Reference: 2017-14-INF-2572-v1
Target: Público
Date: 13.11.2018

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-14**
TOE	**KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00**
Applicant	**KONA@I - KONA I Co., Ltd.**
References	

[EXT-3334] Certification Request

[EXT-4363] Evaluation Technical Report

Certification report of the product KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00, as requested in [EXT-3334] dated 27/03/2017, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-4363] received on 19/10/2018.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00.

The TOE defines the security objectives and requirements for the contactless smart card programmed according to ICAO Technical Report "Supplemental Access Control" [ICAO SAC] (which means amongst others according to the Logical Data Structure (LDS) defined in 'ICAO Doc 9303') and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [ICAO 9303] and BSI TR-03110-1 [TR-03110-1], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE [PP-PACE]. It provides the security level of EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

Developer/manufacturer: KONA I Co., Ltd.

Sponsor: KONA I Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profiles:

- Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, version 1.3.2 (5th December 2012).
- Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, version 1.01 (22th July 2014).

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1, R4 – EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 19/10/2018.

All the assurance components required by the evaluation level EAL5 (augmented with ALC_DVS.2 and AVA_VAN.5) have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria for Information Technology Security Evaluation Version 3.1, R4 and the Common Methodology for Information Technology Security Evaluation Version 3.1, R4.

Considering the obtained evidences during the instruction of the certification request of the product KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00, 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 Extended Access Control with PACE", compatible with the expected TOE type described in [PP-PACE] and [PP-EAC].

The TOE comprises:

- the circuitry of the MRTD's chip (16-Bit RISC Microcontroller for Smart Cards, S3FT9MG rev 0)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (KONA2 D2320N ePassport version 02.10.00),
- the associated guidance documentation.

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.

This security target addresses the Chip Authentication Version 1 described in BSI TR-03110-1 as an alternative to the Active Authentication stated in ICAO Doc 9303.

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. For the PACE protocol according to SAC, the following steps shall be performed:

1) The travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with thedomain parameters to the terminal.
2) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
3) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
4) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [ICAO SAC], [TR-03110-1].

The security target requires the TOE to implement the Extended Access Control as defined in BSI TR-03110-1.

The Extended Access Control consists of two parts:

(i) the Chip Authentication Protocol Version 1 and

(ii) the Terminal Authentication Protocol Version 1.

The Chip Authentication Protocol v.1:

(i) authenticates the travel document's chip to the inspection system and

(ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed.

The Terminal Authentication Protocol v.1 consists of

(i) the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and

(ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection Systems Certificates.

The TOE is conformant with the following Protection Profiles:

- Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, version 1.3.2 (5th December 2012).
- Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, version 1.01 (22th July 2014).

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 and the evidences required by the additional components ALC_DVS.2 and AVA_VAN.5, according to Common Criteria for Information Technology Security Evaluation Version 3.1, R4.

Security assurance requirements	Titles
Class 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
Class ADV: Development	
ADV_ARC.1	Architectural design
ADV_FSP.5	Functional specification
ADV_IMP.1	Implementation representation
ADV_INT.2	TSF internals
ADV_TDS.4	TOE design
Class AGD: Guidance documents	
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative user guidance
Class ALC: Life-cycle support	
ALC_CMC.4	CM capabilities
ALC_CMS.5	CM scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development security
ALC_LCD.1	Life-cycle definition
ALC_TAT.2	Tools and techniques
Class ATE: Tests	
ATE_COV.2	Coverage
ATE_DPT.3	Depth
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing
Class AVA: Vulnerability analysis	
AVA_VAN.5	Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria for Information Technology Security Evaluation Version 3.1, R4:

Security functional requirement	Title
FAU_SAS.1	Audit storage
FCS_CKM.1/DH_PACE	Cryptographic Key generation – Diffie-Hellman for PACE session keys
FCS_CKM.1/CA	Cryptographic Key generation – Diffie-Hellman for Chip Authentication session keys
FCS_CKM.1/PACE_CAM	Cryptographic Key generation – Diffie-Hellman for Chip

