Reference: 2020-33-INF-3550- v1
Target: Limitada al expediente
Date: 17.06.2021

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

CERTIFICATION REPORT

Dossier #	**2020-33**
TOE	**MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations**
Applicant	**562 113 530 R.C.S. - THALES DIS FRANCE SA**
References	

[EXT-6145] Certification Request

[EXT-6834] Evaluation Technical Report

Certification report of the product MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations, as requested in [EXT-6145] dated on 17/08/2020, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-6834] received on 12/05/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations.

The Target of Evaluation (TOE) is a product comprising hardware and software corresponding to a Java Card platform operating system in Open Configuration.

Developer/manufacturer: THALES DIS FRANCE SA

Sponsor: THALES DIS FRANCE SA.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: Java Card System – Open Configuration Protection Profile (ANSSI-PP-2010-03M01, Version 3.0, May 2012).

Evaluation Level: Common Criteria v3.1 R5 EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 25/05/2021.

Expiration Date[1]: 18/06/2026.

All the assurance components required by the evaluation level EAL5 (augmented with ALC_DVS.2 and AVA_VAN.5) have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL5+ALC_DVS.2+AVA_VAN.5, 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 MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations, a positive resolution is proposed.

TOE SUMMARY

The MultiApp Essential V1.1 Platform is a smart card operating system (IC and OS) that complies with two major industry standards:

[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.

- Sun Java Card 3.0.4, which consists of the Java Card 3.0.4 Virtual Machine [JCVM304], the Java Card 3.0.4 Runtime Environment [JCRE304] and the Java Card 3.0.4 Application Programming Interface [JCAPI304].
- The Global Platform Card Specification version 2.2.1 [GP221].

It is intended to host a set of Java Card applications and provides cryptographic services for symmetric (3DES, AES), asymmetric (RSA) and hash (SHA) operations, Moreover, it also provides random number generation and integrity check features.

The TOE allows the loading of applets before or after the issuance of the card, but the Issuer can forbid this operation to be carried out.

The TOE has four possible configurations:

- Full Configuration.
- Light Configuration.
- XLight_T1 Configuration.
- XLight_NB Configuration.

The details about the features of each configuration are described in [ST LITE], chapter 2.4 (TOE Description).

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 and the evidences required by the additional component ALC_DVS.2 and AVA_VAN.5, 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.4
	ALC_CMS.5

	ALC_DEL.1
	ALC_DVS.2
	ALC_FLR.1
	ALC_LCD.1
	ALC_TAT.2
ATE	ATE_COV.2
	ATE_DPT.3
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

SECURITY FUNCTIONAL REQUIREMENTS

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

SECURITY FUNCTIONAL REQUIREMENTS
FMT_MSA.1/JCRE
FMT_MSA.1/JCVM
FDP_ACC.2/FIREWALL
FDP_ACF.1/FIREWALL
FDP_IFC.1/JCVM
FDP_IFF.1/JCVM
FDP_RIP.1/OBJECTS
FMT_MSA.2/FIREWALL_JCVM
FMT_MSA.3/FIREWALL
FMT_MSA.3/JCVM
FMT_SMR.1/JCRE
FMT_SMF.1/CORE_LC
FCS_CKM.1 /RSA Std
FCS_CKM.1 /RSA CRT
FCS_CKM.1 /GP
FCS_CKM.1 /DH
FCS_CKM.2/RSA
FCS_CKM.2/TDES
FCS_CKM.2/AES
FCS_CKM.2/DH
FCS_CKM.2/STORE Data
FCS_CKM.2/PUT KEY
FCS_CKM.3/RSA
FCS_CKM.3/AES
FCS_CKM.3/TDES
FCS_CKM.3/DH
FCS_CKM.4
FCS_COP.1/RSA-SIGN
FCS_COP.1/RSA-CIPHER
FCS_COP.1/TDES-CIPHER

FCS_COP.1/AES-CIPHER
FCS_COP.1/TDES-MAC
FCS_COP.1/AES-CMAC
FCS_COP.1/SHA
FDP_RIP.1/APDU
FDP_RIP.1/bArray
FDP_RIP.1/ABORT
FDP_RIP.1/KEYS
FDP_RIP.1/TRANSIENT
FDP_ROL.1/FIREWALL
FAU_ARP.1
FDP_SDI.2
FPT_TDC.1
FPT_FLS.1/JCS
FPR_UNO.1
FMT_MTD.1/JCRE
FMT_MTD.3/JCRE
FIA_ATD.1/AID
FIA_UID.2/AID
FIA_USB.1/AID
FDP_ITC.2/Installer
FMT_SMR.1/Installer
FPT_FLS.1/Installer
FPT_RCV.3/Installer
FMT_MSA.1/ADEL
FMT_MSA.3/ADEL
FMT_SMR.1/ADEL
FMT_SMF.1/ADEL
FDP_ACC.2/ADEL
FDP_ACF.1/ADEL
FDP_RIP.1/ADEL
FPT_FLS.1/ADEL
FDP_RIP.1/ODEL
FPT_FLS.1/ODEL
FMT_MSA.1/CM
FMT_MSA.3/CM
FMT_SMR.1/CM
FMT_SMF.1/CM
FCO_NRO.2/CM
FIA_UAU.1/CM
FIA_UID.1/CM
FDP_IFC.2/CM
FDP_IFF.1/CM
FDP_UIT.1/CM
FTP_ITC.1/CM
FPT_TST.1/SCP
FPT_PHP.3/SCP
FPT_RCV.4/SCP
FDP_ACC.1/CMGR
FDP_ACF.1/CMGR
FMT_MSA.1/CMGR

