Reference: 2017-21-INF-2513-v2
Target: Expediente
Date: 08.10.2018

Created by: CERT9
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-21**
TOE	**COMSec Admin+ v3.1.11a_CA+**
Applicant	**B-84871607 - INDRA SISTEMAS DE COMUNICACIONES SEGURAS, S.L.**
References	
	[EXT-4237] ETR v M0 COMSec Admin+

Certification report of the product “COMSec Admin+ v3.1.11a_CA+”, as requested in [EXT-3376] dated 23/05/2017, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-4237] received on 26/07/2018.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product "COMSec Admin+ v3.1.11a_CA+".

The whole system provides the secure communications through a Virtual Operator (IMS – IP Multimedia System) responsible to manage the communications and its security.

The TOE is a Secure Communications App for Android devices allowing the user to protect its real time communications (VoIP, Instant Messaging & Data) while using regular public networks (3G, 4G, WIFI …) provided by commercial wireless services company.

Developer/manufacturer: INDRA SISTEMAS DE COMUNICACIONES SEGURAS, S.L.

Sponsor: INDRA SISTEMAS DE COMUNICACIONES SEGURAS, S.L..

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

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_ECD.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1. The assurance requirements have been defined in the [PPAS].[1]

Evaluation end date: 26/07/2018.

All the assurance activities and requirements present in the [PPAS] have been assigned a "PASS" verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. assigns the "PASS" VERDICT to the whole evaluation due to all the evaluator actions defined in the [PPAS] are satisfied, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

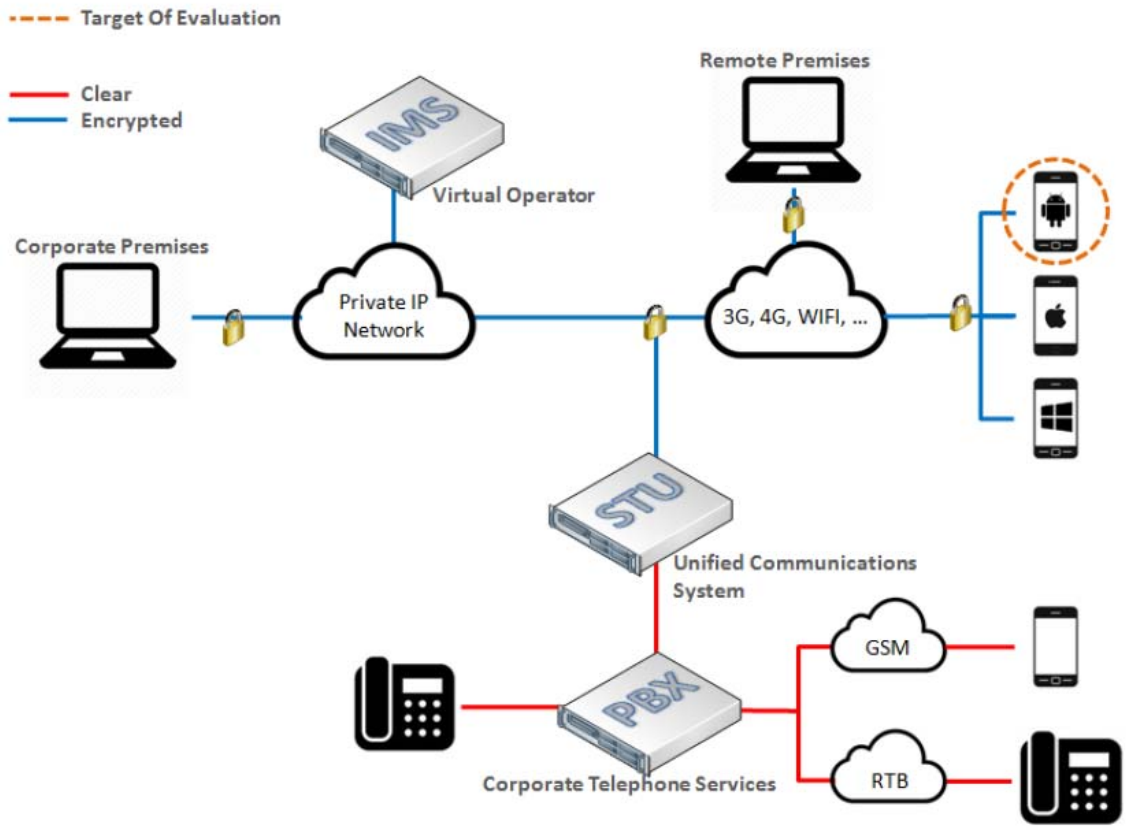
Considering the obtained evidences during the instruction of the certification request of the product "COMSec Admin+ v3.1.11a_CA+", a positive resolution is proposed.