	Authentication Mapping session keys
FCS_CKM.4	Cryptographic key destruction – Session key
FCS_COP.1/PACE_ENC	Cryptographic operation – Encryption / Decryption AES/3DES
FCS_COP.1/PACE_MAC	Cryptographic operation – MAC
FCS_COP.1/CA_ENC	Cryptographic operation – Symmetric Encryption / Decryption
FCS_COP.1/CA_MAC	Cryptographic operation – MAC
FCS_COP.1/PACE_CAM_ENC	Cryptographic operation – Symmetric Encryption / Decryption
FCS_COP.1/PACE_CAM_MAC	Cryptographic operation – MAC
FCS_COP.1/SIG_VER	Cryptographic operation – Signature verification by travel document
FCS_RND.1	Quality metric for random numbers
FIA_AFL.1/TRANS	Authentication failure handling - Transport key authentication
FIA_AFL.1/ISSUER	Authentication failure handling - Issuer authentication
FIA_AFL.1/PACE	Authentication failure handling - PACE authentication
FIA_UID.1/TRANS	Timing of identification
FIA_UID.1/ISSUER	Timing of identification
FIA_UID.1/PACE	Timing of identification
FIA_UID.1/PACE_CAM	Timing of identification
FIA_UAU.1/TRANS	Timing of authentication
FIA_UAU.1/ISSUER	Timing of authentication
FIA_UAU.1/PACE	Timing of authentication
FIA_UAU.1/PACE_CAM	Timing of authentication
FIA_UAU.4/PACE	Single-use authentication mechanisms – Single-use authentication of the Terminal by the TOE
FIA_UAU.4/PACE_CAM	Single-use authentication mechanisms – Single-use authentication of the Terminal by the TOE
FIA_UAU.5/PACE	Multiple authentication mechanisms
FIA_UAU.5/PACE_CAM	Multiple authentication mechanisms
FIA_UAU.6/PACE	Re-authenticating of Terminal by the TOE
FIA_UAU.6/EAC	Re-authenticating of Terminal by the TOE
FIA_UAU.6/PACE_CAM	Re-authenticating of Terminal by the TOE
FIA_API.1/CA	Authentication Proof of Identity
FIA_API.1/PACE_CAM	Authentication Proof of Identity
FDP_ACC.1/TRM	Subset access control
FDP_ACF.1/TRM	Security attribute based access control
FDP_RIP.A	Subset residual information protection
FDP_UCT.1/TRM	Basic data exchange confidentiality – MRTD
FDP_UIT.1/TRM	Data exchange integrity
FMT_SMF.1	Specification of management functions
FMT_SMR.1/PACE	Security roles
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1/INI_ENA	Management of TSF data – writing initialization and pre-personalization data

FMT_MTD.1/INI_DIS	Management of TSF data – reading and using initialization and pre-personalization data
FMT_MTD.1/KEY_READ	Management of TSF data – key read
FMT_MTD.1/PACE_CAM_KEY_READ	Management of TSF data – key read
FMT_MTD.1/PA	Management of TSF data – Personalisation agent
FMT_MTD.1/PACE_CAMPA	Management of TSF data – Personalisation agent
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/CAPK	Management of TSF data – Chip Authentication Private Key
FMT_MTD.1/PACE_CAMPK	Management of TSF data – Chip Authentication Private Key
FMT_MTD.3	Secure TSF data
FPT_EMS.1	TOE Emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF Testing
FPT_PHP.3	Resistance to physical attack
FTP_ITC.1/PACE	Inter-TSF trusted channel after PACE

IDENTIFICATION

Product: KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00

Security Target: KONA2 D2320N ePassport EAC with PACE Security Target, version 1.22 (14th May 2018).

Protection Profile:

- Machine Readable Travel Document with “ICAO Application", Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, version 1.3.2 (5th December 2012).
- Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, version 1.01 (22th July 2014).

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1, R4 EAL5 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00 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 travel document's chip

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.3.

Policy 02: P.Pre-Operational Pre-operational handling of the travel document

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.3.

Policy 03: P.Card_PKI PKI for Passive Authentication (issuing branch)

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.3.

Policy 04: P.Trustworthy_PKI Trustworthiness of PKI

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.3.

Policy 05: P.Terminal Abilities and trustworthiness of terminals

This security policy is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.3.

Policy 06: P.Sensitive_Data Privacy of sensitive biometric reference data

This security policy is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE[PP-EAC], Chap 3.4.

Policy 07: P.Personalisation Personalisation of the travel document by issuing State or Organisation only

This security policy is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [PP-EAC], Chap 3.4.

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.Passive_Auth PKI for Passive Authentication

This assumption is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE] Chap 3.4).

Assumption 02: A.Insp_Sys Inspection Systems for global interoperability

This assumption is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [PP-EAC], Chap 3.2.

Assumption 03: A.Auth_PKI PKI for Inspection Systems

This assumption is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [PP-EAC], Chap 3.2.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00, although the agents implementing attacks have the attack potential High according to the components of EAL5 + 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.Skimming Skimming travel document / Capturing Card-Terminal Communication

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.2.

