip contains its own Active Authentication DES/AES key or RSA/ECC Key pair. A hash representation of Data Group 15 Secret/Public key is stored in the Document Security Object and therefore authenticated by the issuer's digital

[1] BAC is included in the scope through an objective on the environment. This configuration is specifically covered by other certification report.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

signature. If any, the corresponding Private Key is stored in the TOE's secure memory. Note that the access to DG15 is disabled if a secret key is stored. The TOE supports the loading and generation of the Active Authentication DES/AES key or RSA/ECC Key pair.

The Extended Access Control (EAC) enhances the later security features and ensures a strong and mutual authentication of the TOE and the Inspection system. This step is required to access biometric data such as fingerprints and iris stored in DG3 and DG4. In particular, the authentication steps ensures a strong secure channel able to provide confidentiality of the biometric data that are read and authentication of the Inspection system retrieving the date to perform a Match on Terminal comparison. The Extended Access Control authentication steps the TOE implements may be performed either with elliptic curve cryptography, or with RSA cryptography.

Some features of the product are put out of the evaluation scope and are therefore not part of the TOE. Here is the complete list of those functionalities:

- Standard and biometric PIN management (therefore PIN associated commands are out of scope).

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional components ALC_DVS.2 (*Sufficiency of security measures*) and AVA_VAN.5 (*Advanced methodical vulnerability analysis*), according to Common Criteria version 3.1 revision 3.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Assurance Class	Assurance components
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.5 Advanced methodical vulnerability analysis**

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria version 3.1 revision 3:

Class	Components
FAU: Security Audit	FAU_SAS.1 Audit storage
FCS: Cryptographic Support	FCS_CKM.1/Cryptographic key generation
	FCS_CKM.4 Cryptographic key destruction - MRTD
	FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation
	FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption
	FCS_COP.1/MAC Cryptographic operation – MAC
	FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD
	FCS_RND.1 Quality metric for random numbers
FIA: Identification and Authentication	FIA_UID.1 Timing of identification
	FIA_UAU.1 Timing of authentication
	FIA_UAU.4 Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
	FIA_UAU.5 Multiple authentication mechanisms
	FIA_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE
	FIA_API.1 Authentication Proof of Identity
FDP: User Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Basic Security attribute based access control
	FDP_UCT.1 Basic data exchange confidentiality
	FDP_UIT.1 Data exchange integrity
FMT: Security Management	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
	FMT_LIM.1 Limited capabilities
	FMT_LIM.2 Limited availability
	FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Prepersonalization Data
	FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
	FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Class	Components
	FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifying Certification Authority
	FMT_MTD.1/DATE Management of TSF data – Current date
	FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write
	FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key
	FMT_MTD.1/KEY_READ Management of TSF data – Key Read
	FMT_MTD.3 Secure TSF data
FPT: Protection of the Security Functions	FPT_EMSEC.1 TOE Emanation
	FPT_FLS.1 Failure with preservation of secure state
	FPT_TST.1 TSF testing
	FPT_PHP.3 Resistance to physical attack

Additionally to the SFRs defined in [PP-EAC], the following SFRs are defined due to the Active Authentication mechanism included within the TOE scope.

Class	Components
FCS: Cryptographic Support	FCS_COP.1/SIG_MRTD Cryptographic Operation
	FCS_CKM.1/ASYM Cryptographic key generation
FDP: User Data Protection	FDP_DAU.1/AA Basic Data Authentication
	FDP_ITC.1/AA Import of user data without security attributes
FMT: Security Management	FMT_MOF.1/AA Management of security functions behaviour

IDENTIFICATION

Product: LDS EAC Java Applet in EAC configuration with AA v2.2

Security Target: Polymnie Security Target EAC issue:6.

Protection Profile: Common Criteria Protection Profile Machine Readable Travel Documents with “ICAO Application”, Extended Access Control. BSI-CC-PP-0056. Version 1.10. March 2009.