TOE SUMMARY

The TOE is a Secure Communications App for Android devices allowing the user to protect its real time communications (VoIP, Instant Messaging & Data) while using regular public networks (3G, 4G, WIFI …) provided by commercial wireless services company.

The whole system provides the secure communications through a Virtual Operator (IMS – IP Multimedia System) responsible to manage the communications and its security:

[1] Although no conformance has been declared to any Protection Profile, the ST is based on the [PPAS].



The TOE is the COMSec Android Application, consisting of an Android Application Package file, with filename extension “apk”. The TOE is delivered to the customer installed in the Smartphone.

The Android Application is a software client running on the host platform, and only communicating with the IMS Server, via 3G, 4G or WIFI connections. The IMS Server (secure VoIp/SIP server for the system), the corporate communications systems, and other client platforms beyond the Android Client lay outside the scope of the TOE.

Those are the security functions provided by the TOE:

- Cryptographic Support
- User Data Protection
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channel
- Optional Requirements
- Selection Based Requirements

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the assurance requirements ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_ECD.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1., according to Common Criteria v3.1 R4.

Class	**Family/Component**
ASE: Security Target Evaluation	ASE activities defined in [CEM]
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1 Operational User Guidance AGD_PRE.1 Preparative Procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMS.1 TOE CM Coverage ALC_TSU_EXT.1 Timely Security Updates
ATE: Tests	ATE_IND.1 Independent Testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability Survey

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4 and [PPAS]:

Class	**Component**
Cryptographic Support (FCS)	FCS_RBG_EXT.1 Random Bit Generation Services FCS_STO_EXT.1 Storage of Credentials
User Data Protection (FDP)	FDP_DEC_EXT.1 Access to Platform Resources FDP_NET_EXT.1 Network Communications FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

Security Management (FMT)	FMT_MEC_EXT.1 Supported Configuration Mechanism FMT_CFG_EXT.1 Secure by Default Configuration FMT_SMF.1 Specification of Management Functions
Privacy	FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information
Protection of the TSF (FPT)	FPT_API_EXT.1 Use of Supported Services and APIs FPT_AEX_EXT.1 Anti-Exploitation Capabilities FPT_TUD_EXT.1 Integrity for Installation and Update FPT_LIB_EXT.1 Use of Third Party Libraries
Trusted Path/Channel (FTP)	FTP_DIT_EXT.1 Protection of Data in Transit
Optional Requirements	FCS_CKM.1(2) Cryptographic Symmetric Key Generation FCS_TLSC_EXT.2 TLS Client Protocol
Selection Based Requirements	FCS_CKM_EXT.1 Cryptographic Key Generation Services FCS_CKM.1(1) Cryptographic Asymmetric Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1(1) Cryptographic Operation - Encryption/Decryption FCS_COP.1(2) Cryptographic Operation – Hashing FCS_COP.1(3) Cryptographic Operation – Signing FCS_COP.1(4) Cryptographic Operation - Keyed-Hash Message Authentication FCS_TLSC_EXT.1 TLS Client Protocol FCS_TLSC_EXT.4 TLS Client Protocol FIA_X509_EXT.1 X.509 Certificate Validation FIA_X509_EXT.2 X.509 Certificate Authentication

IDENTIFICATION

Product: "COMSec Admin+ v3.1.11a_CA+"

Security Target: COMSec Admin+ Client Security Target (Version A/6, 29 June 2018) [ST].

Protection Profile: None.

