REF: 2012-9-INF-1200 v1	Created by: CERT8
Target: Expediente	Revised by: CALIDAD
Date: 21.05.2013	Approved by: TECNICO

CERTIFICATION REPORT

File: 2012-9 KONA102 EAC

Applicant: 109-81-53365 KONA I Co., Ltd.

References:

[EXT-1700] Certification request of KONA102 EAC

[EXT-2162] Evaluation Technical Report of KONA102 EAC.

The product documentation referenced in the above documents.

Certification report of the product Kona102 ePassport v1 .1 on P5CD081, as requested in [EXT-1700] dated 27-03-2012, and evaluated by the laboratory APPLUS-LGAI, as detailed in the Evaluation Technical Report [EXT-2162] received on 09/05/2013.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**
TOE SUMMARY 4
SECURITY ASSURANCE REQUIREMENTS 5
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION **7**
SECURITY POLICIES **7**
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT **8**
CLARIFICATIONS ON NON-COVERED THREATS 9
OPERATIONAL ENVIRONMENT FUNCTIONALITY 10
ARCHITECTURE **12**
DOCUMENTS **12**
PRODUCT TESTING **13**
PENETRATION TESTING 13
EVALUATED CONFIGURATION **14**
EVALUATION RESULTS **14**
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM **15**
CERTIFIER RECOMMENDATIONS **15**
GLOSSARY **16**
BIBLIOGRAPHY **16**
SECURITY TARGET **18**

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
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 Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2.

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control and Extended Access Control according to the 'ICAO Doc 9303' [ICAO-01] and BSI TR-03110 [TR-03], respectively.

It provides the security level of EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

The TOE type of the current security target is "the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Extended Access Control", compatible with the expected TOE type described in the [PP-EAC].

Developer/manufacturer: KONA I Co., Ltd.

Sponsor: KONA I Co., Ltd.

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 Document with "ICAO Application", Extended Access Control version 1.10, 25th March 2009. BSI-CC-PP-0056.

Evaluation Level: Common Criteria v3.1 r3 EAL5 + AVA_VAN.5 + ALC_DVS.2.

Evaluation end date: 09/05/2013.

All the assurance components required by the evaluation level EAL5 (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 EAL5 + AVA_VAN.5 + ALC_DVS.2, as defined by the Common Criteria v3.1 r3 and the CEM v3.1 r3.

Considering the obtained evidences during the instruction of the certification request of the product Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2, a positive resolution is proposed.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TOE SUMMARY

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control, the Active Authentication and the Extended Access Control according to 'ICAO Doc 9303' [ICAO-01] and BSI TR-03110 [TR-03], respectively.

The TOE comprises of:

- the circuitry of the MRTD's chip (the integrated circuit, IC NXP Secure Smart Card Controllers P5CD081V1A)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system Kona102 ePassport version 1.1.2),
- the MRTD application and
- the associated guidance documentation.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

The TOE covered by this Certification Report addresses the protection of the logical MRTD

(i) in integrity by write-only-once access control and by physical means, and

(ii) in confidentiality by the Extended Access Control Mechanism.

The TOE also addresses Active Authentication as stated in [ICAO-03].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this Certification Report as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Due to the fact that [PPBAC] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately.

The TOE is conformant with the Protection Profile, BSI-CC-PP-0056, Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.10 [PP-EAC].

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfill the evaluation level EAL5 and the evidences required by the additional components AVA_VAN.5 and ALC_DVS.2, according to Common Criteria v3.1 r3.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.1 Implementation representation of the TSF
	ADV_INT.2 Well-structured internals
	ADV_TDS.4 Well-structured internals
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.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.2 Compliance with implementation standards
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
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.3 Testing: modular 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:

Class	Components
FAU: Security Audit	FAU_SAS.1 Audit storage
FCS: Cryptographic Support	FCS_CKM.1/DH Cryptographic key generation - Diffie-Hellman Keys by the TOE
	FCS_CKM.1/ECDH Cryptographic key generation – Elliptic Curve Diffie-Hellman Keys by the TOE
	FCS_CKM.4 Cryptographic key destruction - MRTD