Evaluation Level: Common Criteria version 3.1 revision 3 EAL4 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product LDS EAC Java Applet in EAC configuration with AA v2.2 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target. In short, it establishes the need of implementing organisational policies related to the following aspects.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Policy 01: P.BAC-PP - Fulfillment of the Basic Access Control Protection Profile

This security policy is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 77).

Policy 02: P.Sensitive_Data - Privacy of sensitive biometric reference data

This security policy is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 78).

Policy 03: P.Manufact - Manufacturing of the MRTD's chip

This security policy is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 79).

Policy 04: P.Personalization - Personalization of the MRTD by issuing State or Organization only

This security policy is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 80).

Additionally to the OSPs defined in [PP-EAC], and taking into account that these additional OSPs conform additional restrictions to those given in [PP-EAC], the following OSPs are defined in the ST:

Policy 05: Sensitive_Data_Protection

All the sensitive data are at least protected in integrity. The keys are protected in both integrity and confidentiality.

Application note:

DG3 and DG4 protection is managed by Policy 02:Sensitive_data.

Policy 06: Key_Function

All the cryptographic routines are designed in such a way that they are protected against probing and do not cause any information leakage that may be used by an attacker.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

could not be assumed, it would not be possible to assure the secure operation of the TOE.

Assumption 01: A.MRTD_Manufact - MRTD manufacturing on step 4 to 6

This assumption is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 60).

Assumption 02: A.MRTD_Delivery - MRTD delivery during steps 4 to 6

This assumption is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 61).

Assumption 03: A.Pers_Agent - Personalization of the MRTD's chip

This assumption is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 62).

Assumption 04: A.Insp_Sys - Inspection Systems for global interoperability

This assumption is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 63).

Assumption 05: A.Signature_PKI - PKI for Passive Authentication

This assumption is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 64).

Assumption 06: A.Auth_PKI - PKI for Inspection Systems

This assumption is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 65).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product LDS EAC Java Applet in EAC configuration with AA v2.2, although the agents implementing attacks have a high attack potential according to the assurance level of EAL4 + ALC_DVS.2 + AVA_VAN.5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

Threat 01: T.Read_Sensitive_Data - Read the sensitive biometric reference data

This threat is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 68).

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Threat 02: T.Forgery - Forgery of data on MRTD's chip

This threat is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 69).

Threat 03: T.Counterfeit MRTD's chip

This threat is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 70).

Threat 04: T.Abuse-Func - Abuse of Functionality

This threat is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 72).

Threat 05: T.Information_Leakage - Information Leakage from MRTD's chip

This threat is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 73).

Threat 06: T.Phys-Tamper - Physical Tampering

This threat is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 74).

Threat 07: T.Malfunction - Malfunction due to Environmental Stress

This threat is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 75).

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

Environment objective 01: OE.MRTD_Manufact - Protection of the MRTD Manufacturing

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 98).

Environment objective 02: MRTD_ Delivery - Protection of the MRTD delivery

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 99).

Environment objective 03: OE.Personalization - Personalization of logical MRTD

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 100).

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Environment objective 04: OE.Pass_Auth_Sign - Authentication of logical MRTD by Signature

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 101).

Environment objective 05: OE.Auth_Key_MRTD - MRTD Authentication Key

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 102).

Environment objective 06: OE.Authoriz_Sens_Data - Authorization for Use of Sensitive Biometric Reference Data

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 103).

Environment objective 07: OE.BAC_PP - Fulfillment of the Basic Access Control Protection Profile

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 104).

Receiving State or Organization

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

Environment objective 08: OE.Exam_MRTD - Examination of the MRTD passport book

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 106).

Environment objective 09: OE.Passive_Auth_Verif - Verification by Passive Authentication

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 107).

Environment objective 10: OE.Prot_Logical_MRTD - Protection of data from the logical MRTD

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 108).

Environment objective 11: OE.Ext_Insp_Systems - Authorization of Extended Inspection Systems

This security objective for the environment is included in the ST and it is described in the [PP-EAC] Protection Profile (paragraph 110).

