Referencia: 2024-52-INF-4601- v1
Difusión: Limitada al expediente
Fecha: 15.07.2025

Creado por: I007
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2024-52**
TOE	**SIAVAL SafeCert Manager v3**
Solicitante	**A82733262 - Sistemas Informáticos Abiertos, S.A.**
Referencias	

[EXT-9341] Solicitud de Certificación

[EXT-9590] Informe Técnico de Evaluación (ETR) v1.1

[EXT-9625] Informe Técnico de Evaluación (ETR) v1.2

Informe de Certificación del producto SIAVAL SafeCert Manager v3, según la solicitud de referencia [EXT-9341], de fecha 08/11/2024, evaluado por el laboratorio DEKRA Testing and Certification S.A.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-9590] y [EXT-9625], recibido el pasado 05/06/2025.

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto SIAVAL SafeCert Manager v3.

SIAVAL SafeCert es una solución de firma centralizada de la familia SIAVAL orientada a facilitar la gestión y el uso de las claves privadas y públicas de los usuarios finales, también identificados como titulares o firmantes.

Fabricante: Sistemas Informáticos Abiertos, S.A.

Patrocinador: Sistemas Informáticos Abiertos, S.A.

Organismo de Certificación: Centro Criptológico Nacional (CCN).

Laboratorio de Evaluación: DEKRA Testing and Certification S.A.U.

Perfil de Protección: No.

Nivel de Evaluación: Common Criteria CC:2022 R1 EAL 4 + ALC_FLR.1 + AVA_VAN.5.

Fecha de término de la evaluación: 12/06/2025

Fecha de expiración[1]: 15/07/2030

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 (aumentado con ALC_FLR.1 + AVA_VAN.5) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio DEKRA Testing and Certification S.A.U. asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL 4 + ALC_FLR.1 + AVA_VAN.5, definidas por los Common Criteria CC:2022 R1 y la CEM CC:2022 R1.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto SIAVAL SafeCert Manager v3, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

Funcionando en un entorno operacional seguro, con los componentes con un nivel de seguridad adecuado y siendo gestionado por un prestador cualificado, el producto SIAVAL SafeCert está diseñado para funcionar como un dispositivo cualificado de creación de firma (QSCD), según los requisitos especificados en el Reglamento (UE) nº 910/2014 del Parlamento Europeo (eIDAS: Anexo II), haciendo posible la generación de firmas electrónicas avanzadas (AdES) y de firmas electrónicas cualificadas o reconocidas (QES) en un servidor remoto, constituyéndose como un sistema

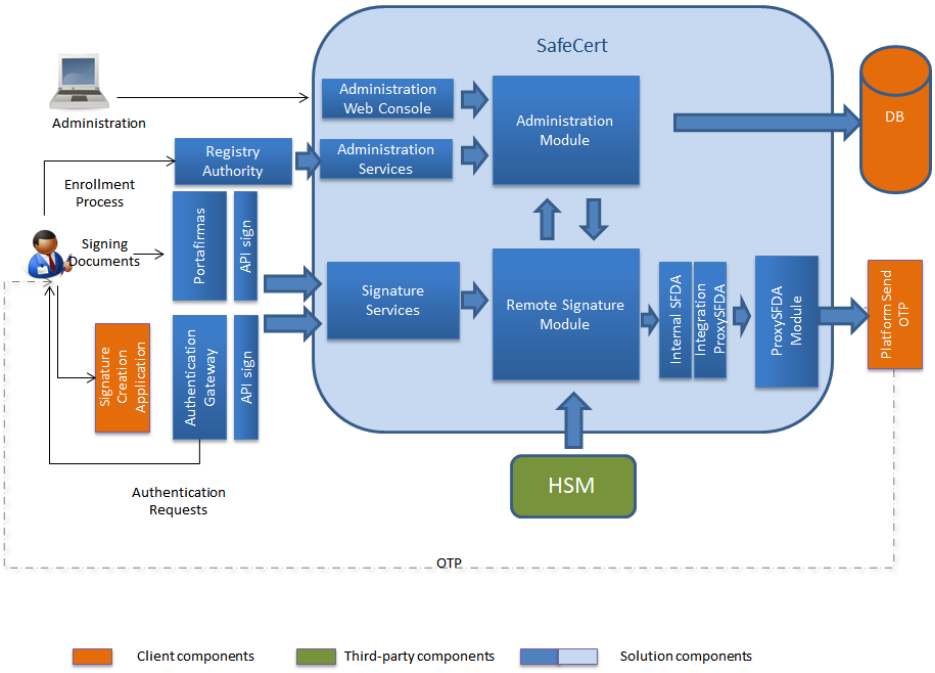
[1] Este campo se refiere a la fecha de expiración del reconocimiento del certificado en el ámbito de los acuerdos de reconocimiento mutuo firmados por este Organismo de Certificación.