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Class	Components
	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_RSA Cryptographic operation – Signature verification by MRTD
	FCS_COP.1/SIG_VER_ECDSA Cryptographic operation – Signature verification by MRTD
	FCS_COP.1/AA Cryptographic operation – Signature creation by MRTD – Active Authentication
	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
	FIA_API.1/AA 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
	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/AAPK Management of TSF data – Active Authentication Private Key
	FMT_MTD.1/KEY_READ Management of TSF data – Key Read
	FMT_MTD.1/KEY_READ_AA Management of TSF data – Key Read
	FMT_MTD.3 Secure TSF data
FPT: Protection of the Security Functions	FPT_EMSEC.1 TOE Emanation
	FPT_EMSEC.1/AA TOE Emanation
	FPT_FLS.1 Failure with preservation of secure state

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Class	Components
	FPT_TST.1 TSF testing
	FPT_PHP.3 Resistance to physical attack

The applicable security target does not introduce any additional threat, organization security policy or assumption to those defined in the PP. The developer has only applied iteration operations over several SFR to differentiate features of the additional mechanism Active Authentication over the existing requirements in the PP:

- FCS_CKM.1/DH and FCS_CKM.1/ECDH (because two kinds of key exchanging are implemented)
- FCS_COP.1/SIG_VER_ECDSA (DSA verification with EC)
- FCS_COP.1/AA
- FIA_API.1/AA
- FMT_MTD.1/AAPK
- FMT_MTD.1/KEY_READ_AA
- FPT_EMSEC.1/AA

IDENTIFICATION

Product: Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2

Security Target:

Document No:	SP-02-02
Document Title:	Kona102 ePassport with EAC Security Target
Version:	1
Revision:	8
Release date:	19/04/2013

Protection Profile: Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control version 1.10, 25th March 2009. BSI-CC-PP-0056.

Evaluation Level: Common Criteria v3.1 r3 EAL5 + AVA_VAN.5 + ALC_DVS.2.

SECURITY POLICIES

The use of the product Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2 shall implement a set of security policies assuring the fulfillment 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 organizational policies related to the following aspects.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
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 MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (paragraph 80).

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.MRTD_Manufact MRTD manufacturing on step 4 to 6

This assumption is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (paragraph 61).

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

This assumption is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (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 MRTD, "ICAO Application", Extended Access Control PP (paragraph 63).

Assumption 05: A.Signature_PKI PKI for Passive Authentication

This assumption is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 64).

Assumption 06: A.Auth_PKI PKI for Inspection Systems

This assumption is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 65).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2, although the agents implementing attacks have a high attack potential according to the assurance level of EAL5 + AVA_VAN.5 + ALC_DVS.2 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 MRTD, "ICAO Application", Extended Access Control PP (paragraph 68).

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

This threat is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 69).

Threat 03: T.Counterfeit MRTD's chip

This threat is included in the ST and it is described in the MRTD, "ICAO Application", Extended Access Control PP (paragraph 70).

Threat 04: T.Abuse-Func Abuse of Functionality

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (paragraph 73).

Threat 06: T.Phys-Tamper Physical Tampering

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 74).

Threat 07: T.Malfunction Malfunction due to Environmental Stress

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 75).

OPERATIONAL ENVIRONMENT FUNCTIONALITY

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

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

Issuing State or Organization

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

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 MRTD, “ICAO Application", Extended Access Control PP (paragraph 98).

Environment objective 02: OE.MRTD_ Delivery Protection of the MRTD delivery

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (paragraph 100).

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

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (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 MRTD, “ICAO Application", Extended Access Control PP (paragraph 108).