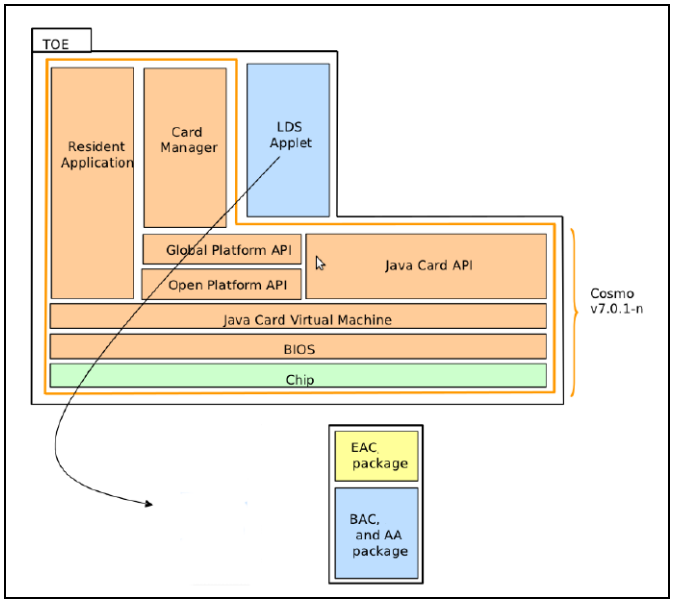
ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are detailed in the associated security target.

ARCHITECTURE

The Target of Evaluation (TOE) is a smartcard composed of the following components:

- An ID One Cosmo v7.0.1-n JavaCard platform including Global Platform support and a cryptographic library,
- An LDS applet providing both the BAC/EAC features loaded on the platform.



DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- Polymnie AGD_OPE ed.2
  - Code: FQR 220 0437 Edition: 2 Date: 14/12/2011
  - The current document aims at ensuring Common Criteria requirements for the POLYMNIE project by fully describing the AGD_OPE.
- Polymnie AGD_PRE ed.3
  - Code: FQR 220 0406 Edition: 3 Date: 27/01/2012
  - The current document aims at ensuring Common Criteria requirements for the POLYMNIE project by fully describing the AGD_PRE.
- LDS EAC V2.2 Java Applet SOFTWARE REQUIREMENTS SPECIFICATIONS SRS v edAB.
  - **Code**: 067007 00 Edition: 7-AB Date: 26/01/2011
  - This document defines the functional characteristics of the Oberthur Technologies LDS EAC applet. It contains the full description of the

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

supported file structure elements, as well as the APDU commands available during the personalization phase and the use phase.

PRODUCT TESTING

The evaluation has been performed according to the Composite Evaluation Scheme as defined in the guides [COMP_JIL] and [COMP_CCRA] in order to assess that the combination of the TOE with the underlying platform did not lead to any exploitable vulnerability. The Java Card Platform and the microcontroller have already been certified.

This evaluation has then taken into account the evaluation results and security recommendations for the following platforms which are part of the evaluated composite TOE:

- ANSSI-CC-2011/64
- ANSSI-CC-2010/40
- BSI-DSZ-CC-0645-2010
- BSI-DSZ-CC-0555-2009

The developer has executed test for all the declared security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.
During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluation team has applied a sampling strategy and concluded that the given information is complete and coherent to reproduce tests and identify the functionality tested. Moreover, additional tests where proposed independently of the developer. These tests covered ePassport EAC functionalities and tested the underlying RNG.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests according to JIL supporting documents such as [JILAAPS]. Within these activities all

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

aspects of the security architecture which were not covered by functional testing have been considered.

The implementation of the requirements of the provided platform's ETR for Composition and guidance, as well as of the security mechanisms of the applet in general has been verified by the evaluation team. An appropriate test set was devised to cover these potential vulnerabilities.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential **High** has been successful in the TOE's operational environment as defined in the security target when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE is defined by its name and version number LDS EAC Java Applet in EAC configuration with AA v2.2.

