Reference: 2021-43-INF-4154- v1
Target: Limitada al expediente
Date: 18.09.2023

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

CERTIFICATION REPORT

Dossier #	**2021-43**
TOE	**SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4)**
Applicant	**IT12845840151 - HID Global**
References	

[EXT-7198] Certification Request

[EXT-8509] Evaluation Technical Report

Certification report of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4), as requested in [EXT-7198] dated 13/08/2021, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-8509] received on 18/05/2023.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4).

Developer/manufacturer: HID Global

Sponsor: HID Global.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

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

Evaluation Level: Common Criteria version 3.1 R5 - EAL4 + ALC_DVS.2.

Evaluation end date: 07/07/2023.

Expiration Date[1]: 15/09/2028.

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 + ALC_DVS.2, as defined by the Common Criteria version 3.1 R5 and the CEM version 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4), a positive resolution is proposed.

TOE SUMMARY

The TOE is an electronic document representing a contactless/contact smart card programmed according to the Logical Data Structure (LDS) [ICAO-10] and providing the Basic Access Control (BAC) according to ICAO Doc 9303 8th edition Part 11 [ICAO-11].

The TOE is composed of:

[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.

- the circuitry of the dual-interface e-Document's chip Infineon M7892 G12,
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the smart card operating system SOMA-c007 version 4,
- an ICAO application LDS1 compliant with ICAO Doc 9303-10 [ICAO-10] and Doc 9303-11 [ICAO-11] providing the Basic Access Control (BAC),
- the associated guidance documentation.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component ALC_DVS.2, according to Common Criteria v3.1 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.4
	ADV_IMP.1
	ADV_TDS.3
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.1
ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.3

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the functional requirements, according to Common Criteria v3.1 R5, Part 2 extended and can be found in section 6 Security Requirements of the [ST].

IDENTIFICATION

Product: SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4)

Security Target: TCAE160001 - Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - Basic Access Control, , version 1.14, 15.05.2023.

Protection Profile: BSI-CC-PP-0055 Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application” Basic Access Control version 1.10 25th March, 2009.

Evaluation Level: Common Criteria version 3.1 R5 EAL4 + ALC_DVS.2.

SECURITY POLICIES

The use of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4) 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 3.4 “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 3.2 “Assumptions”.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4), although the agents implementing attacks have an **Enhanced-basic** attack potential according to the assurance level of

EAL4 + ALC_DVS.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.3 “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 4.2 “Security Objectives for the operational Environment”.

ARCHITECTURE

LOGICAL SCOPE

The SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4) operating system manages all the resources of the integrated circuit that equips the e-Document, providing secure access to data and functions. Major tasks performed by the operating system are:

- Communication between internal objects
- Communication with external devices
- Data storage in the file system
- Execution of commands
- Cryptographic operations
- Management of the security policies

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

- In Step 5 “Initialization” of Phase 2, the Initialization Agent must prove his/her identity by means of an authentication mechanism based on AES with 256-bit key.
- In Step 6 “Pre-personalization” of Phase 2, the Pre-personalization Agent must prove his/her identity by means of an authentication mechanism based on Triple-DES with 112-bit keys.
- In Phase 3 “Personalization”, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on Triple-DES with 112-bit keys.

- 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 [ICAO-11].

After a successful authentication, the communication between the e-Document and the terminal is protected by the Secure Messaging mechanism defined in section 6 of the ISO 7816-4 specification [ISO-7816-4].

The integrity of data stored under the LDS is checked by means of the Passive Authentication mechanism defined in [ICAO-11].

PHYSICAL SCOPE

The physical TOE is comprised of the following parts:

- dual-interface integrated circuit chip M7892 G12 equipped with IC Dedicated Software and Crypto Library (cf. [ST] Appendix A for more details);
- smart card operating system SOMA-c007 version 4;
- an International Civil Aviation Organization (ICAO) application compliant with ICAO Doc 9303 providing the Basic Access Control [ICAO-10] [ICAO-11]
- guidance documentation about the initialization of the TOE, the preparation and use of the ICAO application, composed by:
    - the Initialization Guidance,
    - the Pre-personalization guidance,
    - the Personalization Guidance, and
    - the Operational User Guidance.

The following table describes the format, delivery method, recipients and the hash value of each TOE components.

