Reference: 2017-13-INF-2571-v1
Target: Público
Date: 13.11.2018

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

CERTIFICATION REPORT

Dossier #	**2017-13**
TOE	**KONA2 D2320N ePassport [BAC Configuration] version 02 revision 10 update 00**
Applicant	**KONA@I - KONA I Co., Ltd.**
References	

[EXT-3333] Certification Request

[EXT-4360] Evaluation Technical Report

Certification report of the product KONA2 D2320N ePassport [BAC Configuration] version 02 revision 10 update 00, as requested in [EXT-3333] dated 27/03/2017, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-4360] received on 19/10/2018.

CONTENTS

EXECUTIVE SUMMARY 3

TOE SUMMARY 4

SECURITY ASSURANCE REQUIREMENTS 4

SECURITY FUNCTIONAL REQUIREMENTS 5

IDENTIFICATION 7

SECURITY POLICIES 7

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 7

CLARIFICATIONS ON NON-COVERED THREATS 8

OPERATIONAL ENVIRONMENT FUNCTIONALITY 9

ARCHITECTURE 11

DOCUMENTS 11

PRODUCT TESTING 12

PENETRATION TESTING 12

EVALUATED CONFIGURATION 13

EVALUATION RESULTS 13

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 14

CERTIFIER RECOMMENDATIONS 14

GLOSSARY 14

BIBLIOGRAPHY 15

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) 16

RECOGNITION AGREEMENTS 17

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 17

International Recognition of CC – Certificates (CCRA) 17

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product KONA2 D2320N ePassport [BAC Configuration] version 02 revision 10 update 00.

The TOE defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security method Basic Access Control in the 'ICAO Doc 9303' [ICAO]. It provides the security level of EAL4 augmented with ALC_DVS.2.

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 Basic Access Control", compatible with the expected TOE type described in the [PP-BAC]

Developer/manufacturer: KONA I Co., Ltd.

Sponsor: KONA I Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-CC-PP-0055 version 1.10 (25th March 2009).

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1, R4 – EAL4 + ALC_DVS.2.

Evaluation end date: 19/10/2018.

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 Laboratories assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4, 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 [BAC 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 the Basic Access Control according to 'ICAO Doc 9303' [ICAO 9303].

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 Basic Access Control Mechanism.

The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

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.

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].

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 for Information Technology Security Evaluation Version 3.1, R4.

Security assurance requirements	**Titles**
Class ADV: Development	
ADV_ARC.1	Architectural design
ADV_FSP.4	Functional specification
ADV_IMP.1	Implementation representation
ADV_TDS.3	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.4	CM scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development security
ALC_LCD.1	Life-cycle definition
ALC_TAT.1	Tools and techniques
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 ATE: Tests	
ATE_COV.2	Coverage
ATE_DPT.1	Depth
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing
Class AVA: Vulnerability analysis	
AVA_VAN.3	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	Cryptographic Key generation – Generation of Document Basic Access Keys by the TOE
FCS_CKM.4	Cryptographic key destruction – MRTD
FCS_COP.1/SHA	Cryptographic key operation – Hash for key derivation
FCS_COP.1/ENC	Cryptographic key operation – Encryption /Decryption Triple DES
FCS_COP.1/AUTH	Cryptographic key operation – Authentication
FCS_COP.1/MAC	Cryptographic key operation – Retail MAC
FCS_RND.1	Quality metric for random numbers
FIA_UID.1/TRANS	Timing of identification
FIA_UID.1/ISSUER	Timing of identification
FIA_UID.1/BAC	Timing of identification
FIA_UAU.1/TRANS	Timing of authentication
FIA_UAU.1/ISSUER	Timing of authentication
FIA_UAU.1/BAC	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/TRANS	Authentication failure handling - Transport key authentication
FIA_AFL.1/ISSUER	Authentication failure handling - Issuer authentication
FIA_AFL.1/BAC	Authentication failure handling - BAC authentication
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
FDP_UIT.1	Data exchange integrity – MRTD
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 pre-personalization data
FMT_MTD.1/INI_DIS	Management of TSF data – disabling or 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_EMSEC.1	TOE Emanation
FPT_TST.1	Failure with preservation of secure state
FPT_FLS.1	TSF testing
FPT_PHP.3	Resistance to physical attack

IDENTIFICATION

Product: KONA2 D2320N ePassport [BAC Configuration] version 02 revision 10 update 00

Security Target: KONA2 D2320N ePassport BAC Security Target, version 1.18 (14th May 2018).

Protection Profile: Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-CC-PP-0055 version 1.10 (25th March 2009).

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1, R4 EAL4 + ALC_DVS.2.

SECURITY POLICIES

The use of the product KONA2 D2320N ePassport [BAC 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 MRTD's chip

This security policy is included in the ST and it is described in the MRTD, "ICAO Application", Basic Access Control PP (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 MRTD, "ICAO Application", Basic Access Control PP (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 MRTD, "ICAO Application", Basic Access Control PP (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 MRTD, "ICAO Application", Basic Access Control PP (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 MRTD, "ICAO Application", Basic Access Control PP (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 MRTD, "ICAO Application", Basic Access Control PP (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 MRTD, "ICAO Application", Basic Access Control PP (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 MRTD, "ICAO Application", Basic Access Control PP (paragraph 59)

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product KONA2 D2320N ePassport [BAC Configuration] version 02 revision 10 update 00, although the agents implementing attacks have the attack potential according to the Enhanced Basic of EAL4 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 MRTD, "ICAO Application", Basic Access Control PP (paragraph 63).