Threat 02: T.Eavesdropping Eavesdropping on the communication between the TOE and the PACE terminal

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.2.

Threat 03: T.Tracing Tracing travel document

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.2.

Threat 04: T.Forgery Forgery of Data

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.2.

Threat 05: T.Abuse-Func Abuse of Functionality

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE],Chap 3.2.

Threat 06: T.Information_Leakage Information Leakage from travel document

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.2.

Threat 07: T.Phys-Tamper Physical Tampering

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.2.

Threat 08: T.Malfunction Malfunction due to Environmental Stress

This threat is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE], Chap 3.2.

Threat 09: T.Read_Sensitive_Data Read the sensitive biometric reference data

This threat is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [PP-EAC],Chap3.3.

Threat 10: T.Counterfeit Counterfeit of travel document chip data

This threat is included in the ST and it is described in the Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE [PP-EAC], Chap 3.3.

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.Auth_Key_Travel_Document Travel document 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 with PACE [PP-EAC] (section4.2).

Environment objective 02: 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 with PACE [PP-EAC] (section4.2).

Environment objective 03: OE.Exam_Travel_Document Examination of the physical part of the travel document

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [PP-EAC] (section4.2).

Environment objective 04: OE.Prot_Logical_Travel_Document Protection of data from the logical travel document

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Extended Access Control with PACE [PP-EAC] (section4.2).

Environment objective 05: 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 with PACE [PP-EAC] (section4.2).

Environment objective 06: OE.Legislative_Compliance Issuing of the travel document

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE] (section 4.2).

Environment objective 07: OE.Passive_Auth_Sign Authentication of travel document by Signature

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE] (section 4.2).

Environment objective 08: OE.Personalisation Personalisation of travel document

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE] (section 4.2).

Environment objective 09: OE.Terminal Terminal operating

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE] (section 4.2).

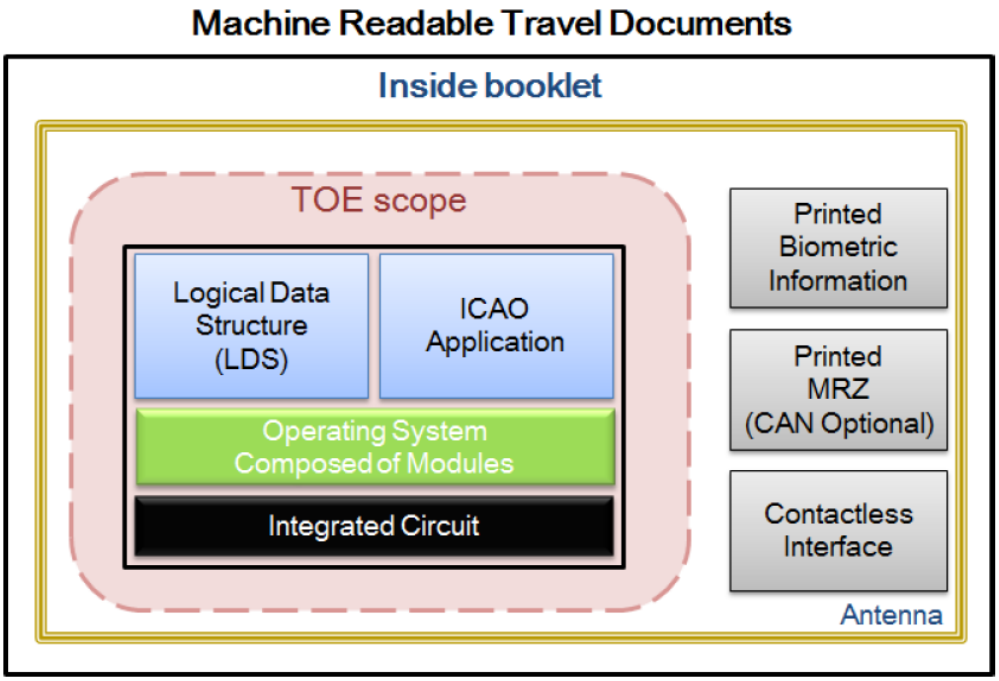
Environment objective 10: OE.Travel_Document_Holder Travel document holder Obligations

This security objective for the environment is included in the ST and it is described in the Machine Readable Travel Document using Standard Inspection Procedure with PACE [PP-PACE] (section 4.2).

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

- KONA2 D2320N ePassport Operational Guidance, version 01.16. This guide is delivered to the card holder (Card holder or receiving State).
- KONA2 D2320N ePassport Preparative Guidance, version 01.16. This guide is delivered to the personalization agent (Issuing State).
- KONA2 D2320N ePassport Delivery Procedure 01.14. This guide is used by all the entities to deliver the TOE between them.

