Referencia: 2018-14-INF-2763-v1
Difusión: Pœblico
Fecha: 08.05.2019

Creado por: CERT9
Revisado por: CALIDAD
Aprobado por: TECNICO

CERTIFICATION REPORT

Expediente #	**2018-14**
TOE	**ANCERT Server Signing Application v1.1.8**
Solicitante	**B83395988 - Agencia Notarial de Certificacion**
Referencias	

[EXT-3941] Solicitud Re-evaluacion-ANCERT

Certification report of the product ANCERT Server Signing Application v1.1.8, as requested in [EXT-3941] dated 27/04/2018, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-4907] received on 29/04/2019.

CONTENIDOS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product ANCERT Server Signing Application v1.1.8.

The TOE corresponds to a software component running on an operating system that provides remote signature generation services to Signer.

Developer/manufacturer: Agencia Notarial de Certificacion

Sponsor: Agencia Notarial de Certificacion.

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

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4+ALC_FLR.2+AVA_VAN.5.

Evaluation end date: 25/04/2019.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.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 EAL4+ALC_FLR.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 ANCERT Server Signing Application v1.1.8, a positive resolution is proposed.

TOE SUMMARY

The TOE is a software component that provides services for the generation of remote signature in a manner that:

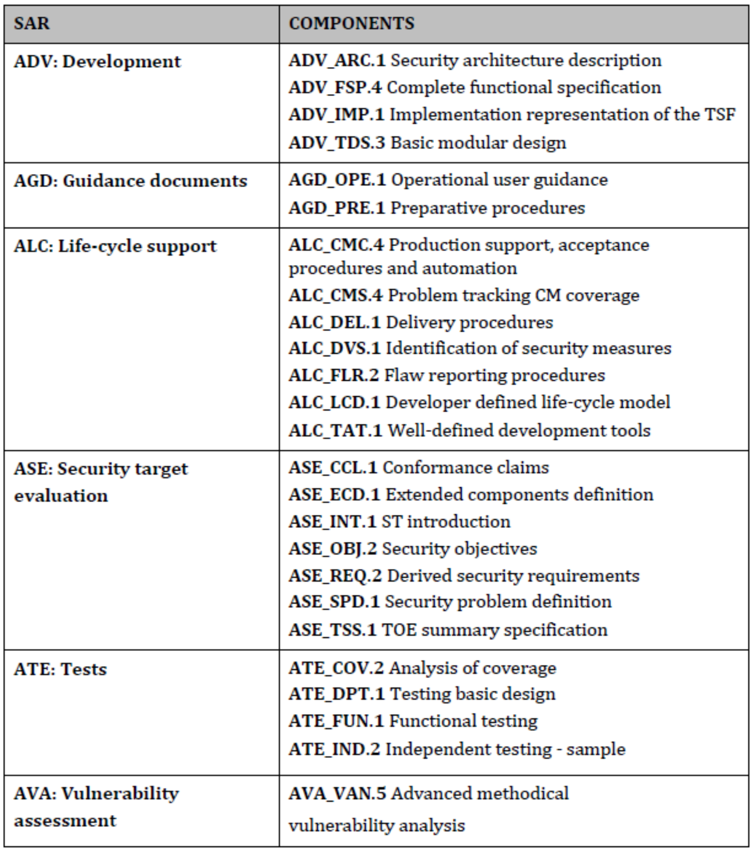
- It is able to receive and process Data to Be Signed Requests (DTBS/R) from external Signer or Signature Creation Application (requesters), protecting the integrity of the requests when managed by the TOE.
- The integrity of the signed document produced by the TOE is protected when created and managed by the TOE and during transfer from the TOE to an external entity.
- Any external entity can verify the authentication of the signed document produced by the TOE.
- The TOE services (TOE initialization, start of TOE operation, stop of TOE operation, TOE configuration, generation of Signer's key pair (SCD and SVD), Signer's public key (SVD)

export for certificate request, certificate import, signature export, signer bundle, Signer SAP information and internal audit) are only used in an authorized way.

- Manages (generation, backup, usage and destruction) SCD and SVD of the Signer using an external HSM, and authentication information of the Signer provided by SCA or external trusted source and produce CSR in order to be delivered to CA.
- Links a Signer to SAP/SAD with SCD and SVD and DTBS/R in order to guaranty that the Signer has sole control over his SCD.
- Two independent authenticator factors are combined in the SAD/SAP in order to gain access to Signer’s SCD.
- It is able to produce an audit trail where all the security events and all the Signer’s interactions with his SCD are logged.
- Protects the integrity and authenticity of the TOE configuration data, signer bundles and audit trail.

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 components ALC_FLR.2 and AVA_VAN.5, according to Common Criteria v3.1 R5.



