| | |
|---|---|
| REF: 2015-30-INF-1650 v2 | Created by: CERT10 |
| Target: Público | Revised by: CALIDAD |
| Date: 23.10.2017 | Approved by: TECNICO |

# CERTIFICATION REPORT

File:        2015-30 KONA2 ePassport BAC

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

References:

[EXT-2850] Certification request of KONA2 ePassport BAC

[EXT-3077] Evaluation Technical Report of KONA2 ePassport BAC.

The product documentation referenced in the above documents.

Certification report of the product KONA2 D2320N ePassport (BAC configuration) version 01 revision 03 patch 00, as requested in [EXT-2850] dated 04/11/2016, and evaluated by the laboratory Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-3077] received on 13/06/2016.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product KONA2 D2320N ePassport (BAC configuration) version 01 revision 03 patch 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) del Centro Nacional de Inteligencia (CNI).

**ITSEF**: Applus Laboratories.

**Protection Profile**: Common Criteria Protection Profile Machine Readable Travel Documents with "ICAO Application", Basic Access Control. Version 1.10. March 2009. BSI-CC-PP-0055.

**Evaluation Level**: Common Criteria v3.1 R4 EAL4 + ALC_DVS.2.

**Evaluation end date**: 13/06/2016.

All the assurance components required by the evaluation level EAL4 augmented with ALC_DVS.2 (Sufficiency of security measures) 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 + ALC_DVS.2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product KONA2 D2320N ePassport (BAC configuration) version 01 revision 03 patch 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-01].

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 V01.03.00),
- 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].

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 (Sufficiency of security measures), according to Common Criteria v3.1 R4.

| Assurance Class | Assurance components |
|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description |
| | ADV_FSP.4 Complete functional specification |
| | ADV_IMP.1 Implementation representation of the TSF |
| | ADV_TDS.3 Basic modular design |
| AGD: Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| ALC: Life-cycle support | ALC_CMC.4 Production support, acceptance procedures and automation |
| | ALC_CMS.4 Problem tracking CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | **ALC_DVS.2 Sufficiency of security measures** |
| | ALC_LCD.1 Developer defined life-cycle model |
| | ALC_TAT.1 Well-defined development tools |
| ASE: Security Target evaluation | ASE_CCL.1 Conformance claims |
| | ASE_ECD.1 Extended components definition |
| | ASE_INT.1 ST introduction |
| | ASE_OBJ.2 Security objectives |
| | ASE_REQ.2 Derived security requirements |
| | 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 R4:

| 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 |
| | 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 Pre-personalization 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**: KONA2 D2320N ePassport (BAC configuration) version 01 revision 03 patch 00

**Security Target:** SP-06-01 KONA2 D2320N ePassport BAC Security Target version 1 revision 8. 2016-05-21.

**Protection Profile**: Common Criteria Protection Profile Machine Readable Travel Documents with "ICAO Application", Basic Access Control. Version 1.10, 25th March 2009. BSI-CC-PP-0055.

**Evaluation Level**: Common Criteria v3.1 R4 EAL4 + ALC_DVS.2.

# SECURITY POLICIES

The use of the product KONA2 D2320N ePassport (BAC configuration) version 01 revision 03 patch 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 01 revision 03 patch 00, although the agents implementing attacks have an <u>enhanced-basic</u> attack potential according to the assurance level EAL4 + ALC_DVS.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat <u>not included in this list</u>, 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.

**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", 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).

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

## 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).
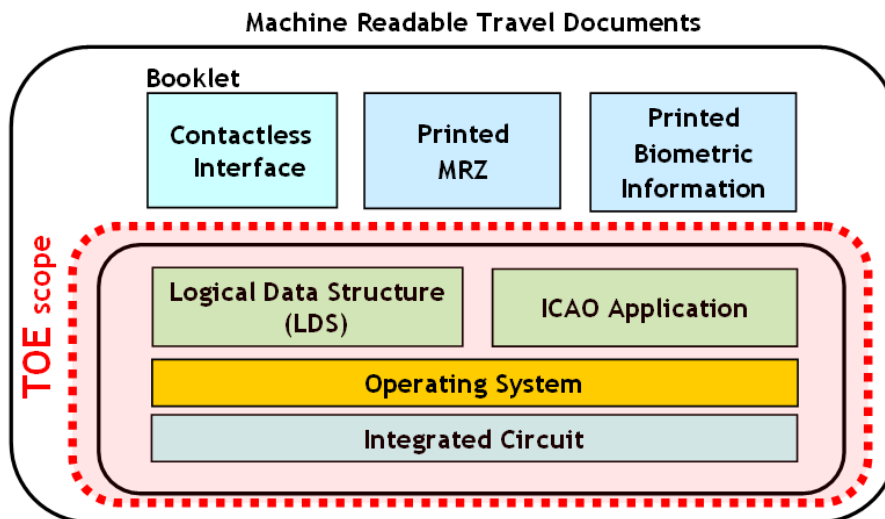
## ARCHITECTURE

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 01.01 [GU]. This guide is delivered to the card holder (Card holder or receiving State).
- KONA2 D2320N ePassport Preparative Guidance, version 01.07 [GP]. This guide is delivered to the personalization agent (Issuing State).
- KONA2 D2320N ePassport Administrator Guidance, version 01.03 [GA]. This guide is only used by KONA I internally
- KONA2 D2320N ePassport Delivery Procedure 01.02 [DEL]. This guide is used by all the entities to deliver the TOE between them.