confiable de firma en servidor, Trustworthy Systems Supporting Server Signing (TW4S), según se define en la norma CEN/TS 419 241 que rige este tipo de sistemas.

Tiene las siguientes características generales:

- El producto se centra en la firma del hash o hashes que representa el documento o documentos a firmar, quedando fuera de su alcance la composición de los formatos de los diferentes estándares de firma que pudieran ser construidos por la aplicación de creación de firma que utilizase este producto.
- Permite a los usuarios finales la realización de firmas electrónicas de manera sencilla, sin que éstos deban preocuparse de la gestión y mantenimiento de sus claves.
- Las claves se mantienen seguras y controladas mediante el uso de hardware criptográfico (HSM).
- Facilita la gestión del ciclo de vida de los certificados, puesto que las claves están centralizadas.
- Evita la dispersión o descontrol de las claves de los usuarios al no ser distribuidas y permanecer siempre bajo el control del HSM.
- Controla y audita el acceso a las claves mediante varios niveles de seguridad (PIN, Segundo Factor de Autenticación, etc).
- Dispone de Cliente CSP para Windows, que ofrece a las aplicaciones Windows ya existentes, que utilicen CAPI, la posibilidad de utilizar los certificados del usuario almacenados en SafeCert.
- Permite a los usuarios finales, titulares o firmantes importar certificados (con su clave privada) ya existentes de manera directa, a través del Cliente CSP para Windows.
- Facilita la integración desacoplada con terceros para delegar la generación, gestión y validación del segundo factor de autenticación (SFDA) que puede proteger el acceso a las claves.
- De manera integrada, puede utilizar el producto Identity Guard para la gestión del segundo factor de autenticación, bien mediante el uso de OTPs (One Time Password) enviados por SMS, bien mediante claves de un solo uso generadas en Token físico o software o, también, utilizando Tarjetas de Coordenadas, entre otros.
- Dispone de un componente interno de generación de OTPs (One Time Password) para ser utilizadas como segundo factor de autenticación del firmante.
- Dispone de una Consola web para la administración y gestión centralizada del producto, con distintos niveles de acceso mediante perfilado configurable. Mediante la consola puede realizarse la configuración de repositorios HSMs, conectores de segundo factor de autenticación, sistemas de segundo factor de autenticación, gestión de titulares, asignación y configuración de segundos factores de autenticación para el uso de las claves de cada titular, etc.

- Facilita un conjunto de Servicios web de gestión que permiten que se puedan confeccionar consolas específicas para determinados grupos de administradores con permisos controlados.
- Escalabilidad y Alta Disponibilidad: el diseño de Siaval Safecert y su distribución en formato hardware/appliance permite su adaptación a múltiples entornos de forma sencilla. Por diseño, Safecert permite escalar horizontalmente la infraestructura de firma, de forma que pueda absorber las necesidades de cualquier organización, desde entornos con decenas de firmantes hasta millones de ellos. SIAVAL Safecert ofrece flexibilidad para su instalación en clústeres de Alta Disponibilidad y Tolerancia a Fallos, convirtiéndose en una infraestructura de Firma centralizada totalmente confiable por las organizaciones.



REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL4, más las requeridas para los componentes adicionales ALC_FLR.1 + AVA_VAN.5, según los Common Criteria 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_LCD.1
	ALC_TAT.1
	ALC_FLR.1
ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según los Common Criteria CC:2022 R1.

