Reference: 2023-39-INF-4729- v1
Target: Limitada al expediente
Date: 03.02.2026

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2023-39**
TOE	**MK Lotus GovID IMDa in BAC configuration v4.6.8.8**
Applicant	**2500218495 - MK Smart Joint Stock Company**
References	

[EXT-8838] Certification Request

[EXT-9950] Evaluation Technical Report

Certification report of the product MK Lotus GovID IMDa in BAC configuration v4.6.8.8, as requested in [EXT-8838] dated 23/11/2023, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9950] received on 19/12/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product MK Lotus GovID IMDa in BAC configuration v4.6.8.8.

The TOE type is an electronic travel document representing a contactless smart card programmed according to ICAO Doc 9303, and BSI TR-03110.

Developer/manufacturer: MK Smart Joint Stock Company

Sponsor: MK Smart Joint Stock Company.

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

ITSEF: Applus Laboratories.

Protection Profile: Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control (BAC PP), BSI-CC-PP-0055 (Version 1.10, 25 March 2009).

Evaluation Level: Common Criteria v3.1 R5 EAL4 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_DVS.2 + ALC_TAT.2 + ATE_DPT.3

Evaluation end date: 19/12/2025.

Expiration Date[1]: 17/01/2031

All the assurance components required by the evaluation level EAL 4 (augmented with ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_DVS.2 + ALC_TAT.2 + ATE_DPT.3) 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 EAL 4 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_DVS.2 + ALC_TAT.2 + ATE_DPT.3, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product MK Lotus GovID IMDa in BAC configuration v4.6.8.8, 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) described on

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

ICAO Doc 9303 Part10 and providing the Basic Access Control and Passive Authentication mechanism according to ICAO Doc 9303 Part11.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 4 and the evidences required by the additional component ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_DVS.2 + ALC_TAT.2 + ATE_DPT.3 to the table, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.5
	ADV_IMP.1
	ADV_INT.2
	ADV_TDS.4
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.5
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.2
ATE	ATE_COV.2
	ATE_DPT.3
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.3

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS
FAU_SAS.1
FCS_CKM.1
FCS_CKM.4
FCS_COP.1/SHA
FCS_COP.1/ENC
FCS_COP.1/AUTH
FCS_COP.1/MAC
FCS_RND.1
FIA_UID.1
FIA_UAU.1
FIA_UAU.4
FIA_UAU.5
FIA_UAU.6
FIA_AFL.1
FDP_ACC.1
FDP_ACF.1
FDP_UCT.1
FDP_UIT.1
FMT_SMF.1
FMT_SMR.1
FMT_LIM.1
FMT_LIM.2
FMT_MTD.1/INI_ENA
FMT_MTD.1/INI_DIS
FMT_MTD.1/KEY_WRITE
FMT_MTD.1/KEY_READ
FPT_EMSEC.1
FPT_FLS.1
FPT_TST.1
FPT_PHP.3

IDENTIFICATION

Product: MK Lotus GovID IMDa in BAC configuration v4.6.8.8

Security Target: Security Target Description – MK Lotus GovID IMDa V4.6.8.8 – Basic Access Control, version 1.14 (12 December 2025).

Protection Profile: Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control (BAC PP), BSI-CC-PP-0055 (Version 1.10, 25 March 2009).

Evaluation Level: Common Criteria v3.1 R5 EAL 4 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_DVS.2 + ALC_TAT.2 + ATE_DPT.3.

SECURITY POLICIES

The use of the product MK Lotus GovID IMDa in BAC configuration v4.6.8.8 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, section 4.3 ("Organizational Security Policies").

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.

The detail of these assumptions is documented in the Security Target, section 4.4 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product MK Lotus GovID IMDa in BAC configuration v4.6.8.8, although the agents implementing attacks have the attack potential according to the Enhanced-Basic of EAL 4 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_DVS.2 + ALC_TAT.2 + ATE_DPT.3 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 those defined in the Security Target, section 4.2 ("Threats").

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 those defined in the Protection Profile and they are documented in the Security Target, section 5.2 ("Security Objectives for the Operational Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

The operating system manages all the resources of the integrated circuit that equips the ePassport ICAO document, providing secure access to data and functions.

In more detail, in each life cycle phase/step, access to data and functions is restricted by means of cryptographic mechanisms as follows:

- In phase 3, Personalization, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on GlobalPlatform card specification SCP03 protocol.
- In phase 4, Operational use, the user must prove his entitlement to access less sensitive data, i.e. DG1, DG2, and DG5 to DG16, by means of the BAC mechanism compliant to ICAO Doc 9303-11.

After a successful authentication, the communication between the ePassport ICAO document and the terminal is protected by the Secure Messaging mechanism defined in section 6 of the ISO 7816-4 specification.

The integrity of the data stored under the LDS can be checked by means of the Passive Authentication mechanism defined ICAO Doc 9303 part 11. Passive Authentication and BAC mechanisms are described in more detail in the following subsections.

Passive Authentication

Passive Authentication uses a digital signature to authenticate data stored in the data groups on the MRTD chip. This signature is generated in the personalization phase of the MRTD chip over a Document Security Object containing the hash values of all data groups stored on the chip.

