REF: 2016-39-INF-2260 v1	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 05.03.2018	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-39 ANCERT Server Signing Application version 1.1.7

Applicant: B83395988 Agencia Notarial de CertificaciónENRIC HERNÁNDEZ JIMÉNEZ

References:

[EXT-3147] Certification request of ANCERT Server Signing Application version 1.1.7

[EXT-3771] Evaluation Technical Report of ANCERT Server Signing Application version 1.1.7.

The product documentation referenced in the above documents.

Certification report of the product ANCERT Server Signing Application v1.1.7, as requested in [EXT-3147] dated 06/09/2016, and evaluated by the laboratory APPLUS+ Laboratories, as detailed in the Evaluation Technical Report [EXT-3771] received on 09/02/2018.

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION **7**
SECURITY POLICIES **7**
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT **8**
CLARIFICATIONS ON NON-COVERED THREATS 9
OPERATIONAL ENVIRONMENT FUNCTIONALITY 10
ARCHITECTURE **13**
LOGICAL ARCHITECTURE 13
PHYSICAL ARCHITECTURE 14
DOCUMENTS **14**
PRODUCT TESTING **14**
PENETRATION TESTING **15**
EVALUATED CONFIGURATION **15**
EVALUATION RESULTS **17**
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM **17**
CERTIFIER RECOMMENDATIONS **17**
BIBLIOGRAPHY **18**
SECURITY TARGET **18**
RECOGNITION AGREEMENTS **19**
EUROPEAN RECOGNITION OF ITSEC/CC – CERTIFICATES (SOGIS-MRA) 19
INTERNATIONAL RECOGNITION OF CC – CERTIFICATES (CCRA) 19

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product ANCERT Server Signing Application v1.1.7.

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

Developer/manufacturer: ANCERT - Agencia Notarial de Certificación.

Sponsor: ANCERT - Agencia Notarial de Certificación.

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

ITSEF: APPLUS+ Laboratories

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R4 EAL4+ALC_FLR.2.

Evaluation end date: 09/02/2018.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.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_FLR.2, 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 ANCERT Server Signing Application v1.1.7, 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 component ALC_FLR.2, according to Common Criteria v3.1 R4.

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.3 Focused vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

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

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 v1.1.7

Security Target: Security Target for Server Signing Application, v1.2 (14 December 2017).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R4 EAL4+ALC_FLR.2.

SECURITY POLICIES

The use of the product ANCERT Server Signing Application v1.1.7 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. In short, it establishes the need of implementing organisational policies related to the following aspects.

Policy 01: P.CERTIFICATE

The certificates generated to be used in the TOE are trusted and according to eIDAS Art.3:14, Art.3:15, Annex I and to the policy for certificate generation of the TSP.

Policy 02: P.SIGNATURE_DATA

The signature creation data related to the DTBS or DTBSR used by the TOE are under control of the signer and allows detecting subsequent modifications.

Policy 03: P.REGISTRY

The identity of the holder is checked through a secure identification procedure before registering.

Policy 04: P.SIGNER_DATA

User data and certificates for accessing the TOE services by the signature creation applications and the related authentication data will be securely maintained during the signature procedure.

Policy 05: P.CONFIGURATION

The TOE is installed and configured by following the guidance's provided by the vendor.

Policy 06: P.ALERT

Alerts received during the authenticity checking of data stored in the database will be reviewed by the authorized personnel.

Policy 07: P.HSM

The hardware security module provides security features enough to ensure the robustness of the cryptographic operations.

Policy 08: P.ROL_GRANULARITY

The administrative users are related to a unique role so that not all the operations in the TOE and the environment are not in charge of a single administrator.

Policy 09: P.AUDIT_EXPORTATION

The auditory data are periodically exported from the TOE and are securely stored by authorized personnel by using secure means.

Policy 10: P.BACKUP

The TOE data necessary to perform a recovery of the system are periodically backed up and securely stored by authorized personnel by using secure means.

Policy 11: P.SIGN_ALGORITHMS

It is established the use of asymmetric cryptographic algorithms and key sizes recommended by "ETSI/TS 119 312" [ESI312] for hashing and signing.