Requirement Class	Requirement Component
Security Audit (FAU)	GEN.1 Operaciones del TOE
	GEN.1 Operaciones de los usuarios firmantes
	GEN.2 Identificación del usuario de la operación
	SAR.1 Revisión de los datos de auditoría de operaciones del TOE
	SAR.1 Revisión de los datos de auditoría de operaciones del usuario firmante
	SAR.2 Acceso restringido a los datos de auditoría del TOE
	SEL.1 Selección de los datos de auditoría de operaciones del TOE
	SEL.1 Selección de los datos de auditoría de operaciones de los usuarios firmantes
	STG.3 Archivado de datos de auditoría del TOE
	SAA.1 Potential violation analysis
	ARP.1 Security alarms

Communication (FCO)	NRO.1 CSR Generación del certificado
Cryptographic operations (FCS)	COP.1 descifrado / cifrado simétrico de datos
	COP.1 descifrado fichero configuración HMAC
	COP.1 verificación fichero configuración HMAC
	COP.1 cálculo / verificación HMAC
	CKM.1 descifrado/cifrado simétrico de datos
	CKM.3 clave protección fichero de configuración HMAC
	CKM.3 almacén comunicación segura ProxySFDA
	COP.2 generación de SCD/SVD (extendido)
	COP.2 activación del SCD en firma/autenticación (extendido)
	COP.2 cambio de contraseña (extendido)
User Data Protection (FDP)	ACC.2 Acceso a los servicios web SFP
	ACC.1 Operaciones de los usuarios firmantes SFP
	ACF.1 Acceso a los servicios web SFP
	ACF.1 Operaciones de los usuarios firmantes SFP
	ETC.2 Exportación CSR
	ITC.1 Histórico de contraseñas
	ITC.1 Asociación de certificado
	SDI.1 Stored data integrity monitoring
	SDC.1 Stored data confidentiality
	UDC.1 User data correspondence (extendido)
Identification & Authentication (FIA)	UAU.2 User authentication before any action
	UAU.5 Para los usuarios firmantes en las operaciones de firma y cambio de contraseña
	UID.2 User identification before any action
	AFL.1 Usuarios firmantes en la operación de firma/cambio de contraseña
Security Management (FMT)	MSA.1 ADMIN-OWNER
	MSA.1 CREATE_KEY
	MSA.1 CHANGE_PASSWORD_SERVICE
	SMF.1 Specification of Management Functions
	MTD.1 Consulta datos de auditoría
Trusted path/channels (FTP)	ITC.1 Aplicación de Registro
	ITC.1 Aplicación de Creación de Firma

	ITC.1 Base de datos
	ITC.1 Componente ProxySFDA

IDENTIFICACIÓN

Producto: SIAVAL SafeCert Manager v3.

Declaración de Seguridad: *SIAVAL SafeCert Manager - Declaración de Seguridad, versión 6.0, 24/04/2025*.

Perfil de Protección: No.

Nivel de Evaluación: Common Criteria CC:2022 R1 EAL 4 + ALC_FLR.1 + AVA_VAN.5.

POLÍTICA DE SEGURIDAD

El uso del producto SIAVAL SafeCert Manager v3 debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de estas políticas se encuentra en la Declaración de Seguridad en el apartado 3.4 “Políticas de seguridad organizacionales”.

HIPÓTESIS Y ENTORNO DE USO

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas. Por tanto, para garantizar el uso seguro del TOE, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE. Se pueden encontrar en el apartado 3.5 “Hipótesis” de la Declaración de Seguridad.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto SIAVAL SafeCert Manager v3, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a *High* de EAL4 + ALC_FLR.1 + AVA_VAN.5, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Las amenazas cubiertas por las propiedades de seguridad del TOE se encuentran en el apartado 3.3 “Amenazas” de la Declaración de Seguridad.

FUNCIONALIDAD DEL ENTORNO

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del TOE se encuentran en el apartado 4.2 “Objetivos de Seguridad del Entorno Operacional” de la Declaración de Seguridad.

