Reference: 2020-34-INF-3784- v1
Target: Limitada al expediente
Date: 20.04.2022

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

CERTIFICATION REPORT

Dossier #	**2020-34**
TOE	**SIAVAL PKI VERSION 1**
Applicant	**A82733262 - Sistemas Informáticos Abiertos, S.A.**
References	

[EXT-6146] Certification Request

[EXT-7670] Evaluation Technical Report

Certification report of the product SIAVAL PKI VERSION 1, as requested in [EXT-6146] dated 31/08/2020, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-7670] received on 28/03/2022.

CONTENTS

EXECUTIVE SUMMARY 3
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION 6
SECURITY POLICIES 6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 6
CLARIFICATIONS ON NON-COVERED THREATS 7
OPERATIONAL ENVIRONMENT FUNCTIONALITY 7
ARCHITECTURE 7
LOGICAL ARCHITECTURE 7
PHYSICAL ARCHITECTURE 8
DOCUMENTS 9
PRODUCT TESTING 9
EVALUATED CONFIGURATION 10
EVALUATION RESULTS 10
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 11
CERTIFIER RECOMMENDATIONS 11
GLOSSARY 11
BIBLIOGRAPHY 12
SECURITY TARGET 12
RECOGNITION AGREEMENTS 13
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 13
International Recognition of CC – Certificates (CCRA) 13

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SIAVAL PKI VERSION 1.

Developer/manufacturer: Sistemas Informáticos Abiertos, S.A.

Sponsor: Sistemas Informáticos Abiertos, S.A..

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profile: No.

Evaluation Level: Common Criteria for Information Technology Security Evaluation v3.1 R5EAL4 + ALC_FLR.1.

Evaluation end date: 06/04/2022.

Expiration Date[1]: 21/04/2027.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.1) have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 + ALC_FLR.1, as defined by the Common Criteria for Information Technology Security Evaluation v3.1 R5 and the Common Methodology for Information Technology Security Evaluation v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product SIAVAL PKI VERSION 1, a positive resolution is proposed.

TOE SUMMARY

SIAVAL PKI comprises all the security functions required by a Certification Authority, allowing the issuance of certificates and CRLs, the management of the life cycle of these certificates and the capacity to provide information about the revocation status so that from a VA its status can be verified.

The TOE SIAVAL PKI consists of a set of modules based on the open source solution of EJBCA in its Community version where other proprietary modules of the SIAVAL family have been incorporated, such as the component for the protection of audit logs and integration with the SIAVAL VA.

The main functionality offered by the TOE is detailed next:

- **Access Control**: Access control is established for the operations performed in the TOE so that only authorized users can perform the operations for which they have been authorized.

[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.

Only the HealthCheck service does not establish user access control but performs IP access control to validate the origin of the requests.

- **Key Management**: The private keys of the CAs will reside in a cryptographic module outside the TOE scope and the TSF will make use of them for the issuance of certificates and CRLs, invoking the signature operation on the device. The public keys are stored in x509 certificates and protected in integrity
- **Management of the issuance of certificates and CRLs**: Several CA's can be managed by establishing a hierarchy among them, so that a Root CA and subordinate CA's can be established to issue for example certificates with different purposes, personal signature certificates, SSL/TLS Web certificates, etc

  Certificates and signed CRLs are generated, making it possible to request certificates through CSR using a mechanism such as PKCS # 10 or CRMF.

  Profiles and configurations are established for the issuance of certificates and generation of CRLs, so that it is possible to establish your own characteristics depending on the configuration of the profile.

  It enables the publication of certificates and CRLs in different repositories as well as the recovery of these certificates and CRLs from the TOE itself.
- **Transmission Data security**: The user keys will always be exported in keystores and certificates and CRLs will always be issued in a way that preserves their integrity.
- **Audit Data**: Audit trail is recorded for all operations performed by users in the system. A value calculated by the TSF will be added so that the integrity of the contained data can be checked. The analysis and consultation of audit data is not part of the scope of the TOE.