Type	TOE component	Format	Delivery method	Delivery recipient	Hash value (SHA-512)
IC with Dedicated Software and Crypto Library	***¡Error! Nombre desconocido de propiedad de documento.***	Module on chip	Secure courier	-	Cf. [M7892], section 10
OS and ICAO Application	SOMA-c007 version 4 Machine Readable	HEX file	Secure IC Manufacturer’s Web application	Infineon	2328A2C0C731BC0D C37A63CD7CE80530 FB582E2430684289 0919CFCC1DF8B3C8

	Electronic Document (TOE Identification data: **¡Error! Nombre desconocido de propiedad de documento.**)				23FA9B970250075A F90AADD55CCF08D5 081865211E3C8C74 B39DE44ED3DCE94C
Document	Initialization Guidance for SOMA-c007 Machine Readable Electronic Document v2.5, ref. TCAE160012	docx	Encrypted email message	Initialization Agent	A67B927BB875030A DD05FDFDD922D52A 9C01B95A1CA74AAC 2810674EDB1F3626 EC89BC3EB9BE8903 5D34711EB7EF4A42 221E30E4EB02C386 F8493B7F31A012AE
Document	Pre-personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.4, ref. TCAE160016	docx	Encrypted email message	Pre-personalization Agent	10A4B86817F57974 DF6126FF6352C492 4C0FF8C0415A2FD1 C60778BCA8855DB7 273BB121208997AD 774A86F62534C834 6215AA1AC4181D62 8A4D8F7FBB72D712
Document	Personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.4, ref. TCAE160017	docx	Encrypted email message	Personalization Agent	B1B9418A7431FA77 45D6D4B8760FF7C8 0E6B5DD38E5FE65B E99B6459904ECB93 4B9E40062C7BD339 032FAEEECDFB8886 E5072B6CA236E8E8 1CBA596312F28A1F
Document	Operational User Guidance for SOMA-c007 Machine Readable	docx	Encrypted email message	User (Inspection System)	21D8BB15ADEB6B72 2598F8A9555F609F F1890CB9C745AD3B 63411E1514BE468A AF929D779AA06BEA

	Electronic Document ICAO Application v2.4, ref. TCAE160018				E983F6BEA46B1661 A04A7DBA7D2D2E94 817561E98B411775

The delivery procedure for the TOE is described in detail in Secure Delivery Procedure, ref. TCAE110027.

DOCUMENTS

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

- Initialization Guidance for SOMA-c007 Machine Readable Electronic Document, version 2.5, ref. TCAE160012.
- Pre-personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application, version 2.4, ref. TCAE160016.
- Personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application, version 2.4, ref. TCAE160017.
- Operational User Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application, version 2.4, ref. TCAE160018.
- Secure Delivery Procedure, version 2.5, ref. TCAE110027.

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 BSI-DSZ-CC-0891-V6-2021.

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 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 Enhanced-basic potential 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 software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4) it is not necessary any additional software or hardware components.

The version of the software may be retrieved by following the procedure in section 4.2 (Retrieval of TOE, product and chip information) of the "Initialization Guidance for SOMA-c007 Machine Readable Electronic Document, version 2.5, ref. TCAE160012".

To identify the TOE is necessary for the initialization agent to execute the "GET DATA (Even INS)" command with P1 = 01h and P2 = 20h. APDU shall be encoded as follows:

- CLA = E0h

- INS = CAh
- P1 = 01h
- P2 = 20h
- LE = 00h

The e-Document certified under Common Criteria v.3.1 shall return SOMA-c007_4 (ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 30h 37h 5Fh 34h), representing the TOE Identification Data.

EVALUATION RESULTS

The product SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4) has been evaluated against the Security Target TCAE160001 - Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - Basic Access Control, , version 1.14, 15.05.2023.

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 version 3.1 R5 and the CEM version 3.1 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.
- To periodically review the status of the certification of the underlying platform.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c007 Machine Readable Electronic Document Basic Access Control version 4 (SOMA-c007_4), a positive resolution is proposed.

The certifier strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on guidance documents as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

Some of the key lengths for some of the cryptographic mechanisms defined in the ST are considered as legacy mechanisms according to [ACM]. Please check [ACM] to consult recommended dates to sunset the applicable key lengths.

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:

[ACM] SOG-IS agreed cryptographic mechanisms, version 1.3. SOG-IS crypto working group. February 2023.

[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.

[ICAO-10] ICAO: Doc 9303 Machine Readable Travel Documents, Eighth Edition, 2021, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

[ICAO-11] ICAO: Doc 9303 Machine Readable Travel Documents, Eighth Edition, 2021, Part 11: Security Mechanisms for MRTDs

[ISO-7816-4] ISO/IEC: International Standard 7816-4:2020. Identification cards - Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange

[JILAAPS]Joint Interpretation Library. Application of Attack Potential to Smartcards, version 3.2. Nov.2022.

[JILADVARC] Joint Interpretation Library. Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.1, Jul, 2021.

[JILCOMP] Joint Interpretation Library. Composite Product evaluation for Smart Cards and similar devices, version 1.5.1. May 2018.

[M7892] Infineon: Security Target Lite, Common Criteria EAL6 augmented / EAL6+, M7892 Design Steps D11 and G12, Document version 3.6 as of 2021-10-06.

[ST] TCAE160001 - Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - Basic Access Control, , version 1.14, 15.05.2023

SECURITY TARGET / SECURITY TARGET LITE

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:

- TCAE160001 - Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - Basic Access Control, version 1.14, 15.05.2023.

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:

- TCAE160019 - Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - Basic Access Control, version 1.3, 15.05.2023.

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.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.