MINISTERIO DE LA PRESIDENCIA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2011-10-INF-836 v1	Created by: CERT8
Target: Público	Revised by: CALIDAD
Date: 17.04.2012	Approved by: TECNICO

CERTIFICATION REPORT

File: 2011-10 KONA 102J1 ePassport BAC v1.1

Applicant: KEBTechnology Co., Ltd.

References:

[EXT-1364] Certification request of KONA 102J1 ePassport BAC

[EXT-1564] Evaluation Technical Report of KONA 102J1 ePassport BAC

The product documentation referenced in the above documents.

Certification report of the product Kona102J1 ePassport v1.1, as requested in [EXT-1364] dated 30/05/2011, and evaluated by the laboratory Applus LGAI Technological Center S.A., as detailed in the Evaluation Technical Report [EXT-1564] received on 01/03/2012.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Kona102J1 ePassport v1.1.

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 according to the 'ICAO Doc 9303' [ICAO-01].

The TOE provides the security level of EAL4 augmented with ALC_DVS.2.

The TOE type 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", compatible with the expected TOE type described in the [PP-BAC].

Developer/manufacturer: Korea Electronic Banking Technology Co., Ltd.

Sponsor: Korea Electronic Banking Technology Co., Ltd.

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

ITSEF: Applus LGAI Technological Center S.A.

Protection Profile: BSI-CC-PP-0055. Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.10.

Evaluation Level: Common Criteria v3.1 r3 EAL4 + ALC_DVS.2.

Evaluation end date: 01/03/2012.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_DVS.2) 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, 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 Kona102J1 ePassport v1.1, a positive resolution is proposed.

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 according to 'ICAO Doc 9303' [ICAO-01].

- the NXP J3A081 Revision 3 Secure Smartcard Controller (named JCOP v2.4.1), comprising of
    - the circuitry of the MRTD's chip (the integrated circuit, IC NXP Secure Smart Card Controllers P5CD081V1A),
    - the IC Embedded Software (operating system): JCOP v2.4.1 Revision 3,
- the MRTD application: ePassport Kona102J1 v1.1 Applet that is compliant with [ICAO-01].
- the associated guidance documentation.

The TOE is conformant with the Protection Profile, BSI-CC-PP-0055, Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.10 [PP-BAC].

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

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

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

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system

(i) reads optically the MRTD,

(ii) authenticates itself as inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO-01], normative appendix 5.

This Certification Report **does not** cover the Active Authentication and the Extended Access Control as optional security mechanisms.

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 component ALC_DVS.2, according to Common Criteria v3.1 r3.

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

Assurance Class	Assurance components
	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
	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.3 Focused vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 r3:

Class	Components
FAU: Security Audit	FAU_SAS.1 Audit storage
FCS: Cryptographic Support	FCS_CKM.1/Cryptographic key generation - Generation of Document Basic Access Keys by the TOE
	FCS_CKM.4 Cryptographic key destruction - MRTD
	FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation
	FCS_COP.1/ENC Cryptographic operation – Encryption / Decryption Triple DES
	FCS_COP.1/AUTH Cryptographic operation – Authentication
	FCS_COP.1/MAC Cryptographic operation – Retail MAC
	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_AFL.1 Authentication failure handling
FDP: User Data Protection	FDP_ACC.1 Subset access control – Basic Access control
	FDP_ACF.1 Basic Security attribute based access control – Basic Access Control
	FDP_UCT.1 Basic data exchange confidentiality - MRTD

Class	Components
	FDP_UIT.1 Data exchange integrity - MRTD
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/KEY_WRITE Management of TSF data – Key Write
	FMT_MTD.1/KEY_READ Management of TSF data – Key Read
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

IDENTIFICATION

Product: Kona102J1 ePassport v1.1

Security Target: Kona102J1 ePassport with BAC Security Target v1.1.

Protection Profile: BSI-CC-PP-0055. Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.10.

Evaluation Level: Common Criteria v3.1 r3 EAL4 + ALC_DVS.2.

SECURITY POLICIES

The use of the product Kona102J1 ePassport v1.1 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.Manufact - Manufacturing of the MRTD’s chip

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

Policy 02: 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-BAC] Protection Profile (paragraph 74).

Policy 03: P.Personal_Data - Personal data protection policy

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

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 [PP-BAC] Protection Profile (paragraph 54).

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-BAC] Protection Profile (paragraph 55).

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-BAC] Protection Profile (paragraph 56).

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

This assumption is included in the ST and it is described in the [PP-BAC] Protection Profile (paragraph 57).

Assumption 05: A.BAC-Keys - Cryptographic quality of Basic Access Control Keys

This assumption is included in the ST and it is described in the [PP-BAC] Protection Profile (paragraph 59).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Kona102J1 ePassport v1.1, although the agents implementing attacks have an **Enhanced-Basic** attack potential according to the assurance level of EAL4 + 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.Chip_ID - Identification of MRTD's chip

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

Threat 02: T.Skimming - Skimming the logical MRTD

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

Threat 03: T.Eavesdropping - Eavesdropping to the communication between TOE and inspection system

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

Threat 04: T.Forgery - Forgery of data on MRTD's chip

This threat is included in the ST and it is described in the [PP-BAC] Protection Profile (paragraph 66).

Threat 05: T.Abuse-Func - Abuse of Functionality

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

Threat 06: T.Information_Leakage - Information Leakage from MRTD's chip

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

Threat 07: T.Phys-Tamper - Physical Tampering

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

Threat 08: T.Malfunction Malfunction due to Environmental Stress

This threat is included in the ST and it is described in the [PP-BAC] Protection Profile (paragraph 71).

