Reference: 2024-29-INF-4667- v1
Target: Limitada al expediente
Date: 26.01.2026

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-29**
TOE	**SIAVAL PKI 2**
Applicant	**A82733262 - Sistemas Informáticos Abiertos, S.A.**
References	

[EXT-9103] Certification request

[EXT-9805] Evaluation Technical Report

Certification report of the product SIAVAL PKI 2, as requested in [EXT-9103] dated 22/05/2024, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-9103] received on 02/09/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SIAVAL PKI 2.

SIAVAL PKI as a Certification Authority is the certificate management solution of the SIAVAL product family, designed for the implementation of certification authorities and the management of the certificate life cycle, covering the main use cases associated with this technology.

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

Sponsor: Sistemas Informáticos Abiertos, S.A..

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

ITSEF: Nombre Laboratorio.

Protection Profile: None.

Evaluation Level: CC:2022 R1 EAL4 + ALC_FLR.1

Evaluation end date: 27/10/2025.

Expiration Date[1]: 16/11/2030

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 CC:2022 R1 and the CEM:2022 R1.

Considering the obtained evidence during the instruction of the certification request of the product SIAVAL PKI 2, a positive resolution is proposed.

TOE SUMMARY

The TOE is intended to issue certificates as well as manage their states throughout their life cycle, their publication in different repositories as well as the issuance of CRLs in order to determine the certificates that have been revoked from the CA.

A hierarchy of CA's can be established according to the needs of the system, allowing different profiles to be established for each CA so that certificates can be issued for different purposes.

[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.

Control of their signature keys is established at all times, ensuring the issuance of certificates by the CA as well as from their subordinate CA's.

The most common use cases that can be solved by using the TOE are:

- **eIDAS Providers.** SIAVAL PKI serves as an essential basis for the provision of qualified and reliable services for the issuance of signature certificates, seals, time stamps and associated profiles, according to the ETSI EN 319 4xx family of standards.
- **ICAO eMRTD/ePassport**. Allowing the implementation of the infrastructure for issuing e-passport certificates.
- **SSL Certificates for websites and components.** Allows the implementation of certification authorities for the issuance of server certificates, including the basis for the establishment of browser-trusted web server certificate issuance services according to CA/Browser Forum.
- **IoT-Internet of Things**. Authenticated, integrated and reliable communication between devices.
- **Integration with MDM/UEM systems**. Integrating with leading manufacturers of mobile device management technology to automate the rolling out of certificates to multi-use devices.
- **Private Networks /VPN. T**o establish trusted environments for networks, remote access clients and VPNs by issuing digital certificates.
- **User authentication. I**ncluding active directory services or cloud-based applications, from desktops or mobile devices.
- **Secure email**. With advanced key management capabilities for email encryption.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidence required by the additional component ALC_FLR.1, according to CC:2022 R1.

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_FLR.1
	ALC_LCD.1
	ALC_TAT.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 the CC:2022 R1:

FUNCTIONAL CLASS	FUNCTIONAL COMPONENT
Security Audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_STG.6 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 initialization
	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.1 Certificate status export
	FKI_EXP.2 User private key export protected

IDENTIFICATION

Product: SIAVAL PKI 2

Security Target: SIAVAL PKI – Security Target, version 7.3, 01/08/2025.

Protection Profile: None.

Evaluation Level: CC:2022 R1 EAL4 + ALC_FLR.1

SECURITY POLICIES

The use of the product SIAVAL PKI 2 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 (“Organization 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 following threats do not suppose a risk for the product SIAVAL PKI 2, although the agents implementing attacks have the attack potential according to the Enhanced-Basic of 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.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.1 (“Threats”).

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 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.

PHYSICAL ARCHITECTURE

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

- sia_ca.ear, version 2

The software is delivered to the end user installed on a hardware machine as an appliance or portable machine, 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 1.4, 26/05/2025: Operations manual for SIAVAL PKI roles in pdf format.

  (SHA-256: 3db871c88d9be509b6610e0c57b51132ba9de4059e591d1c0aa8820b26c8df37)
- SIAVAL PKI - Manual de Configuración Segura, version 1.7, 29/07/2025: Secure configuration for compliance of common criteria certification in pdf format.