Policy 12: P.ENCRYPTION_ALGORITHMS

It is established the use of cryptographic symmetric algorithms and key sizes recommended by "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms" [SOGCRYPT] for data encryption.

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.

Assumption 01: A.TSP

The certification authority and TSP that issues certificates uses practices and methodology according to the approved certification policy.

Assumption 02: A.SCA

The SCA used to generate DTSB or DTBSR works properly and generates the data in a proper way to be used by the TOE.

Assumption 03: A.ENVIRONMENT

The environment (DB, HSM, operating system, application server and all the devices involved) are properly installed and secure configured to ensure the protection of the TOE and TOE resources.

Assumption 04: A.NO_EVIL

Administrators are non-hostile, appropriately trained and follow all administrator guidance.

Assumption 05: A.SIGNERS

All the signers have knowledge enough to operate the TOE correctly and will follow the guidance's provided by the vendor.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product ANCERT Server Signing Application version 1.1.7, although the agents implementing attacks have the attack potential according to the Enhanced Basic of EAL4+ALC_FLR.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 categorized below.

Threat 01: T.ACCESS_CONTROL

External agent accessing the management of the TOE and performing not allowed operations.

Threat 02: T.COUNTERFEIT

External agent accessing to signature services and using SCD to perform signatures on behalf of the legitimate user.

Threat 03: T.DTBS_MODIFICATION

External agent modifies the data to be signed or their representation (DTBS or DTBS/R) used by the TOE in the way that the signed data is not the same that the signer sent to the TOE for being signed.

Threat 04: T.SD_MODIFICATION

External agent modifies the signed data (SD) in order to have new signed data that are not detected by the signature verification.

Threat 05: T.SAD_ACCESS

External agent accesses to the authentication data or signature activation data of the signers and is able to generate a signature without the signer having authorized the operation.

Threat 06: T.SCD_ACCESS

Internal agent access to signature creation data (SCD) out of the TOE or the environment and is able to generate a signature without the signer having authorized the operation.

Threat 07: T.USERS_DATA_MOD

External or internal agent without privileges modifies the signer's data to assign the SCD to another signer.

Threat 08: T.CONF_MODIFICATION

External or internal agent without privileges modifies the TOE configuration data to modify the privileges or the communication with the environment.

Threat 09: T.AUDIT_MODIFICATION

External or internal agent modifies the information recorded by the auditory data or generates invalid auditory information recorded as actual information.

Threat 10: T.BBDD_DATA

External or internal agent generates data in the database coming from another TOE or coming from a misconfiguration of the proper database that are taken by the TOE as valid data.

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 categorized below.

Environment objective 01: OE.PHYS_ACCESS

The TOE is installed in a restricted access environment under control of the administrative users that are in charge of control the physical access to the TOE.

Environment objective 02: OE.TOE_ACCESS

The IT environment shall provide mechanisms that control user's logical access to the TOE.

Environment objective 03: OE.TOE_PROTECTION

The IT environment shall protect the TOE and TOE resources from external interference, tampering, or unauthorized disclosure and modification.

Environment objective 04: OE.NO_EVIL

The TSP using the TOE shall ensure that administrative users are non-hostile, appropriately trained and follow all administrative guidance.

Environment objective 05: OE.SECURE_COMMS

The operational environment shall provide a secure communication line between the TOE and the other devices used for the correct operation of the TOE, in particular the command line interface, the RA and the Cloud KSP using the TLS protocol. TLS communications channels are provided and managed in the JBOSS application server.
The TOE communicates with the HSM making local calls to the PKCS#11 library provided by the HSM manufacturer (cryptographic module support software).

Environment objective 06: OE.SVD_VALIDATION

The TSP will check the SVD validity with the proof of possession (PKCS#10) exported from the TOE before providing the appropriate certificate to the SVD.

Environment objective 07: OE.SCD_SVD

The HSM guarantees the quality of the pair SCD/SVD to ensure that the probability of generating two times the same SCD is negligible.

Environment objective 08: OE.CERTIFICATE_GEN

The registration authority request the TSP to generate the certificates according to eIDAS Art.3:14, Art.3:15, Annex I and EN 319 411 including the name of the signer, the SVD related to the SCD generated by means of the TOE and the signature of the TSP.