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-BAC] Protection Profile (paragraph 94).

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-BAC] Protection Profile (paragraph 95).

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-BAC] Protection Profile (paragraph 96).

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-BAC] Protection Profile (paragraph 97).

Environment objective 05: OE.BAC-Keys Cryptographic quality of Basic Access Control Keys

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

Environment objective 06: 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-BAC] Protection Profile (paragraph 100).

Environment objective 07: 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-BAC] Protection Profile (paragraph 101).

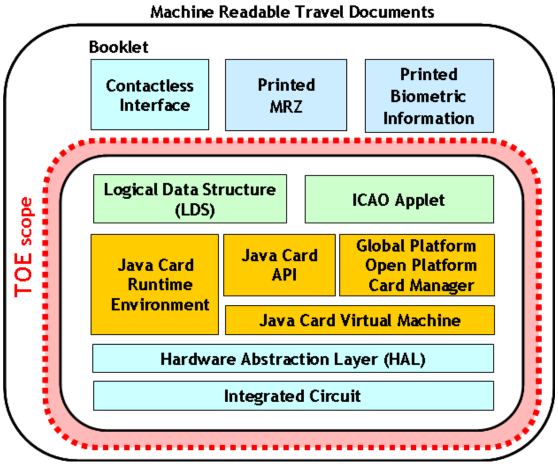
Environment objective 08: OE.Prot_Logical_MRTD - Protection of data from the logical MRTD

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

The details of the product operational environment (assumptions, threats and organisational 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.


Machine Readable Travel Documents
Booklet
Contactless Interface
Printed MRZ
Printed Biometric Information
TOE scope
Logical Data Structure (LDS)
ICAO Applet
Java Card Runtime Environment
Java Card API
Global Platform Open Platform Card Manager
Java Card Virtual Machine
Hardware Abstraction Layer (HAL)
Integrated Circuit

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

1. *"(SP-03-01) Kona102J1 ePassport with EAC Security Target v1.2",* in a lite and public version.
2. *"(SP-03-05) Kona102J1 ePassport Proprietary Command Manual v1.0",* May 2011. KEBT.
3. *"(SP-03-06) Kona102J1 ePassport Technical Manual v1.0",* May 2011. KEBT.
4. *"(SP-03-08) Kona102J1 ePassport Life-Cycle Definition v1.0",* August 2011. KEBT.
5. *"(SP-03-11) Kona102J1 ePassport Delivery Procedure v1.1",* December 2011. KEBT.

PRODUCT TESTING

The developer has executed test for all the 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 on the developer functional tests in the testing platform implemented in the evaluation laboratory. The evaluation team has concluded the obtained information during the repeated tests was enough to reproduce tests devised by the developer, identify the functionality tested, confirm the expected results and gain confidence on developer's tests as the information was complete and coherent.

Moreover, additional tests where proposed independently of the developer. These tests covered the ePassport BAC 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. 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 have 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 **Enhanced-Basic** 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 **Kona102J1 ePassport v1.1**.

The composite TOE includes:

- the NXP J3A081 Revision 3 Secure Smartcard Controller (named JCOP v2.4.1), comprising of
    - the circuitry of the MRTD's chip (the integrated circuit, IC NXP Secure Smart Card Controllers P5CD081V1A),
    - the IC Embedded Software (operating system): JCOP v2.4.1 Revision 3,

- the MRTD application: ePassport Kona102J1 v1.1 Applet that is compliant with [ICAO-01], and
- the associated guidance documentation.

The GET DATA command* available in the TOE can be used by TOE's consumers (Issuers) to verify if the acquired product corresponds to the certified version of the TOE. The first 5 bytes of GET DATA command response included below, specifically correspond to the certified TOE, Kona102J1 ePassport v1.1.

GET DATA response:

10 21 01 00 00 (5 bytes) → Kona102J1 ePassport version 1.1

* Specific detail on GET DATA command can be found in *"(SP-03-05) Kona102J1 ePassport Proprietary Command Manual v1.0"* which is distributed along with the TOE.

EVALUATION RESULTS

The product Kona102J1 ePassport v1.1 has been evaluated against the Security Target Kona102J1 ePassport with BAC Security Target v1.1.

All the assurance components required by the evaluation level EAL4 + ALC_DVS.2 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, 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.

- The developer follows all the underlying platform security recommendations and contributes with additional countermeasures to enforce the security of the whole product. Therefore the Kona102J1 ePassport v1.1 fulfils the requirements of CC version 3.1 with an evaluation assurance level EAL4 + ALC_DVS.2.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Kona102J1 ePassport v1.1, a positive resolution is proposed.

Additionally, the Certification Body wants to clarify that the GET DATA command cited in this Certification Report, provides information strictly related to the code masked in the ROM of the TOE.

GLOSSARY

BAC	Basic Access Control
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
OC	Organismo de Certificación
PP	Protection Profile
ROM	Read-Only Memory
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.

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

[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).

[PRE] ORDEN PRE/2740/2007 Reglamento de evaluación y certificación de seguridad de las tecnologías de la información. 19/09/2007.

[CCDB-2008-04-001] Application of Attack Potential to Smartcards Version 2.7 February 2009.

[CCDB-2007-09-001] Composite product evaluation for Smart Cards and similar

Devices Version 1.0 Revision 1. September 2007

[AM] Attack Methods for Smartcards and Similar Devices Version 1.5. February 2009

[C5401456] AVA_VAN.5 evaluation methodology M0. 2009-03-10

[ARC] ADV_ARC guidance Security Architecture requirements (ADV_ARC) Version 1.0 draft 1. June 2008

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Kona102J1 ePassport with BAC Security Target v1.1.