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

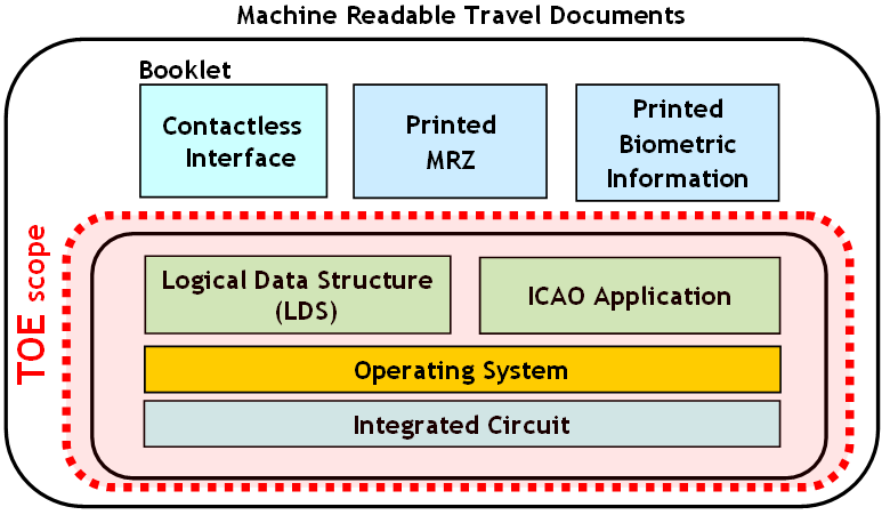
This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control PP (paragraph 110).

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

ARCHITECTURE

The TOE is a composition of IC hardware and embedded software that controls the IC.



The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

DOCUMENTS

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

- Kona102 ePassport Technical Manual, version 1.3 [GU]. This guide is delivered to the card holder (Card holder or receiving State).
- Kona102 ePassport Proprietary Command Manual, version 1.5 [GP]. This guide is delivered to the personalization agent (Issuing State).
- Kona102 ePassport Delivery Procedure Version 1.2 [DEL]. This guide is used by all the entities to deliver the TOE between them.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

PRODUCT TESTING

The evaluation has been performed according to the Composite Evaluation Scheme as defined in the guides [JILCOMP] and [JILADVARC] in order to assess that the combination of the TOE with the underlying platform did not lead to any exploitable vulnerability.

This evaluation has then taken into account the evaluation results and security recommendations for the platform which is part of the evaluated composite TOE, and was already certified with certificate 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, each test unit has been executed to check that the declared security functionality has been identified and also to check that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using a 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 has concluded that the information is complete and coherent enough to reproduce tests and identify the functionality tested. Moreover, the evaluation team has planned and executed additional tests independently of those executed by the developer. The latter tests covered the TOE EAC functionalities and Active Authentication mechanism. The underlying RNG has been also tested.

The obtained results have been checked to be conformant to the expected results and in cases where a deviation relative to the expected results has been detected, 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 [JILAAPS] and [JILADVARC]. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered.

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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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 Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2.

The TOE is composed of:

- the circuitry of the MRTD's chip (the integrated circuit, IC NXP Secure Smart Card Controllers P5CD081V1A)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system Kona102 ePassport version 1.1.2),
- the MRTD application and
- the associated guidance documentation

The commercial version and internal version of the applet may be retrieved by following the procedure in section *6.1.6.2. Reading Card Information and Card Serial Number* of [GP].

The resumed procedure is as follows:

1. The Personalization Agent (Phase 3 of [PP-EAC]) must send command GET DATA to the TOE: APDU==00ca004600
2. Then, the Personalization Agent must check the first 5 bytes of the response to verify that the TOE identification is the following:

Items Version	Meaning
IC identification	'01 02' – Kona102: IC NXP P5CD081V1A
Version	'01'
Revision	'01'
Update (patch)	'02'

Note: This information is no longer available once the TOE has been issued to the Card Holder.

EVALUATION RESULTS

The product Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2 has been evaluated against the Security Target SP-02-02 Kona102 ePassport with EAC Security Target version 1.8.