SAR	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.1** Identification of security measures **ALC_FLR.2** Flaw reporting procedures **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.5** Advanced methodical vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

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

FAU_GEN.1
FAU_GEN.2
FAU_SAR.1
FAU_SAR.2
FAU_SAR.3
FAU_STG.1
FAU_STG.4
FCO_NRO.2
FCS_CKM.3
FCS_COP.1/SAD PIN decipher
FCS_COP.1/SAD PIN envelope decipher
FCS_COP.1/HMAC
FCS_COP.1/SAD signature verification
FCS_COP.2/SCD-SVD generation
FCS_COP.2/SCD activation
FCS_COP.2/SAD PIN change
FIA_UID.2
FIA_UAU.2
FIA_UAU.6
FIA_AFL.1
FIA_SOS.1
FDP_ACC.1/Administrative
FDP_ACC.1/Signer
FDP_ACC.2/Applications
FDP_ACF.1/Management
FDP_ACF.1/Signature
FDP_ACF.1/Applications
FDP_ETC.2/CSR
FDP_ITC.1/Certificate association
FDP_ITC.1/SSA public key
FDP_RIP.1
FDP_SDI.2
FDP_SDC.1
FDP_UDC.1
FDP_UCT.1
FDP_UIT.1
FMT_MSA.1/Accounts
FMT_MSA.1/Create key
FMT_MSA.1/Activate key
FMT_MSA.1/Change SAD PIN
FMT_MSA.2

FMT_MSA.4
FMT_SMF.1
FMT_MTD.1
FMT_SMR.1/Administrative
FMT_SMR.1/Applications
FTA_SSL.3
FTA_SSL.4

IDENTIFICATION

Product: ANCERT Server Signing Application v1.1.8

Security Target: Security Target for Server Signing Application, v1.10 (16 April 2019).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4+ALC_FLR.2+AVA_VAN.5.

SECURITY POLICIES

The use of the product ANCERT Server Signing Application v1.1.8 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 4.4 (Organizational policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 4.5 (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], chapter 4.3 (Threats) not suppose a risk for the product ANCERT Server Signing Application v1.1.8, although the agents implementing attacks have the attack potential according to the High of EAL4+ALC_FLR.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], chapter 5.2 (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.

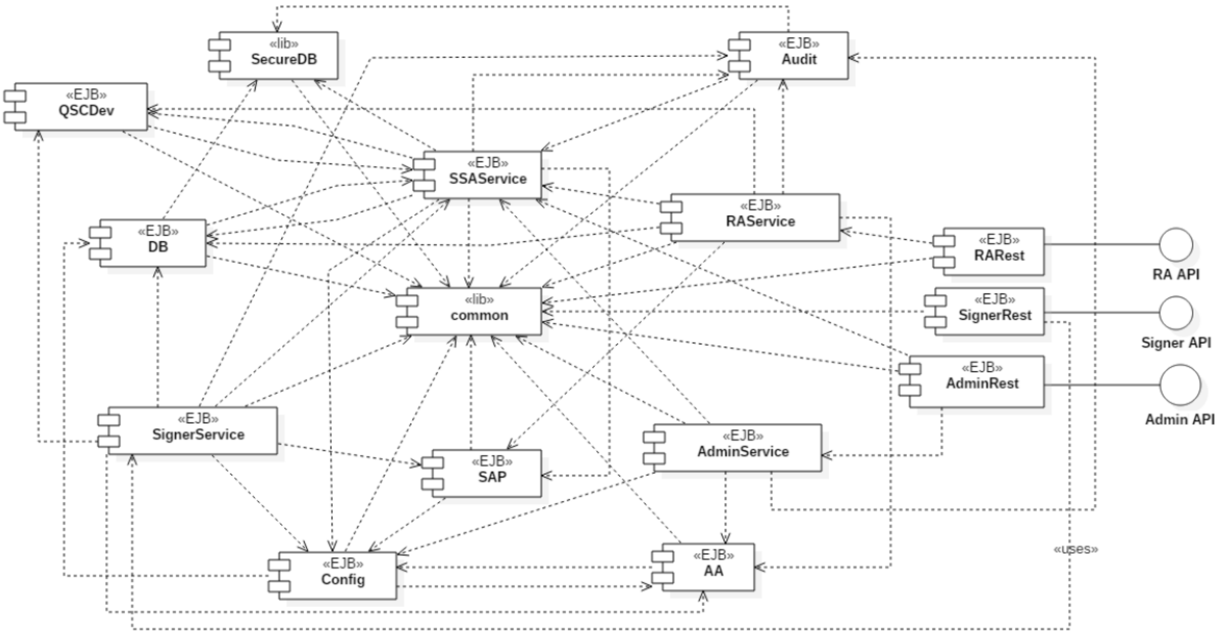
ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE consists of four subsystems and fifteen modules, which are related as shown in the table below.

SUBSYSTEM	MODULE
CORE	Common
	SecureDB
	AA
	Audit
	Config
	DB
	QSCDev
	SAP
	SSAService
ADMIN	AdminService
	AdminRest
RA	RAService
	RARest
SIGNER	SignerService
	SignerRest

The logical relations between modules are shown in the figure below.



PHYSICAL ARCHITECTURE

The TOE is a software application where all the components belonging the TOE are included and they are delivered in a single file (*ssa.ear*). The version number (1.1.8) is specified in the software package.