Threat 02: T.Skimming Skimming the logical MRTD

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Basic Access Control PP, 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 MRTD, “ICAO Application", Basic Access Control PP (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 MRTD, “ICAO Application", Basic Access Control PP (paragraph 66).

Threat 05: T.Abuse-Func Abuse of Functionality

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

Threat 07: T.Phys-Tamper Physical Tampering

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

Threat 08: T.Malfunction Malfunction due to Environmental Stress

This threat is included in the ST and it is described in the MRTD, “ICAO Application", Basic Access Control PP (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 MRTD, “ICAO Application", Basic Access Control PP (paragraph 94).

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", Basic Access Control PP (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 MRTD, “ICAO Application", Basic Access Control PP (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 MRTD, “ICAO Application", Basic Access Control PP (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 MRTD, “ICAO Application", Basic Access Control PP (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 MRTD, “ICAO Application", Basic Access Control PP (paragraph 100).

Environment objective 07: OE.Passive_Auth_Verif Verification by Passive Authenticationt

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Basic Access Control PP (paragraph 101

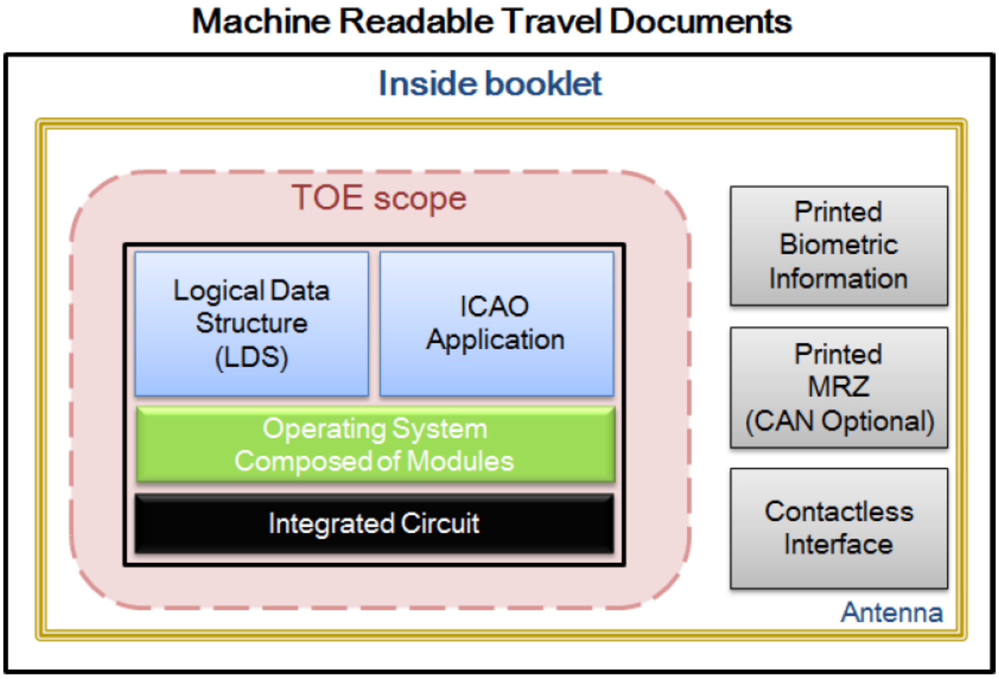
Environment objective 08: OE.Prot_Logical_MRTD Protection of data from the logical MRTD

This security objective for the environment is included in the ST and it is described in the MRTD, “ICAO Application", Basic Access Control PP (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 an embedded software that controls the IC.


Machine Readable Travel Documents
Inside booklet
TOE scope
Logical Data Structure (LDS)
ICAO Application
Operating System Composed of Modules
Integrated Circuit
Printed Biometric Information
Printed MRZ (CAN Optional)
Contactless Interface
Antenna

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

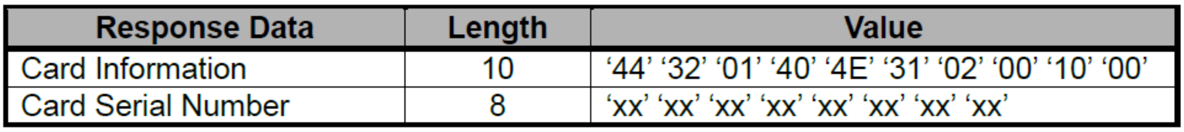
The TOE is defined by its name and version number KONA2 D2320N ePassport [BAC configuration] version 02 revision 10 update 00.

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 [BAC Configuration] version 02 revision 10 update 00 has been evaluated against the Security Target KONA2 D2320N ePassport BAC Security Target, version 1.18 (14th May 2018).

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

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.

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

[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-BAC] Machine Readable Travel Document with “ICAO Application”, Basic Access Control, BSI-CC-PP-0055 version 1.10 (25th March 2009).

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 BAC Security Target, version 1.18 (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 BAC 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.