## 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 ANSSI-CC-2015/66.

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 BAC functionalities. 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.

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 01 revision 03 patch 00.

The TOE is composed of:

- 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 V01.03.00),
- the associated guidance documentation.

The version of the software may be retrieved by following the procedure in section 6. Secure acceptance procedure [GP].

To identify the TOE is necessary for the personalization agent to execute the GET DATA command (APDU==00ca004600) and check the returned 10 Bytes against the following table (described in Table 54 TOE identification of [GP]):

| Response Data | Length | Value |
|---|---|---|
| Card Information | 10 | '44' '32' '01' '40' '4E' '31' '01' '00' '03' '00' |
| Card Serial Number | 8 | 'xx' 'xx' 'xx' 'xx' 'xx' 'xx' 'xx' 'xx' |

The identification of the Card information data is identified as follows:

- *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)*

- *01 00 03 : meaning TOE version 01.03*

- *00 : meaning update (patch) version 00 (no patch has been done)*

Regarding the Card Serial Number, as this data depends on the particular card delivered, it is not necessary to check this information.

## EVALUATION RESULTS

The product KONA2 D2320N ePassport (BAC configuration) version 01 revision 03 patch 00 has been evaluated against the Security Target SP-06-01 KONA2 D2320N ePassport BAC Security Target version 1 revision 8. 2016-05-21 .

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 v3.1 R4 and the CEM v3.1 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.

1. The TOE includes the patching mechanism during development in order to update the TOE after possible issues found during this development stage. However, the patching mechanism is not available once the personalization has been finished by setting the card into OPERATION state or the card has reached TERMINATION state. Moreover, this patching is done with a key that is different from the personalization one and is specially protected.
   The evaluator assessed that the MRTD data is secure when the issuer uses the SET LIFE CYCLE command to set the card into OPERATION state once the MRTD personalization is finished.
   Due to this, the laboratory recommends to the customer to be especially strict following the preparative procedure guidance and operational guidance until the OPERATION state is reached.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product KONA2 D2320N ePassport (BAC configuration) vversion 01 revision 03 patch 00, a positive resolution is proposed.

## 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:

[CC_P1]     Common Criteria for Information Technology Security
            Evaluation Part 1: Introduction and general model, Version
            3.1 R4, September 2012.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

| | |
|---|---|
| [CC_P2] | Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 R4, September 2012. |
| [CC_P3] | Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 R4, September 2012. |
| [CEM] | Common Methodology for Information Technology Security Evaluation: Version 3.1 R4, September 2012. |
| [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. |
| [ICAO-10] | International Civil Aviation Organization (ICAO) Doc 9303 Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contacless Intedrated Circuit (IC), 7th Edition, 2015 |
| [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). |
| [CCCOMP] | Common Criteria. Composite product evaluation for Smartcards and similar devices, Evaluation methodology |
| [INT10] | Organismo de Certificación. Centro Criptológico Nacional. Certificación de productos, Versión 0.6 |
| [PO-005] | Organismo de Certificación. Centro Criptológico Nacional. Certificación de productos, Versión 24, 12-12-2015 |
| [PO-008] | Organismo de Certificación. Centro Criptológico Nacional. Certificación de smartcards, Versión 8, 11-11-2014 |
| [AMCA] | Organismo de Certificación. Centro Criptológico Nacional. Attack Methods using Side Channels or Perturbations, Technical Guide, Versión 5 |

| [AMSCP] | Organismo de Certificación. Centro Criptológico Nacional. Attack Methods using Side Channels or Perturbations, Technical Guide, Versión 4 |
| [JILAAPS] | Joint Interpretation Library. Application of Attack Potential to Smartcards, version 2.9. Jan. 2013. |
| [JILCOMP] | Joint Interpretation Library. Composite Product evaluation for Smart Cards and similar devices, version 1.2. Jan. 2012 |
| [JIL-MSSR] | Joint Interpretation Library. Minimum site security requirements. Version 1.1 |
| [JILADVARC] | Joint Interpretation Library. Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices. Version 2.0, January 2012 |
| [ISO-14443] | ISO/IEC 14443 Identification Cards – Contactless integrated circuit(s) cards – Proximity cards. 2nd ed. 2008-06-15 |
| [ISO-7816-4] | ISO/IEC 7816-4:2005 Identification cards – Integrated circuits cards –Part 4: organization, security and commands for interchange. 2nd ed. 2005-01-15 |
| [CCDB-2006-04-004] | ST sanitising for publication. CCMC. Apr. 2006. |
| [GU] | KONA2 D2320N ePassport Operational Guidance V01.01 (2016.05.06) |
| [GP] | KONA2 D2320N ePassport Preparative Procedure Guidance V01.07, (2016.05.18) |
| [GA] | KONA2 D2320N ePassport Administrator Guidance, V01.03, (2016.05.21) |
| [DEL] | KONA2 D2320N ePassport Delivery Procedure V01.02 (2016.05.18) |

# 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:

- SP-06-01 KONA2 D2320N ePassport BAC Security Target version 1 revision 8. 2016-05-21.

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-06-21 KONA2 D2320N ePassport BAC Security Target Lite version 1 revision 2. 2016-05-21.