Environment objective 09: OE.AUT_DATA_PROT

The application requesting the authentication data will ensure the confidentiality and integrity of them until being sent to the TOE.

Environment objective 10: OE.DTBS_CORRECT

The DTBS and DTBSR provided by the users through the environment to the TOE are correctly formatted and are provided by a secure channel that ensures the confidentiality and integrity of these data.

Environment objective 11: OE.TOE_CONFIG

The guidance's to correctly configure and operate the TOE are available.

Environment objective 12: OE.SIGNER_ACCOUNT

Registration authority will check the identity of the signer and ensures the user to configure the SAD and will maintain the confidentiality and integrity of the data until sending to the TOE.

Environment objective 13: OE.SECURE_BACKUP

Periodic backups will be done and the environment will ensure the integrity and confidentiality of the stored data. The backups will contain the information enough to ensure the correct operation of the TOE and the environment (HSM and DB) after an eventual failure of the system.

Environment objective 14: OE.SECURE_HSM

The HSM used to perform signature among other cryptographic operations will maintain a high security level by fulfilling the following:

- FIPS PUB 140-2 level 3 certified.

Environment objective 15: OE.VALIDATION_HMAC

The auditory and DB data will be periodically checked to find data that could be non-generated by the TOE.

Environment objective 16: OE.SIGNERS_OPER

The guidance's to correctly operate the TOE are available, including security warnings for keeping the VAD secured.

Environment objective 17: OE.ROLE_ASSIGNMENT

User's belonging to a particular role cannot be assigned to another role at the time.

Environment objective 18: OE.AUDIT_BACKUP

The procedure for backing up the audit data will be periodically executed by the authorized personnel and the resulting backup will be securely stored.

Environment objective 19: OE.SECURE_CRYPTO

The following algorithms will be used by the TOE and the environment to ensure the fulfillment of [ESI312]:

- SHA-256 or higher for hashing on the DTBS.
- RSA with key of 2048 bits or higher for signature.

The following algorithms will be used by the TOE and the environment to ensure the fulfillment of [SOGCRYPT]:

- AES with key of 128 bits or higher for data encryption and Signer key wrapping.

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.

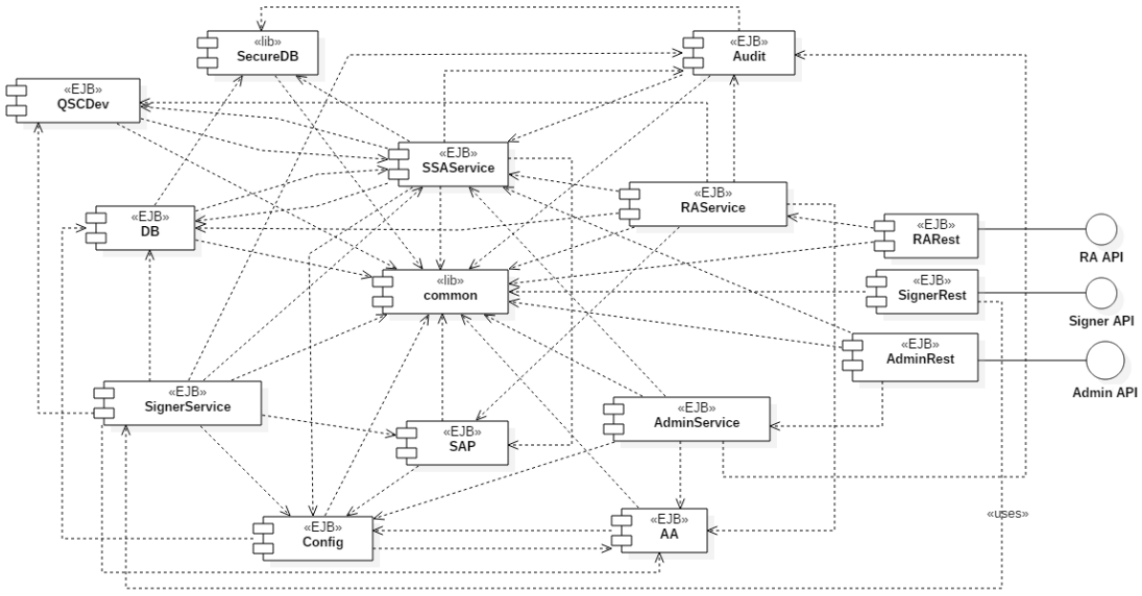
ARCHITECTURE

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 (1.1.7) 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 (v2.6).
- AGD_OPE: Operational procedures (v1.7).
- ADV_FSP: Application functional specification (v2.8).