The composite TOE includes:

- the integrated circuit, IC NXP Secure Smart Card Controllers P5CD081V1A or P5CD145V0A
- the Java Card Platform ID One Cosmo v7.0.1-n masked in one of the above ICs including Global Platform support and a cryptographic library,
- the LDS EAC Java Applet in EAC configuration with AA v2.2
- the associated guidance documentation.

The commercial version and internal version of the applet may be retrieved by following the procedure below (see AGD_OPE ed.2):

1. Select the applet
2. Perform BAC or BAP if BAC/BAP is supported
3. Send GET DATA command with the tag "DF66" to retrieve the commercial version of the applet (see GET DATA in AGD_OPE). The applet shall return: "DF66 0A 067007 02020100 000000"
4. Send GET DATA command with the tag "DF67" to retrieve the internal version of the applet (see GET DATA).
    a. The applet shall return: "DF67 0E 30 0C 04040A00060D 04040F00000E" if EAC package is loaded.
5. Send GET DATA command with the tag "DF63" to retrieve the EAC configuration of the applet (see GET DATA).
    a. The applet is configured in EAC if the BAC/BAP configuration byte indicates BAC "000xxxxxb"
    b. and the EAC package is loaded (see point 4).

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

EVALUATION RESULTS

The product LDS EAC Java Applet in EAC configuration with AA v2.2 has been evaluated against the Security Target Polymnie Security Target EAC issue: 6.

All the assurance components required by the evaluation level EAL4 + ALC_DVS.2 + AVA_VAN.5 have been assigned a "PASS" verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria version 3.1 revision 3 and the Common Methodology for Information Technology Security Evaluation version 3.1 revision 3.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- The developer follows all the underlying platform security recommendations and contributes with additional countermeasures to enforce the security of the whole product. Therefore the LDS EAC Java Applet in EAC configuration with AA, Version 2.2 fulfills the requirements of CC version 3.1 with an evaluation assurance level EAL4 + ALC_DVS.2 + AVA_VAN.5.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product LDS EAC Java Applet in EAC configuration with AA v2.2, a positive resolution is proposed.

Additionally, the Certification Body wants to remark to the TOE's consuming organizations the following:

- Oberthur's Project Leader at Manilla's facilities plays a key role in the security procedures followed to generate the TOE. Project Leader at this facility assures by following the security procedures that the generated TOE reflects its implementation representation managed in the Configuration Management System.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

GLOSSARY

AA	Active Authentication
BAC	Basic Access Control
CC	Common Criteria
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
DG	Data Group
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ICAO	International Civil Aviation Organization
IDL	ISO compliant Driving Licence
LDS	Logical Data structure
MRTD	Machine readable Travel Document
MRZ	Machine readable Zone
OC	Organismo de Certificación
ST	Security Target
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R3 Final, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R3 Final, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R3 Final, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R3 Final, July 2009.

[JILCOMP] Composite product evaluation for Smart Cards and similar devices version 1.2. Jan. 2012.

[CCCOMP] Composite product evaluation for Smartcards and similar devices Version 1.0. Sept. 2007.

[JILAAPS] Application of Attack Potential to Smartcards, Version 2.7. March 2009.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

[PP-EAC] Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.10. BSI-CC-PP-0056. Version 1.10. March 2009.

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

[ICAO_P1] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization

[ISO18013-1] Information Technology - Personal Identification – ISO Compliant Driving Licence – Part 1:Physical characteristics and basic data set, ISO/IEC FDIS 18013-1:2005(E)

[ISO18013-2] Information Technology - Personal Identification — ISO Compliant Driving Licence — Part 2: Machine-readable technologies, ISO/IEC FDIS 18013-2:2007(E)

[ISO18013-3] Personal Identification — ISO Compliant Driving Licence — Part 3: Access control, authentication and integrity validation, ISO/IEC FDIS 18013-3:2008(E)

SECURITY TARGET

Along with the certification report, the complete security target for the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- **Polymnie Security Target EAC issue:6 – Document id.: FQR : 110 5693**

The public version of this document constitutes the ST Lite. The ST Lite has also been evaluated for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- **Polymnie Security Target EAC Ed.1 – Document id.: FQR 110 6342 Ed.1**

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es