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad) o de los requisitos de seguridad del TOE se encuentran en la correspondiente Declaración de Seguridad.

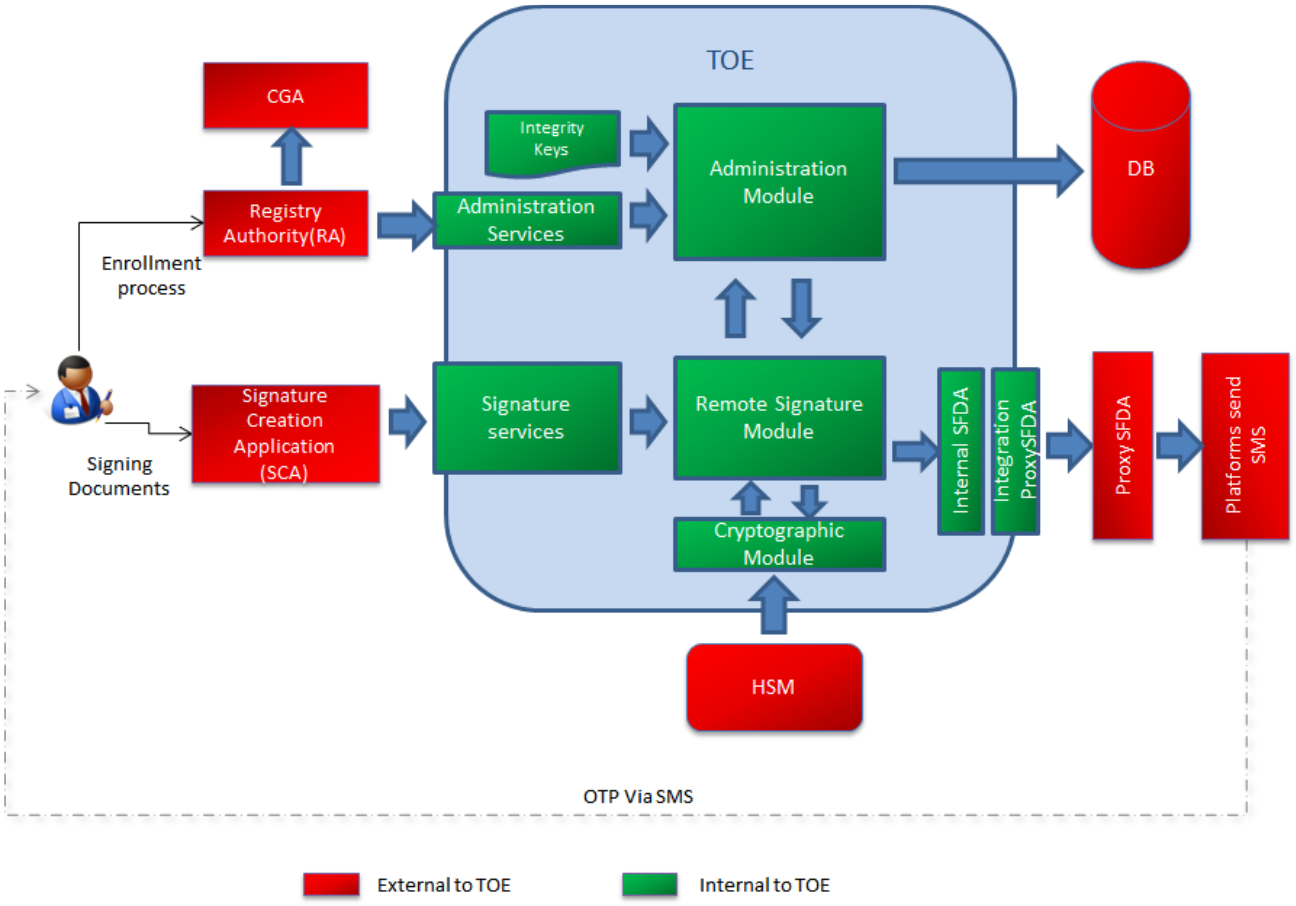
ARQUITECTURA

ARQUITECTURA LÓGICA

El TOE es un subconjunto de los componentes que conforman la solución global aportada por el producto. Los componentes lógicos incluidos en el TOE son:

- Módulo de firma: software que proporciona los servicios de firma, importación de claves mediante PKCS#12 y cambio de PIN de activación de la clave privada a través de Servicios Web convencionales y mediante el uso del API de Integración Java.
- Módulo criptográfico: invoca al HSM para realizar las operaciones criptográficas de protección de las claves y firma electrónica.
- Servicios web de administración: actúan sobre el módulo de administración.
- Módulo de gestión de Segundo Factor de Autenticación: generación y validación de OTPs como segundo factor de autenticación incluido en el TOE.
- Componentes de integración con Plataformas de Segundo Factor de Autenticación y envío de OTPs externos al TOE.
- Ficheros de configuración y claves para la generación y comprobación de la autoría de los datos.

En la siguiente ilustración se representa la arquitectura lógica de los componentes que constituyen la solución completa, distinguiendo entre los que pertenecen al TOE y aquellos componentes que no forman parte del TOE y son externos a él pero que son necesarios para su correcto funcionamiento:



ARQUITECTURA FÍSICA

El TOE es un software donde todos los componentes que lo conforman están incluidos y se suministran en un único fichero de tipo .war, de nombre "rss-webapp.war", en su versión 3 que vendrá especificado en su fichero MANIFEST interno.

El software se le entrega al consumidor final instalado en una máquina hardware, a modo de appliance, con el sistema operativo, servidor de aplicaciones y resto de utilidades e interfaces necesarios previamente instalados.

En la máquina en modo appliance ya se incluye además del software instalado, los ficheros de configuración necesarios para la correcta inicialización del sistema, entre esta configuración inicial se encuentran los ficheros y claves relativos a la generación HMAC que proporcionarán la autoría por parte del TOE de sus datos en la base de datos. No obstante, una vez configurada la conexión con la base de datos y ejecutado el script inicial de creación de datos de configuración, será necesario lanzar un proceso que se encargará de calcular los valores HMAC para estos datos iniciales de configuración.

Junto con el software del TOE se facilita un conjunto de manuales, en formato .pdf, en los que se describe la forma de instalar, configurar y operar cada uno de los componentes que lo constituyen, los ficheros .wsdl y el interfaz Hessian en los que se incluye la documentación de los servicios web

facilitados por el software del TOE junto con los esquemas de xml para el envío de datos a través de los servicios.

Listado de manuales del TOE:

- SIAVAL_SafeCert-Manual_de_Administración, Rev. 1.0
- SIAVAL_SafeCert-Manual_de_Instalación, Rev. 1.0
- SIAVAL_SafeCert-Manual_de_Integración, Rev. 1.0
- SIAVAL SafeCert-Manual de operaciones, Rev. 1.0
- SIAVAL SafeCert-Manual_de_configuración_segura, Rev. 3.0
- SIAVAL_SafeCert-Manual_de_Integración_ProxySFDA, Rev. 1.0

Definición de los servicios de firma y gestión

Servicios Web vía SOAP para los servicios de firma y gestión:

- AdminRSS_Services.wsdl.
- RemoteRSS_Services.wsdl.

Servicios Web Binarios Hessian para los servicios de firma:

- Services-Hessian-Firma-1.0.jar

Definición de los esquemas de datos para los servicios de firma y gestión:

- Services_1.xsd, XMLExtra_1.xsd, MonitorRSS_1.xsd, MonitorRSS_Result_1.xsd, Commons_Types_1.xsd, Operation_Error_1.xsd, Operation_Result_1.xsd.

En caso de tener que instalar alguna actualización del producto en una máquina de la que ya disponga el consumidor final, a éste se le facilita, por correo electrónico o accesible mediante acceso FTP, un proceso de actualización, en formato “.tgz” o “.zip”, que incluye el pre-proceso, el proceso y el post-proceso de la actualización del producto, que el consumidor final puede ejecutar sobre la máquina appliance utilizando la herramienta de gestión disponible para tal fin.

