REF: 2011-15-INF-1098 v1	Created by: CERT8
Target: Expediente	Revised by: CALIDAD
Date: 17.12.2012	Approved by: TECNICO

CERTIFICATION REPORT

File: 2011-15 POLYMNIE LDS EAP applet

Applicant: B340709534 OBERTHUR TECHNOLOGIES

References:

[EXT-1369] Certification request of LDS EAC Java Applet in EAP configuration with AA v2.2

[EXT-1919] Evaluation Technical Report of LDS EAC Java Applet in EAP configuration with AA v2.2, version M4.

The product documentation referenced in the above documents.

Certification report of the product POLYMNIE, as requested in [EXT-1369] dated on 10-06-2011, and evaluated by the laboratory APPLUS-LGAI, as detailed in the Evaluation Technical Report [EXT-1919] 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

EXECUTIVE SUMMARY **3**
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 5
SECURITY FUNCTIONAL REQUIREMENTS 6
IDENTIFICATION **7**
SECURITY POLICIES **7**
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT **8**
CLARIFICATIONS ON NON-COVERED THREATS 10
OPERATIONAL ENVIRONMENT FUNCTIONALITY 13
ARCHITECTURE **16**
DOCUMENTS **16**
PRODUCT TESTING **17**
PENETRATION TESTING 18
EVALUATED CONFIGURATION **18**
EVALUATION RESULTS **19**
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM **19**
CERTIFIER RECOMMENDATIONS **20**
GLOSSARY **20**
BIBLIOGRAPHY **21**
SECURITY TARGET **21**

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 EAP 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 [ISO18013-1], [ISO18013-2] and [ISO18013-3] EAP IDL specifications 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: No conformance to any Protection Profile is claimed.

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 EAP 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 library,
- LDS EAC Java Applet in EAP 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 IDL EAP specification of this application.

The main features provided by the LDS EAC Java Applet in EAP 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	No
Active Authentication (DES, AES, RSA CRT and ECC)	Yes	Yes
Cryptosystem migration (Algorithm change during certificate verification transaction)	Yes	No
BAP	Yes	Yes[1]
EAP	Yes	Yes

The TOE in the scope of this Certification Report provides Basic Access Protection[1] and Extended Access Protection according to [ISO18013-1][ISO18013-2] [ISO18013-3] and Active Authentication mechanisms.

The Basic Access Protection (BAP) is especially used in the context of IDL as an alternative to BAC. Indeed it is actually a generalization of BAC allowing usage of extra algorithms and key length. It exists in 4 modes:

- BAP1 - 3DES with key length of 128 bits (equivalent to BAC),
- BAP2 - AES with key length of 128 bits,
- BAP3 - AES with key length of 192 bits,
- BAP4 - AES with key length of 256 bits.

Following Secure messaging is performed using the algorithm used in the selected BAP mode.

Note that the term MRZ is specific to ICAO standard; [ISO18013-3] uses the term “Keydoc” which refers to an equivalent unique identifier printed on the physical TOE as a random number or barcode.

[1] BAC/BAP are included in the scope through an objective on the environment but these configurations are specifically covered by other certification reports.

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

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 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 Protection (EAP) extends EAC to allow a more flexible protocol. It can protect up to 24 DGs (from 1 to 24) and is no more restricted to DG3 and 4. Note that a BAP must be performed prior to starting EAP.

Following secure messaging can be either in 3DES or AES taking into that the algorithm used must be the same as the one used for BAP.

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
	FCS_COP.1/SHA Cryptographic operation
	FCS_COP.1/SYM Cryptographic operation
	FCS_COP.1/MAC Cryptographic operation
	FCS_COP.1/SIG_VER Cryptographic operation
	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
	FIA_UAU.5 Multiple authentication mechanisms
	FIA_UAU.6 Re-authenticating
	FIA_API.1 Authentication Proof of Identity
FDP: User Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 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
	FMT_MTD.1/INI_DIS Management of TSF data
	FMT_MTD.1/CVCA_INI Management of TSF data
	FMT_MTD.1/CVCA_UPD Management of TSF data
	FMT_MTD.1/DATE Management of TSF data
	FMT_MTD.1/KEY_WRITE Management of TSF data
	FMT_MTD.1/CAPK Management of TSF data
	FMT_MTD.1/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

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
	FPT_PHP.3 Resistance to physical attack
Active Authentication	
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
Extended Access Protection	
FCS: Cryptographic Support	FCS_COP.1/EAP-SM Cryptographic Operation
	FCS_CKM.1/EAP Cryptographic key generation

IDENTIFICATION

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

Security Target: Polymnie Security Target EAP issue:7.

Protection Profile: No conformance to any Protection Profile is claimed.

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 EAP 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.

Policy 01: P.BAP-PP

The issuing organisations or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRD data DG1, DG2, DG5 to DG24 if specified in EF.SOD as well as to the data groups Common and Security Data. The MRD is successfully evaluated and certified in accordance with the "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control" [PP-BAC] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRD data.