All the assurance components required by the evaluation level EAL5 + AVA_VAN.5 + ALC_DVS.2 have been assigned a "PASS" verdict. Consequently, the laboratory APPLUS LGAI TECHNOLOGICAL CENTER S.A. assigns the "**PASS**" **VERDICT** to

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL5 + AVA_VAN.5 + ALC_DVS.2, as defined by the Common Criteria v3.1 r3 and the CEM v3.1 r3.

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.

During the ADV class evaluation the evaluator detected that the Manufacturing and Personalization lifecycle stages as described in the BSI-CC-PP-0056 is implemented as a single logical lifecycle stage. This implies that it would be possible for a card that has some MRTD data on it to be patched and the MRTD data would be disclosed.

However, the TOE implementation of the patching mechanism is done with a key that is different from the personalization one. Moreover the patching mechanism is not available once the personalization has been finished by setting the card into OPERATIVE state. As an additional security measure the card is not usable if the lifecycle stage is not OPERATIVE so it is not possible to have a working card with MRTD data in a stage that is not OPERATIVE.

The evaluator assessed that the MRTD data is secure if the Issuer uses the SET_LIFE_CYCLE to set the card into OPERATIVE state once the MRTD personalization is finished.

Additionally, the evaluation team states that the developer follows all the underlying platform security recommendations and contributes with additional countermeasures to enforce the security of the whole product.

Therefore the Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2 fulfills the requirements of CC version 3.1 with an evaluation assurance level EAL5 + ALC_DVS.2 + AVA_VAN.5.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Kona102 ePassport [EAC configuration], Version 1 Revision 1 Update(patch) 2, a positive resolution is proposed.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

GLOSSARY

AA	Active Authentication
BAC	Basic Access Control
BIS	Basic Inspection System
CC	Common Criteria
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
EIS	Extended Inspection System
ETR	Evaluation Technical Report
GIS	General Inspection System
ICAO	International Civil Aviation Organization
IT	Information Technology
MRTD	Machine Readable Travel Document
OC	Organismo de Certificación
OSP	Organizational security policy
PA	Passive Authentication
PP	Protection Profile
RNG	Random Number Generator
SAR	Security assurance requirements
SFP	Security Function Policy
SFR	Security functional requirement
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functions

BIBLIOGRAPHY

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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

[CC_P1] Common Criteria v3.1 r3for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R3 Final, July 2009.

[CC_P2] Common Criteria v3.1 r3for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R3 Final, July 2009.

[CC_P3] Common Criteria v3.1 r3for 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.

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

[PP-BAC] Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.10. BSI-PP-0055. March 2009. Bundesamt für Sicherheit in der Informationstechnik.

[ICAO-01] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization.

[ICAO-03] Internal Civil Aviation Organization. Machine Readable Travel Documents, Part 3, Vol 1 - Specifications for Electronically Enabled MRTDs with Biometric Identification Capability, version 3, edition 2008, International Civil Aviation Organization.

[TR-03] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, Bundesamt für Sicherheit in der Informationstechnik (BSI).

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

[JILAAPS] Application of Attack Potential to Smartcards, Version 2.8. Jan. 2012.

[JILADVARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices. Version 2.0. Jan. 2012.

[CCDB-2006-04-004] ST sanitising for publication. CCMC. Apr. 2006.

[GU] Kona102 ePassport Technical Manual, version 1.3. Kona I. Jan. 2013.

[GP] Kona102 ePassport Proprietary Command Manual, version 1.5. Apr. 2013.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

[DEL] Kona102 ePassport Delivery Procedure Version 1.2. Kona I. Feb. 2013.

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:

- **SP-02-02 Kona102 ePassport with EAC Security Target. Version 1.8. April 2013.**

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed 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:

- **SP-02-19 Kona102 ePassport with EAC Security Target Lite. Version: 1.2. May 2013.**

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es