  (SHA-256: 956f5b815c82ea12c67c1ee3c443b4703f3332e7feefd1be9e3a03bf8e61c743)
- SIAVAL PKI - Manual de uso Servicios Web, version 1.2, 09/09/2024: User manual for use the Web Services interface in pdf format.

  (SHA-256: 2785ea6e6a5a56136c72a9570554669561bbe9488a68ed97f769d7b0f903f8a6)

PRODUCT TESTING

The developer has executed tests for all the TSFIs. 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 has been identified and 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 all the developer functional tests in the developer premises in the testing platform implemented in the evaluation facility.

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

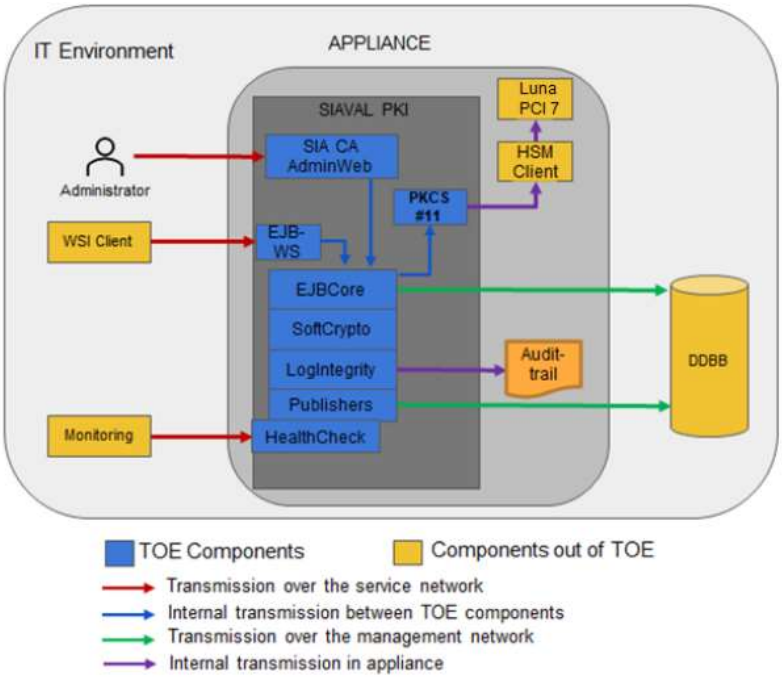
It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

Although the TOE supports other platforms, the evaluated environment is carried out on three specific platforms that have the following characteristics:

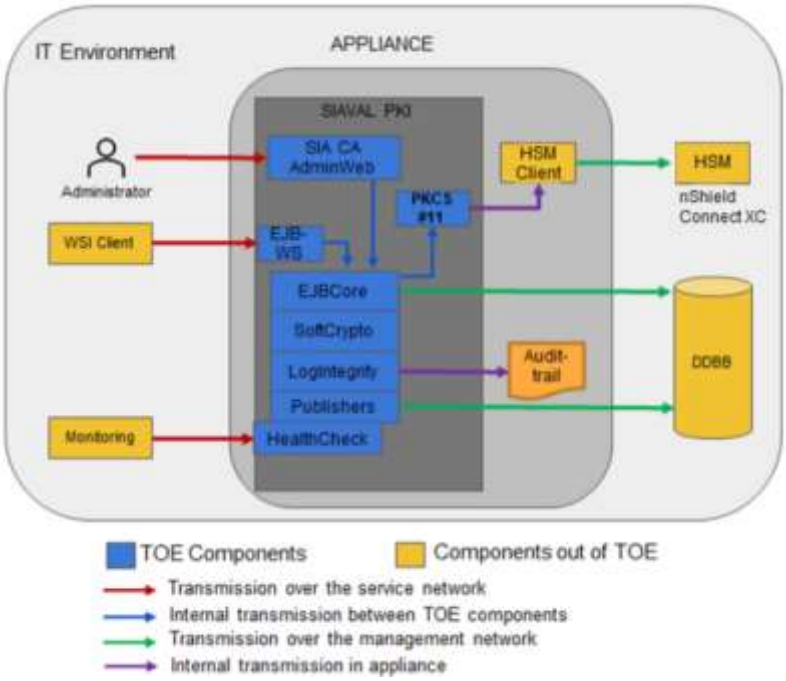
Configuration Environment 1:

- Hardware:
  - Machine appliance where the TOE resides: Dell PowerEdge with Intel(R) Xeon(R)
  - HSM: LUNA PCI-E Cryptographic Module. Luna PCI 7
- Software:
  - Operating system on the TOE server: Rocky Linux release 8.9
  - Application server: WildFly 12
  - Database: PostgreSQL 14
  - HSM Client: Luna PCI Client 7. Version 10.7.0
  - Java Runtime Environment: OpenJDK 1.8.0_402



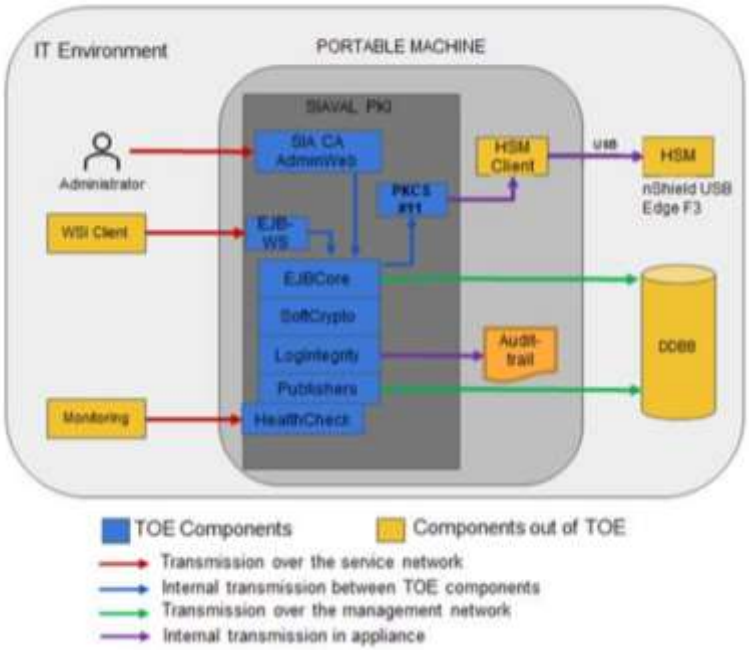
Configuration Environment 2:

- Hardware:
  - Machine appliance where the TOE resides: Dell PowerEdge with Intel(R) Xeon(R)
  - HSM: nShield Connect XC Mid F3
- Software:
  - Operating system on the TOE server: Rocky Linux release 8.9
  - Application server: WildFly 12
  - Database: PostgreSQL 14
  - HSM Client: nShield Client 13. Versión: 13.4.4
  - Java Runtime Environment: OpenJDK 1.8.0_402



Configuration Environment 3:

- Hardware:
  - Portable Machine where the TOE resides: HP EliteBook 650 G9
  - HSM: nShield USB Edge F3
- Software:
  - Operating system on the TOE server: Rocky Linux release 8.9
  - Application server: WildFly 12
  - Database: PostgreSQL 14
  - HSM Client: nShield Client 13. Versión: 13.4.4
  - Java Runtime Environment: OpenJDK 1.8.0_402



EVALUATION RESULTS

The product SIAVAL PKI 2 has been evaluated against the Security Target SIAVAL PKI – Security Target, version 7.3, 01/08/2025.

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 CC:2022 R1 and the CEM:2022 R1.

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.

- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.
- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidence during the instruction of the certification request of the product SIAVAL PKI 2, 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 point 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

CA	Certification Authority
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
CRL	Certification Revocation List
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HSM	Hardware Security Module
HW	Hardware
OC	Organismo de Certificación
PKI	Public Key Infrastructure
TOE	Target Of Evaluation
VA	Validation Authority

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, November 2022, CC:2022, Revision 1

[CC_P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, November 2022, CC:2022, Revision 1

[CC_P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, November 2022, CC:2022, Revision 1

[CC_P4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022, CC:2022, Revision 1

[CC_P5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022, Revision 1

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, November 2022, CC:2022, Revision 1

[ST] SIAVAL PKI – Security Target, version 7.3, 01/08/2025.

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:

- SIAVAL PKI – Security Target, version 7.3, 01/08/2025.

RECOGNITION AGREEMENTS

In order to avoid multiple certifications 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.