Policy 02: P.Sensitive_Data

The highly sensitive reference data are sensitive private personal data of the MRD holder. The highly sensitive reference data can be used only by inspection systems which are authorized for this access at the time the MRD is presented to the inspection system (Extended Inspection Systems). The issuing organisation authorizes the Document Verifiers of the receiving organisations to manage the

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

authorization of inspection systems within the limits defined by the Document Verifier Certificate. The MRD'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.

Policy 03: P.Manufact

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

Policy 04: P.Personalization

The issuing organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the highly sensitive reference data and other data of the logical MRD with respect to the MRD holder. The personalization of the MRD for the holder is performed by an agent authorized by the issuing organisation only.

Policy 05: P.Sensitive_Data_Protection

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

Policy 06: P.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 could not be assumed, it would not be possible to assure the secure operation of the TOE.

Assumption 01: A.MRD_Manufact

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

Assumption 02: A.MRD_Delivery

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

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.

Assumption 03: A.Pers_Agent

The Personalization Agent ensures the correctness of(i) the logical MRD with respect to the MRD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key if stored on the MRD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRD'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.

Assumption 04: A.Insp_Sys

The Inspection System is used by the border control officer of the receiving organisation (i) examining an MRD presented by the holder and verifying its authenticity and (ii) verifying the holder as MRD holder. The Basic Inspection System for global interoperability (i) includes the Organisation Signing CA Public Key and the Document Signer Public Key of each issuing organisation, and (ii) implements the terminal part of the Basic Access Protocol [ISO18013-3]. The Basic Inspection System reads the logical MRD under Basic Access Protocol and performs the Passive Authentication to verify the logical MRD.

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 MRD'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 organisation through the Document Verifier of the receiving organisation to read the highly sensitive reference data.

Assumption 05: A.Signature_PKI

The issuing and receiving organisations or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRD. The issuing organisation runs a Certification Authority (CA) which securely generates, stores and uses the Organisation Signing CA Key pair. The CA keeps the Organisation Signing CA Private Key secret and is recommended to distribute the Organisation Signing CA Public Key to ICAO, all receiving organisations 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)

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

uses securely the Document Signer Private Key for signing the Document Security Objects of the MRDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving organisations.

Assumption 06: A.Auth_PKI

The issuing and receiving organisations or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Protocol. The Organisation 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 Organisation Verifying Certification Authorities of the issuing organisations 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 organisations or Organizations. The issuing organisations or Organizations distribute the public keys of their Organisation Verifying Certification Authority to their MRD's chip.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product LDS EAC Java Applet in EAP 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

Adverse action: An attacker tries to gain the highly sensitive reference data through the communication interface of the MRD's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [PP-BAC]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRD's chip) but differs from those in the asset under the attack (highly sensitive reference data vs. digital keydoc, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the highly sensitive reference data are stored only on the MRD's chip as private sensitive personal data whereas the keydoc data and the portrait are visually readable on the physical MRD as well.

Threat agent: having high attack potential, knowing the Document Basic Access Keys, being in possession of a legitimate MRD

Asset: confidentiality of sensitive logical MRD (i.e. highly sensitive reference) data

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

Adverse action: An attacker alters fraudulently the complete stored logical MRD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRD holder's identity or highly sensitive reference data.

This threat comprises several attack scenarios of MRD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed keydoc and in the digital keydoc to claim another identity of the holder. 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 highly sensitive reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRDs to create a new forged MRD, e.g. the attacker writes the digitized portrait and optional highly sensitive reference finger data read from the logical MRD of a holder into another MRD's chip leaving their digital keydoc unchanged to claim the identity of the holder this MRD. The attacker may also copy the complete unchanged logical MRD to another contactless chip.

Threat agent: having high attack potential, being in possession of one or more legitimate MRDs.

Asset: authenticity of logical MRD data.

Threat 03: T.Counterfeit

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

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

Threat agent: having high attack potential, being in possession of one or more legitimate MRDs

Asset: authenticity of logical MRD data,

Threat 04: T.Abuse-Func

Adverse action: 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.

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

This threat addresses the misuse of the functions for the initialization and the personalization in the operational organisation after delivery to MRD holder.

Threat agent: having high attack potential, being in possession of a legitimate MRD.

Asset: confidentiality and authenticity of logical MRD and TSF data, correctness of TSF.

Threat 05: T.Information_Leakage

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

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements.

This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

Threat agent: having high attack potential, being in possession of a legitimate MRD.

Asset: confidentiality of logical MRD and TSF data.

Threat 06: T.Phys-Tamper

Adverse action: An attacker may perform physical probing of the MRD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRD's chip Embedded Software. An attacker may physically modify the MRD's chip in order to (i) modify security features or functions of the MRD's chip, (ii) modify security functions of the MRD's 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 highly sensitive reference data for the inspection system) or TSF Data (e.g. authentication key of the MRD'' 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 MRD's chip internals. Techniques

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

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.

Threat agent: having high attack potential, being in possession of a legitimate MRD.

Asset: confidentiality and authenticity of logical MRD and TSF data, correctness of TSF.