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].

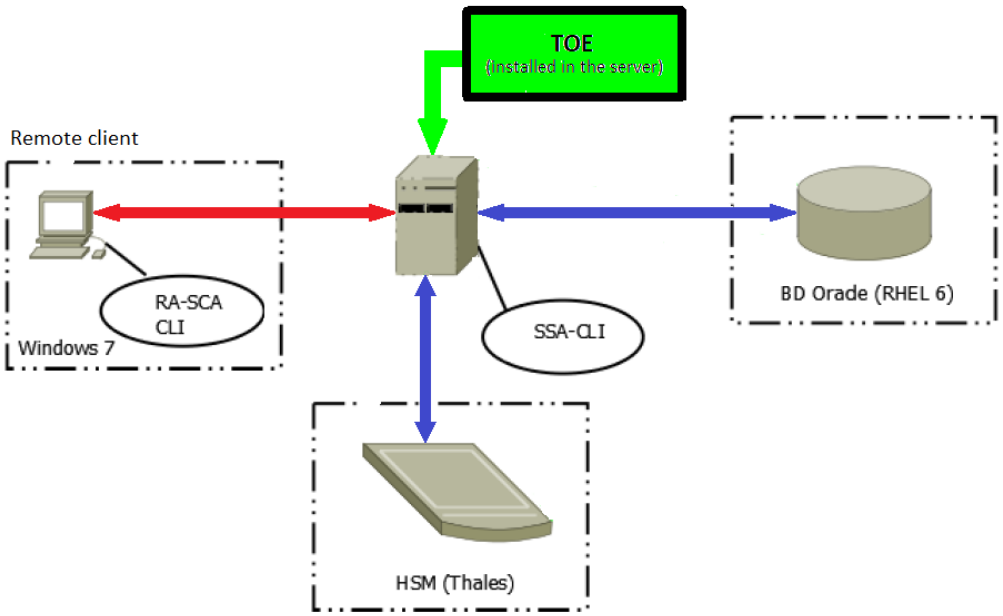
The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report 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 “Enhanced Basic” 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 v1.1.7”. The following figure depicts the detailed deployment diagram for the evaluated configuration.



The requirements for the server where the TOE is installed and the other operational environment elements are detailed below:

- Server running the TOE (SSA v1.1.7 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 11.62
  - Cryptographic support libraries: Bouncy Castle JCE version 1.54
  - Database driver: Oracle Instant Client and JDBC Driver version 12.1
- Cryptographic module:
  - Thales nCipher HSM with firmware 2.50.16-fips
- 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 v1.1.7 has been evaluated against the Security Target for Server Signing Application, v1.2 (14 December 2017).

All the assurance components required by the evaluation level EAL4+ALC_FLR.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_FLR.2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

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.

1. Since the signature authentication keys are stored in the end user device (signer device), it is recommended to set strong security measures in the device in order to protect the keys, including the screen with PIN and activating the security measures available in the operating system.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product ANCERT Server Signing Application v1.1.7, a positive resolution is proposed.

1. It must be noted that the manufacturer has assigned a PUBLIC level to the TOE confidentiality, according to the risk analysis carried out by the company. As a consequence, the evaluation for the component ALC_DVS.1 has been carried out accordingly considering that the TOE confidentiality classification is PUBLIC.

2. Users must take into account that the audit trail integrity and audit records authenticity is only checked on the TOE start-up and on each time an auditor requests an audit log search or export operation, according to the application note included by the manufacturer in the Security Target.

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.

[SOGCRYPT] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, version 1.0, May 2016.

[ST] Security Target for Server Signing Application, v1.2 (14 December 2017).

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Security Target for Server Signing Application, v1.2 (14 December 2017).

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.