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.1, according to Common Criteria v3.1 R5 Part 3.

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.1
	ALC_LCD.1
	ALC_TAT.1
	ALC_FLR.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 following functional requirements, according to Common Criteria v3.1 R5 Part2:

Requirement Class	Requirement Component
Security Audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_STG.5 Audit log signing event
Communication (FCO)	FCO_NRO.1 Selective proof of origin
User Data Protection (FDP)	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
	FDP_UCT.1 Basic data exchange confidentiality
Identification & Authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.1 Timing of authentication
	FIA_UID.1 Timing of identification
	FIA_USB.1 User-subject binding
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MSA.1 Management of security attributes

	FMT_MSA.3 Static attribute initialisation
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Cryptographic operations (FCS)	FCS_COP.1 Cryptographic operation
	FCS_COP.2 Delegated Cryptographic operation
Security Key Infrastructure (FKI)	**FKI_CER.1 Certificate X509 Generation**
	FKI_CER.2 Stored public key integrity
	FKI_CRL.1 Certificate revocation list generation
	FKI_EXP.2 User private key export protected
	FKI_EXP.1 Certificate status export

IDENTIFICATION

Product: SIAVAL PKI VERSION 1

Security Target: SIAVAL PKI – Security Target, version 5.0, 23/03/2022.

Protection Profile: No.

Evaluation Level: Common Criteria for Information Technology Security Evaluation v3.1 R5 EAL4 + ALC_FLR.1.

SECURITY POLICIES

The use of the product SIAVAL PKI VERSION 1 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 3.2 (“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 3.3 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The threats declared in section 3.1(“Threats”) of the Security Target do not suppose a risk for the product SIAVAL PKI VERSION 1, although the agents implementing attacks have the attack potential according to EAL4 + ALC_FLR.1 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 those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security Objectives for the Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is a set of components that make up the solution, all of them running on an application server but in a modular way.

The logical components included in the TOE are:

- SIAVAL PKI AdminWeb: Administration Console Web.
- EJBCore Module: Core System functional module.
- WebServices Interface: Provides access to the TOE through a WebServices interface.
- Certificate and CRLs publisher module: Module that is in charge of publishing the certificates and CRLs issued by the TOE.
- Certificate status publisher module: Module that is responsible for publishing the status of certificates.
- SIAVAL Certificate status publisher module: Module that is responsible for publishing the status of certificates for SIAVAL VA.
- SIAVAL Audit records generation and protection module: Module called LogIntegrity that records the security events of the system so that they are protected in integrity.

- PKCS#11 module: Module used for communication between the TOE and the cryptographic module. The TOE uses the PKCS11 standard to communicate with the customer that each manufacturer of the cryptographic module provides in order to interact with it.
- SoftCrypto module: Module for cryptographic operations made by the TOE to protect assets that will be stored in the database, such as passwords, activation codes or users' key pairs.
- HealthCheck Interface: Provides system status of the TOE.

The following illustration represents the logical architecture of the components that make up the complete solution, distinguishing between those that belong to the TOE and those components that are not part of the TOE and are external to it but are necessary for its proper functioning:

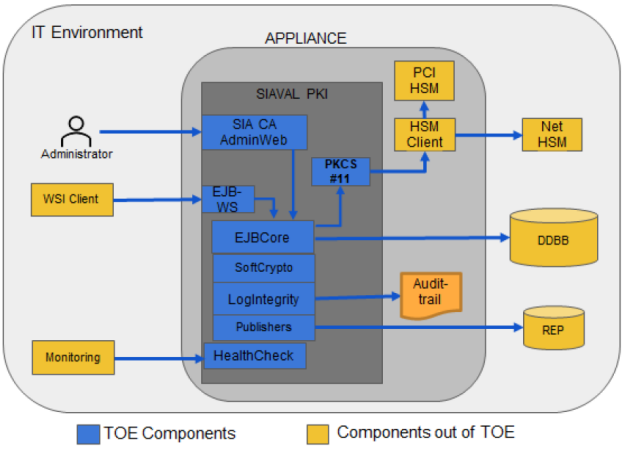

Figure 1 Logical TOE architecture

PHYSICAL ARCHITECTURE

The TOE is software where all components are included and supplied in a single file type ear.