DOCUMENTOS

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- SIAVAL_SafeCert-Manual_de_Administración, Rev. 1.0
- SIAVAL_SafeCert-Manual_de_Instalación, Rev. 1.0
- SIAVAL_SafeCert-Manual_de_Integración, Rev. 1.0
- SIAVAL SafeCert-Manual de operaciones, Rev. 1.0
- SIAVAL SafeCert-Manual_de_configuración_segura, Rev. 3.0
- SIAVAL_SafeCert-Manual_de_Integración_ProxySFDA, Rev. 1.0

PRUEBAS DEL PRODUCTO

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante, en sus instalaciones, con resultado satisfactorios.

Durante el proceso de evaluación se ha verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas, acorde a la arquitectura identificada en la Declaración de Seguridad.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Para verificar los resultados de las pruebas del fabricante, el laboratorio ha repetido todas estas pruebas funcionales en la plataforma de pruebas montada en el laboratorio de evaluación.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados y, en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no representa un problema para la seguridad ni supone una merma en la capacidad funcional del producto.

CONFIGURACIÓN EVALUADA

Los requisitos software y hardware, así como las opciones referidas, son los que se indican a continuación. Así, para el funcionamiento del producto SIAVAL SafeCert Manager v3 es necesario disponer de los siguientes componentes:

Aunque el TOE soporta otras plataformas, las pruebas para llevar a cabo la evaluación del TOE se han realizado sobre una plataforma concreta que tiene las siguientes características significativas:

Hardware Appliance:

- **Máquina servidor en forma de appliance donde reside el TOE:** Dell PowerEdge con Intel(R) Xeon(R).
- **HSM:** Thales Luna K7 Cryptographic Module, con hardware version: 808-000048-002, firmware version: 7.7.2 y bootloader version: 1.1.2.
- **Máquina servicios externos al TOE:** PC externo genérico.

Software:

- **Sistema operativo en el servidor del TOE:** Rocky Linux 8.10.
- **Servidor de aplicaciones:** Apache Tomcat 9.0.97.
- **Sistema operativo en el servidor de servicios externos al TOE:** Windows 64 bits.
- **Base de datos:** PostgreSQL 16.
- **Cliente HSM:** Software Thales Luna K7 Client v10.
- **Java Runtime Environment en servidor del TOE:** OpenJDK 1.8.0_432.
- **Consola web de administración:** SIAVAL SafeCert Console 3.
- **Componente ProxySFDA:** SIAVAL SafeCert ProxySFDA 3.

RESULTADOS DE LA EVALUACIÓN

El producto SIAVAL SafeCert Manager v3 ha sido evaluado en base a la Declaración de Seguridad *SIAVAL SafeCert Manager - Declaración de Seguridad, versión 6.0, 24/04/2025*.

Todos los componentes de garantía requeridos por el nivel de evaluación *EAL 4 + ALC_FLR.1 + AVA_VAN.5* presentan el veredicto de "PASA". Por consiguiente, el laboratorio DEKRA Testing and Certification S.A.U. asigna el **VEREDICTO de "PASA"** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel *EAL 4 + ALC_FLR.1 + AVA_VAN.5*, definidas por los *Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1* y la *[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CC:2022, Revision 1*.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación, se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

- El usuario del TOE debe leer y comprender las guías de usuario para poder operar el TOE de manera adecuada de acuerdo a la Declaración de Seguridad.
- El cumplimiento de las hipótesis indicadas en la Declaración de Seguridad es un punto clave, ya que implica configuraciones del entorno operacional del TOE que dejan fuera del alcance algunas vulnerabilidades potenciales.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto SIAVAL SafeCert Manager v3, se propone la resolución estimatoria de la misma.

GLOSARIO DE TÉRMINOS

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

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[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, November 2022, CC:2022, Revision 1.

DECLARACIÓN DE SEGURIDAD

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

- *SIAVAL SafeCert Manager - Declaración de Seguridad, versión 6.0, 24/04/2025*.

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: https://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.