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 evaluator has repeated all the developer functional tests in the developer premises. Likewise, he has selected and repeated all of the developer functional tests in the testing platform implemented in the evaluation laboratory.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

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 [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.

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 KONA2 D2320N ePassport (EAC with PACE configuration) version 02 revision 10 patch 00.

The TOE is composed of:

- the circuitry of the MRTD's chip (16-Bit RISC Microcontroller for Smart Cards, S3FT9MGrev 0)

- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (KONA2 D2320NePassport V02.10.00),
- the associated guidance documentation.

The version of the software may be retrieved by following the procedure in section 7 "*Secure acceptance of the TOE*" of the Preparative Procedure Guidance document.

The issuer shall verify that the card information data is identical with values in the following table:

Response Data	Length	Value
Card Information	10	'44' '32' '01' '40' '4E' '31' '02' '00' '10' '00'
Card Serial Number	8	'xx' 'xx' 'xx' 'xx' 'xx' 'xx' 'xx' 'xx'

The identification of all the information returned by the TOE is:

- 44: (ASCII) meaning 'D' related to ODA and I/F where ODA=DDA , IF=DI.
- 32: (ASCII) '2' related to IC vendor (Samsung).
- 01 40: (hex-decimal) '320' meaning 320 KB of IC memory.
- 4E: (ASCII) 'N' meaning native platform .
- 31:(ASCII) '1'meaning the first revision of the IC (S3FT9MG rev 0).
- 02 00 10: meaning TOE version 02.10.
- 00:meaning update (patch) version 00 (no patch has been done).

The Card Serial Number is generated for each card uniquely by the IC manufacturer(Samsung) and it does not need to be checked.

EVALUATION RESULTS

The product KONA2 D2320N ePassport [EAC with PACE configuration] version 02 revision 10 update 00 has been evaluated against the Security Target KONA2 D2320N ePassport EAC with PACE Security Target, version 1.22 (14th May 2018).

All the assurance components required by the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria for Information Technology Security Evaluation Version 3.1, R4 and the Common Methodology for Information Technology Security Evaluation Version 3.1, R4.

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.

There is no additional recommendation from the Laboratory in order to use the TOE since guidance documentation is enough to make a secure usage of the TOE.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Applus Laboratories, a positive resolution is proposed.

The CCN Certification Body strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on the applicable guidance in section DOCUMENTS of this certification report, as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

Regarding the use of 3DES algorithm, users should consider the following certifier recommendation:

- The algorithm 3DES is supported by the TOE only for backward compatibility with ICAO 9303 terminals. According to TR-03110, the 3DES is deprecated for CA and PACE authentication operation, so users should use AES for the implementation of CA or PACE.

GLOSSARY

AA	Active Authentication
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CAM	Chip Authentication Mapping
CAN	Card Access Number
CC	Common Criteria
CCN	Centro Criptológico Nacional
EAC	Extended Access Control
EAL	Evaluation Assurance Level
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
MRZ	Machine readable Zone
OC	Organismo de Certificación
OSP	Organizational security policy
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RNG	Random Number Generator
SAR	Security assurance requirements
SFP	Security Function Policy
SFR	Security functional requirement
SOD	Security object Data
ST	Security Target
TA	Terminal Authentication
TOE	Target Of Evaluation
TOE	Target of evaluation
TSF	TOE Security Functions

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, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CCDB-2006-04-004] Common Criteria. Additional CCRA Supporting Documents. ST sanitising for publication. Document number 2006-04-004, April 2006.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.

[ICAO 9303] Doc Series, ICAO Doc 9303, Machine Readable Travel Documents, seventh Edition, 2015. ICAO.

[ICAO SAC] International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010. ICAO.

[JILAAPS] Application of Attack Potential to Smartcards, version 2.9. Jan. 2013. Joint Interpretation Library.

[JILADVARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.0. Jan 2012. Joint Interpretation Library.

[PP-EAC] Machine Readable Travel Document with “ICAO Application", Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, version 1.3.2 (5th December 2012). BSI.

[PP-PACE] Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, version 1.01 (22th July 2014). BSI.

[TR-03110-1] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents -Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26. February 2015. BSI.

SECURITY TARGET

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

- KONA2 D2320N ePassport EAC with PACE Security Target, version 1.22 (14th May 2018).

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:

- KONA2 D2320N ePassport EAC with PACE Security Target Lite, version 1.00 (7th November 2018).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.
The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.
The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.