FMT_MSA.3/CMGR
FPT_FLS.1/SpecificAPI
FPT_ITT.1/SpecificAPI
FPR_UNO.1/SpecificAPI
FCS_RND.1

IDENTIFICATION

Product: MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations

Security Target: MultiApp Essential v1.1: JCS Security Target version 1.10 (14 April 2021).

Protection Profile: Java Card System – Open Configuration Protection Profile (ANSSI-PP-2010-03M01, Version 3.0, May 2012).

Evaluation Level: Common Criteria v3.1 R5 EAL5+ALC_DVS.2+AVA_VAN.5.

SECURITY POLICIES

The use of the product MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST LITE], chapter 5.3 (Organizational security policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST LITE], chapter 5.4 (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.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST LITE], chapter 5.2 (Threats) do not suppose a risk for the product MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations, although the agents implementing attacks have the attack potential according to the High of EAL5+ALC_DVS.2+AVA_VAN.5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

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

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 detailed in [ST LITE], chapter 6.2 (Security objectives for the operational environment).

ARCHITECTURE

LOGICAL ARCHITECTURE

The MultiApp Essential V1.1 platform contains the following components:

- The Core Layer. It provides the basic card functionalities (memory management, I/O management and cryptographic primitives) with native interface with the underlying IC. The cryptographic features implemented in the native layer encompass the following algorithms:
  - DES, 3DES (ECB, CBC)
  - RSA up to 3072 (CRT method), 2048 (Std method)
  - AES 128, 192, 256
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
  - DH up to 2048
  - Optional feature, OBKG 3K (CRT)
  - PRNG
  - CRC16
  - CRC32 (mandatory for GP 2.2.1 ID config)

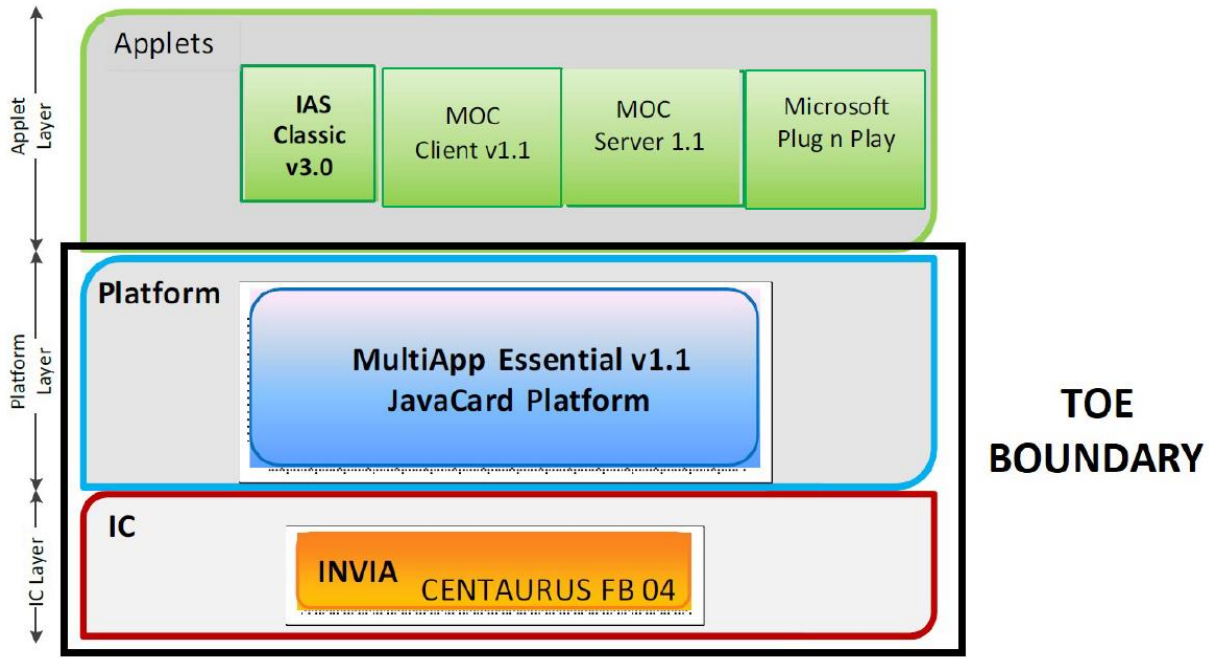
  (*) DES, SHA-1 and RSA keys <1900 bits are algorithms supported by the product but they are not conformant with SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [ACM] and are out of the scope of the CC evaluation.
- The Plug-ins layer. It consists of:
  - The Javacard Runtime Environment. It conforms to [JCRE304] and provides a secure framework for the execution of the Java Card programs and data access management (firewall). Among other features, multiple logical channels are supported, as well as extradition, DAP, Delegated management and SCP03.
  - The Javacard Virtual Machine. It conforms to [JVCM304] and provides the secure interpretation of bytecodes.
  - The API. It includes the standard Java Card API [JCAPI304] and the Gemalto proprietary API.
  - The Global Platform Issuer Security Domain. It conforms to [GP221] and provides card, key and applet management functions (contents and life- cycle) and security control.