DOCUMENTS

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

- AGD_PRE: Preparative procedures (v2.12).
- AGD_OPE: Operational procedures (v1.12).
- ADV_FSP: Application functional specification (v2.12).

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the Security Target [ST].

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

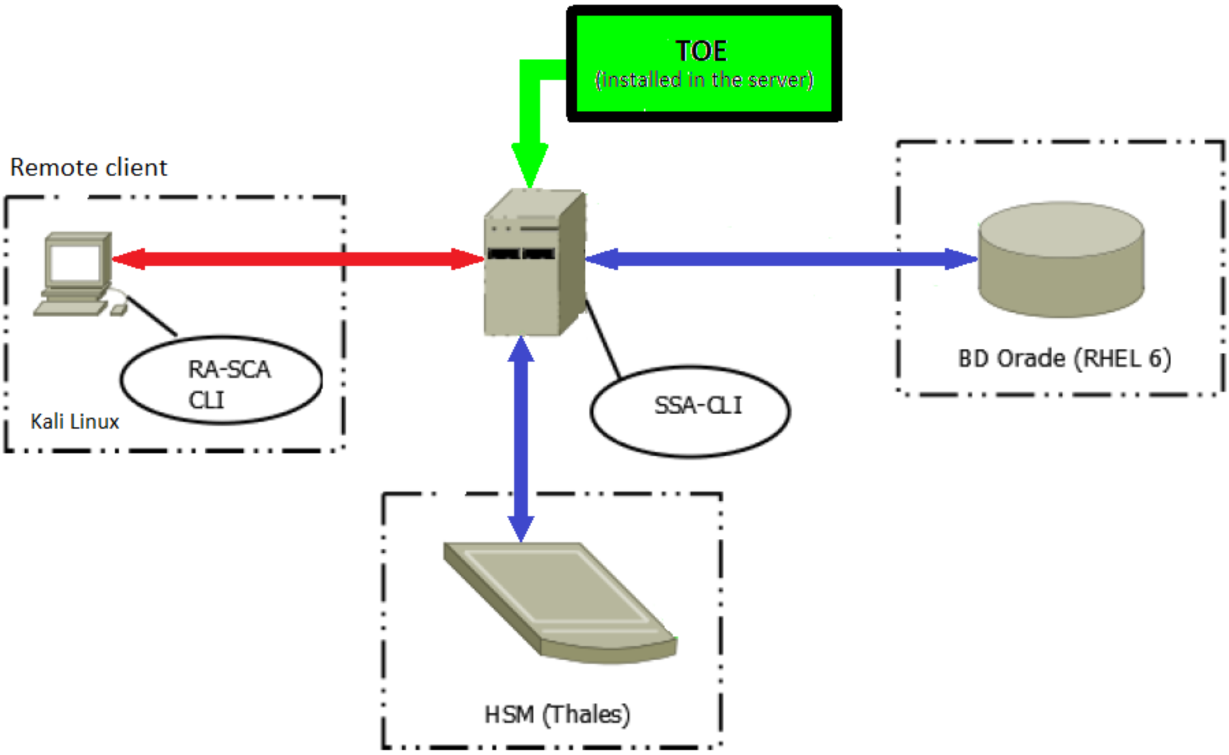
The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in the Security Target [ST].

PENETRATION TESTING

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE does NOT present exploitable vulnerabilities under the environment defined in the Security Target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the Security Target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “High” has been successful in the TOE’s operational environment as defined in the Security Target [ST] when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE under evaluation is the software application “ANCERT Server Signing Application v1.1.8”. The following figure depicts the detailed deployment diagram for the evaluated configuration.



The requirements for the TOE server and the operational environment element are detailed below:

- Server running the TOE (SSA v1.1.8 application):
  - 2 CPU x64 @ 2.0 GHz, 4GB RAM, 40 GB HD
- Operating System:
  - Red Hat EL 6 x64
- Server software:
  - Java Runtime Environment: Oracle JDK version 7u79 with JCE unlimited strength policy extension
  - J2EE Application Server: JBOSS EAP version 6.4.0
  - Cryptographic module support software: Thales Security World software version 11.72.02
  - Cryptographic support libraries: Bouncy Castle JCE version 1.54
  - Database driver: Oracle Instant Client and JDBC Driver version 12.1
- Cryptographic module:
  - Thales nCipher nShield Connect+ HSM with firmware 2.55.1
- Relational Database Management System:
  - Oracle 11g or Oracle 12c (all editions supported from XE to Enterprise Edition).
- PKI components needed to support the signature process:
  - Certification Authority
  - Registration authority

EVALUATION RESULTS

The product ANCERT Server Signing Application v1.1.8 has been evaluated against the Security Target for Server Signing Application, v1.10 (16 April 2019).

All the assurance components required by the evaluation level EAL4+ALC_FLR.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 EAL4+ALC_FLR.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.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Applus Laboratories, 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, 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] Security Target for Server Signing Application, v1.10 (16 April 2019).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Security Target for Server Signing Application, v1.10 (16 April 2019).

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 CCRA for all assurance components up to EAL2 and ALC_FLR.