Threat 07: T.Malfunction

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

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

Threat agent: having high attack potential, being in possession of a legitimate MRD.

Asset: confidentiality and authenticity of logical MRD and TSF data, correctness of TSF.

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.MRD_Manufact

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

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

Environment objective 02: OE.MRD_ Delivery

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

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

- non-disclosure of any security relevant information, o 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.

Environment objective 03: OE.Personalization

The issuing organisation must ensure that the Personalization Agents acting on behalf of the issuing organisation (i) establish the correct identity of the holder and create biographical data for the MRD, (ii) enroll the highly sensitive reference data of the MRD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

Environment objective 04: OE.Pass_Auth_Sign

The issuing organisation must (i) generate a cryptographic secure Organisation Signing CA Key Pair, (ii) ensure the secrecy of the Organisation Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Organisation Signing CA Public Key to receiving organisations maintaining its authenticity and integrity. The issuing organisation must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving organisations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG24 if stored in the LDS according to [ICAO_P1] and [ISO18013-2].

Environment objective 05: OE.Auth_Key_MRD

The issuing organisation has to establish the necessary public key infrastructure in order to (i) generate the MRD's Chip Authentication Key Pair, (ii) sign and store the

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

Chip Authentication Public Key in the Chip Authentication Public Key data and (iii) support inspection systems of receiving organisations or organizations to verify the authenticity of the MRD's chip used for genuine MRD by certification of the Chip Authentication Public Key by means of the Document Security Object.

Environment objective 06: OE.Authoriz_Sens_Data

The issuing organisation has to establish the necessary public key infrastructure in order to limit the access to highly sensitive reference data of MRD's holders to authorized receiving organisations or Organizations. The Organisation Verifying Certification Authority of the issuing organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

Environment objective 07: OE.BAP-PP

It has to be ensured by the issuing organisation, that the TOE is additionally successfully evaluated and certified in accordance with the "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control" [PP-BAC].

This is necessary to cover the BAP mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

Receiving State or Organization

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

Environment objective 08: OE.Exam_MRD

The inspection system of the receiving organisation must examine the MRD presented by the holder to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRD. The Basic Inspection System for global interoperability (i) includes the Organisation Signing CA Public Key and the Document Signer Public Key of each issuing organisation, and (ii) implements the terminal part of the Basic Access Protocol [ICAO_P1]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRD's chip.

Environment objective 09: OE.Passive_Auth_Verif

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

Environment objective 10: OE.Prot_Logical_MRD

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

The inspection system of the receiving organisation ensures the confidentiality and integrity of the data read from the logical MRD. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

Environment objective 11: OE.Ext_Insp_Systems

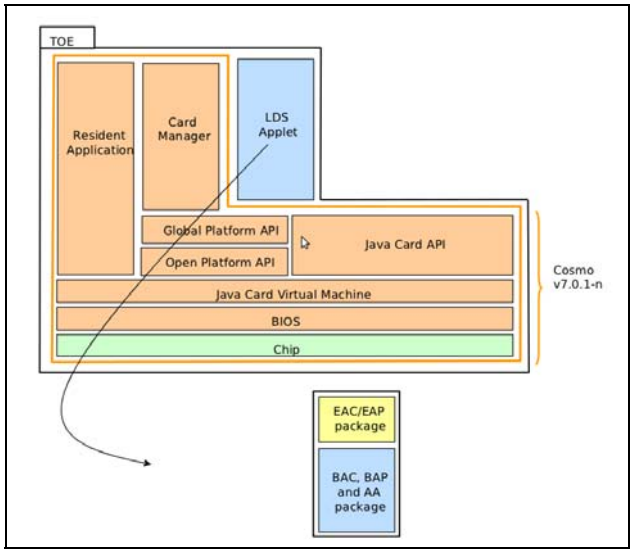
The Document Verifier of receiving organisations or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to highly sensitive reference data of the logical MRD. The Extended Inspection System authenticates themselves to the MRD's chip for access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

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 BAP/EAP 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.

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

- 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 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

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

where proposed independently of the developer. These tests covered ePassport EAP 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 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 EAP 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 EAP 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

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

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 EAP if the BAC/BAP configuration byte indicates BAP (001xxxxxb for BAP-1, 010xxxxxb for BAP-2, 011xxxxxb for BAP-3, and 100xxxxxb for BAP-4.)
    b. and the EAC package is loaded (see point 4).

EVALUATION RESULTS

The product LDS EAC Java Applet in EAP configuration with AA v2.2 has been evaluated against the Security Target Polymnie Security Target EAP issue: 7.

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 EAP configuration with AA, Version 2.2 fulfils the requirements of CC version 3.1 with an evaluation assurance level EAL4 + ALC_DVS.2 + AVA_VAN.5.

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

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product LDS EAC Java Applet in EAP 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.

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

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

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.
[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 EAP issue:7 – Document id.: FQR : 110 5695**

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

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 EAP Ed.2 – Document id.: FQR 110 6344 Ed2**

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