Basic Access Control

Authentication and Key Establishment is provided by a three-pass challenge-response protocol according to ISO/IEC 11770-2, Key Establishment Mechanism 6 using 3DES FIPS 46-3 as block cipher. A cryptographic checksum according to ISO/IEC 9797-1 MAC Algorithm 3 is calculated over and appended to the ciphertexts. The modes of operation described in ICAO Doc 9303 are used.

Exchanged nonces must be of size 8 bytes, exchanged keying material must be of size 16 bytes. The inspection system and the IC must not use distinguishing identifiers as nonces.

The BAC session keys generated during BAC authentication are used to protect the confidentiality and integrity of the transmitted data. The key derivation function specified in ICAO Doc 9303 Part 11 is used, which requires using the hash function SHA-1 to derive the 112 bit Triple-DES key.

PHYSICAL ARCHITECTURE

The TOE consists of the following parts:

- Dual-interface chip IFX_CCI_000039h with firmware 80.306.16.0, including HSL v3.52.9708, UMSLC lib v01.30.0564, NRG SW 05.03.4097, SCL v2.15.000 and ACL v3.35.001.
- Smart card operating system (MK Lotus GovID IMDa in BAC Configuration, v4.6.8.8) with RTE (JC Virtual Machine (JCVM), JC Runtime Environment (JCRE) and GlobalPlatform Runtime Environment for personalization).
- An International Civil Aviation Organization (ICAO) application (ePassport information v1.8) compliant with ICAO Doc 9303.
- Guidance documentation in PDF format about the preparation and use of the ICAO application (described in detail in the next section).

DOCUMENTS

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

Document	Version	Date	Hash value
ICAO Applet Personalization Guide – Additional Information	1.3	2025-08-21	B244C0F4D31D4F4F635785AAEE2861EB5 C79630B12E9C8F8DA02EED167D03D96
ePassport Applet Information	1.8	2025-08-08	A64FC1394E2A5237B57E81007375288CA 4F85139FE6B357CD2D06AC3076807DE
Operational User Guidance	1.8	2025-12-04	D515ABC2CEFB35AAD6C55D09E90BC40A BD0B86CFDA380F0975D0D5691CD84A5E
Preparative Procedures	1.9	2025-12-04	DF80A6796B40E94DCD77E87D20E6D46C9 F08B75D4AEDD4DC9950412035D5C86A
scripts_v1.4_20250724.zip	1.4	2025-07-24	39F4EAA5BC85B4F6D39067AA1E08BAD17 595AA4807B36F6B7E6F4374C69 F5F15

PRODUCT TESTING

The Laboratory performed independent testing to verify the correct behavior of the functions of the TOE. The independent testing was focused in the access conditions, TOE status, random number generation and BAC authentication.

Based on the list of potential vulnerabilities applicable to the TOE in is operational environment, the evaluation team has devised vulnerability analysis and attack scenarios for penetration testing according to JIL supporting documents [JIL-ATTPOT]. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered.

No attack scenario with the attack potential enhanced-basic according to Common Criteria v3.1 R5 has been successful in the TOE's operational environment as defined in the Security Target when all security measures required by the developer are applied.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product MK Lotus GovID IMDa in BAC configuration v4.6.8.8 it is necessary the disposition of the following components:

- Dual-interface chip IFX_CCI_000039h with firmware 80.306.16.0, including HSL v3.52.9708, UMSLC lib v01.30.0564, NRG SW 05.03.4097, SCL v2.15.000 and ACL v3.35.001.
- Smart card operating system (MK Lotus GovID IMDa in BAC Configuration, v4.6.8.8) with RTE (JC Virtual Machine (JCVM), JC Runtime Environment (JCRE) and GlobalPlatform Runtime Environment for personalization).
- An International Civil Aviation Organization (ICAO) application (ePassport information v1.8) compliant with ICAO Doc 9303.

EVALUATION RESULTS

The product MK Lotus GovID IMDa in BAC configuration v4.6.8.8 has been evaluated against the Security Target Security Target Description – MK Lotus GovID IMDa V4.6.8.8 – Basic Access Control, version 1.14 (12 December 2025).

All the assurance components required by the evaluation level EAL 4 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_DVS.2 + ALC_TAT.2 + ATE_DPT.3 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 EAL 4 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_DVS.2 + ALC_TAT.2 + ATE_DPT.3, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The evaluation team makes the following security recommendations:

- To follow the security guidance's of the TOE strictly.
- To keep the TOE under personal control and set all other security measures available from the environment.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product MK Lotus GovID IMDa in BAC configuration v4.6.8.8, a positive resolution is proposed.

The Certification Body strongly recommends to the TOE consumer to review the application notes defined in the applicable Security Target, especially those related to the cryptographic mechanisms.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

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

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[JIL-ATTPOT] Application of Attack Potential to Smartcards, version 3.2.1 February 2024. Joint Interpretation Library.

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

[ST] Security Target Description – MK Lotus GovID IMDa V4.6.8.8 – Basic Access Control, version 1.14 (12 December 2025).

[STLite] PENDIENTE DE ENVÍO POR EL FABRICANTE

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

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:

- Security Target Description – MK Lotus GovID IMDa V4.6.8.8 – Basic Access Control, version 1.14 (12 December 2025).

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:

- <IdST LITE>. PENDIENTE DE ENVÍO POR EL FABRICANTE

RECOGNITION AGREEMENTS

In order to avoid multiple certifications 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.eu.

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.