- sia_ca.ear, version 1

  (SHA-256: ED663E022105701B44713E6C252044E841ED68E7D081F24098EA0259173C81E7)

The software is delivered to the end user installed on a hardware machine as an appliance, with the operating system, application server and other necessary utilities and interfaces previously installed.

Along with the TOE software, a set of manuals in .pdf format is provided, which describe how to configure and operate each of the components that constitute it as well as its operating environment. The list of TOE manuals can be found in the next section.

DOCUMENTS

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

- SIAVAL PKI - Manual de Operaciones, version 1.2, 16/12/2021: Operations manual for SIAVAL PKI roles in pdf format.

  (SHA256: 03B554DACF7E79F5E7E18081AA7DC1D02FB39678D93E75F3BB1509E0BD431564)

- SIAVAL PKI - Manual de Configuración Segura, version 1.3, 23/03/2022: Secure configuration for compliance of common criteria certification in pdf format.

  (SHA256: F95772DEB819FE1B9B1484B708B394159C22BC190116A621D971E2AC84A7DFFA)

- SIAVAL PKI - Manual de uso Servicios Web, version 1.1, 09/12/2021: User manual for use the Web Services interface in pdf format.

  (SHA256: B598136D8A6AF499E75643AC95B3B0F31D4EA0EF5AAD848840F7E1739F1B8F42)

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 repeated 100% of the developer functional tests in the testing platform implemented in the evaluation laboratory, selecting one test for each of the most relevant functional class.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

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 software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product SIAVAL PKI VERSION 1 it is necessary the disposition of the following software components:

- sia_ca.ear, version 1

  (SHA-256: ED663E022105701B44713E6C252044E841ED68E7D081F24098EA0259173C81E7)

The TOE environment is the one defined in the security target in the section "1.2.2.2 Hardware/Software/Firmware Elements that are not part of the TOE but are necessary for its proper functioning" and "1.3.3 TOE Configuration".

- Hardware
  - Machine appliance where the TOE resides: Dell PowerEdge with Intel(R) Xeon(R)
  - HSM: LUNA PCI-E Cryptographic Module. Luna PCI 7
  - Machine with components external to the TOE: Virtual Machine with Operating System Windows 2012 R2.
- Software
  - Operating system on the TOE server: CentOS release 7.8.2003 (Core) of 64 bits.
  - Application server: WildFly 12
  - Database: PostgreSQL 12
  - HSM Client: Luna PCI Client. 7
  - Java Runtime Enviroment: OpenJDK 1.8.0_252
  - TOE: SIAVAL PKI 1

An NTP server is also required for time synchronization through a reliable time source.

EVALUATION RESULTS

The product SIAVAL PKI VERSION 1 has been evaluated against the Security Target SIAVAL PKI – Security Target, version 5.0, 23/03/2022.

All the assurance components required by the evaluation level EAL4 + ALC_FLR.1 have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ALC_FLR.1, as defined by the Common Criteria for Information

Technology Security Evaluation v3.1 R5 and the Common Methodology for Information Technology Security Evaluation 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.

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product SIAVAL PKI VERSION 1, a positive resolution is proposed.

The certifier strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on section DOCUMENTS of this certification report as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

The certifier remarks the following points that should be taken into account by potential consumers:

- The TOE records locally audit data according to security objective *O.Individual accountability and audit records*. The analysis and consultation of audit data is not part of the scope of the TOE. Consumers shall observe the following security objectives for the operational environment *OE.Auditors Review Audit Logs, OE.Physical Protection, OE.Trusted Path* and *OE.Validation of security function* and shall provide procedures and technical measures to accomplish them.

GLOSSARY

CCN Centro Criptológico Nacional

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.

SECURITY TARGET

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

- SIAVAL PKI – Security Target, version 5.0, 23/03/2022.

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.