Evaluation Level: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_ECD.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1. The assurance requirements have been defined in the [PPAS].[2]

SECURITY POLICIES

The use of the product "COMSec Admin+ v3.1.11a_CA+" 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 [ST], chapter 4.1 (ORGANIZATIONAL SECURITY POLICIES).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.2 (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 following threats do not suppose a risk for the product "COMSec Admin+ v3.1.11a_CA+", although the agents implementing attacks have the attack potential according to the Basic Attack Potential 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.

[2] Although no conformance has been declared to any Protection Profile, the ST is based on the [PPAS].

The security objectives declared for the TOE operational environment are detailed in [ST], chapter 4.2 (SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target [ST].

ARCHITECTURE

LOGICAL ARCHITECTURE

There have been defined two main interfaces: User Interface and IMS Interface.

In the User Interface, the following TSFI's have been defined:

- Application Configuration.
- IMS Configuration.
- CA Certificates.
- User Credentials.
- Application Information.
- Login.
- Dialing.
- System Users.
- Secure Call.
- Call history.
- Messaging.

In the IMS Inferface, the following TSFI's have been defined:

- IMS registration.
- Call establishment.
- Administration.

PHYSICAL ARCHITECTURE

Physical Boundaries

The TOE is the COMSec Android Application, consisting of an Android Application Package file, with filename extension "apk". The TOE is delivered to the customer installed in the Smartphone.

Hardware Requirements

The TOE shall be run in a Samsung Galaxy A3 2016 Smartphone.

The Android Application is a software client running on the host platform, and only communicating with the IMS Server, via 3G, 4G or WIFI connections. The IMS Server (secure VoIp/SIP server for the system), the corporate communications systems, and other client platforms beyond the Android Client lay outside the scope of the TOE.

Software Requirements

The TOE shall be run in Android 5.1.1 Operating System (or higher)

DOCUMENTS

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

- Descripción Técnica Sistema COMSec (Doc Nº 4941802000000DF01, Revisión A2, Fecha Junio 2018)
- COMSec Admin+ Manual Android v.3.1.1x (Doc Nº 4941802000000MA02, Revisión A2)
- Carga de Credenciales COMSec Admin+ (Doc Nº 4941802000000MA01, Revisión A3, Fecha 22/06/2018)
- Especificación Funcional COMSec Admin+ (Doc Nº 4941802000000ES01, Revisión A3, Fecha 16/05/2018)

PRODUCT TESTING

Although the TOE does not claim conformity to the [PPAS], it is used by the developer as a base for the ST to define the assurance activities for the evaluation of the ATE class. In particular defines the tests to be executed by the evaluator during the assessment of the ATE activity.

The evaluator has devised the testing plan based completely on the tests described along the protection profile [PPAS] since the changes introduced by the developer are minimal and do not impact the test procedures described in the PP.

The assurance activities have been grouped in two types of activities: Documental activities and testing activities. Both types have been executed and described along the testing plan.

The evaluator has defined the testing steps described in each test case. Nevertheless, some of the test cases developed by the evaluator required minor changes to the tools provided that has been described along each test description.

The tests have been executed first for a previous version of the TOE. For those tests cases having an initial verdict of Fail, the tests have been repeated for the definitive TOE.

The developer has also devised an independent test to evaluate the certificate whitelist behaviour from server side.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product “COMSec Admin+ v3.1.11a_CA+” has been evaluated with the following components:

- Android 7.0 Operating System

Regarding the hardware components, the TOE has been running in a

- Samsung SM-A310F

EVALUATION RESULTS

The product "COMSec Admin+ v3.1.11a_CA+" has been evaluated against the Security Target COMSec Admin+ Client Security Target (Version A/6, 29 June 2018) [ST].

All the assurance components have been assigned a "PASS" verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

No recommendations have been made.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product "COMSec Admin+ v3.1.11a_CA+", a positive resolution is proposed.

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, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

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

[PPAS] Protection Profile for Application Software (Version 1.2, 22 April 2016)

[ST] COMSec Admin+ Client Security Target (Version A/6, 29 June 2018)

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:

- COMSec Admin+ Client Security Target (Version A/6, 29 June 2018) [ST].

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:

- COMSec Admin+ Client Security Target Lite (Version A/0, 03 September 2018)

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

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

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France,

Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.