PHYSICAL ARCHITECTURE

The TOE is part of the MultiApp Essential v1.1 smartcard Product. This smartcard contains the software dedicated to the operation of:

- The MultiApp Essential V1.1 Platform, which supports the execution of the personalized applets and provides the smartcard administration services. It is conformant to JavaCard 3.0.4 and GP 2.2.1 standards.
- The identity applets: IAS Classic v3.0, Microsoft Plugin Play, MOC Client v1.1 & Server v1.1. (These applications could be removed based on customer needs and they are out of scope of the evaluation).
- Additionally, other applets – not determined at the moment of the present evaluation – may be loaded on the smartcard before or after issuance.
- A cryptographic library developed by Thales DIS.

The architecture of the smartcard software and application data can be represented as follows:



DOCUMENTS

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

DOCUMENT TITLE	VERSION AND DATE
MultiApp Essential Operating System Reference Manual	D1352558G November 11, 2020
Guidance for secure application development on Multiapp platforms	D1390326 A01 March 2018
Verification process of Gemalto non sensitive applet	D1390670, A02 Oct 2018
Verification process of Third Party non sensitive applet	D1390671, A02 Oct 2018
Rules for applications on Multiapp certified product	D1390963, Rev. 1.3 Oct 2018
MultiApp Essential v1.1: AGD_PRE document - Javacard Platform	D1524659, Rev 1.6 April 1, 2021
MultiApp Essential v1.1: AGD_OPE document - Javacard Platform	D1524658, Rev 1.10 April 1, 2021
The following item shall be provided only in case of specific commercial agreement and through NDA	
D1484942_GTO API_MAE11_PLTF.7z	D1484942, Rev1.0 December 19, 2018

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 performed a subset of the developer functional tests. 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.

EVALUATED CONFIGURATION

The configuration selected for the evaluation of the TOE MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations is the following:

Integrated Circuit	
Product name	CENTAURUS
Reference	CENTAURUS_FB_04
Hardware revision	F
Platform ROM Firmware revision	B
Platform FLASH Firmware revision	04
BIOS	Version 1.0-739
LOADER	Version 2.1
Java Card Operating System	
OS name	MultiApp Essential v1.1
Mask reference label	LBL30 Checkpoint 1.40

EVALUATION RESULTS

The product MultiApp Essential v1.1 Platform with Full, Light, XLight_T1 and XLight_NB configurations has been evaluated against the Security Target: MultiApp Essential v1.1: JCS Security Target version 1.10 (14 April 2021).

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

- 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 Applus Laboratories, a positive resolution is proposed.

The strength of the cryptographic mechanisms was not rated in the course of this evaluation, but this Certification Body wants to remark that the following cryptographic mechanisms, referenced in the applicable Security Target, are not recommended or considered only for legacy use according to [SOGIS-ACM]. All not recommended cryptographic mechanisms by [SOGIS-ACM] and DES primitives were not evaluated in the course of this certification.

Symmetric Atomic Primitives			
Algorithm	**Key Sizes (bits)**	**Standard**	**Comments**
DES	112	SP800-67, ISO9797-1	[SOGIS-ACM] Legacy use until December 31, 2024
DES	168	SP800-67, ISO9797-1	[SOGIS-ACM] Legacy use until December 31, 2027
Asymmetric Atomic Primitives			
Algorithm	**Key Sizes (bits)**	**Standard**	**Comments**
RSA	1024, 1152, 1280, 1536	ISO9796-2	Not recommended by [SOGIS-ACM].
RSA	2048	ISO9796-2	[SOGIS-ACM] Legacy use until December 31, 2025
Hash functions			
Algorithm	**Key Sizes (bits)**	**Standard**	**Comments**
SHA-1	160		Not recommended by [SOGIS-ACM].
SHA-224	224		[SOGIS-ACM] Legacy use until December 31, 2025

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.

[ST] MultiApp Essential v1.1: JCS Security Target version 1.10, 14 April 2021.

[ST LITE] MultiApp Essential v1.1: JCS Security Target version 1.10p.

[PP] Java Card System – Open Configuration Protection Profile (ANSSI-PP-2010-03M01, Version 3.0, May 2012.

[SOGIS-ACM] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, version 1.2. January 2020.

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:

- MultiApp Essential v1.1: JCS Security Target version 1.10 (14 April 2021).

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:

- MultiApp Essential v1.1: JCS Security Target version 1.10p.

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.