Referencia: 2018-22-INF-2759-v1
Difusión: Público
Fecha: 23.07.2019

Creado por: CERT8
Revisado por: CALIDAD
Aprobado por: TECNICO

# INFORME DE CERTIFICACIÓN

| | |
|---|---|
| Expediente # | **2018-22** |
| TOE | **SIAVAL SafeCert Manager, versión 3** |
| Solicitante | **A82733262 - Sistemas Informáticos Abiertos, S.A.** |
| Referencias | |

[EXT-4179] Solicitud de Certificación

[EXT-4738] Informe Técnico de Evaluación

Informe de Certificación del producto SIAVAL SafeCert Manager, versión 3, según la solicitud de referencia [EXT-4179], de fecha 20/06/2018, evaluado por el laboratorio Epoche & Espri S.L.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-4738], recibido el pasado 01/03/2019.

**CONTENIDOS**

# RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto SIAVAL SafeCert Manager, versión 3.

SIAVAL SafeCert Manager es un software de firma electrónica en servidor, que asegura el control exclusivo de las claves de firma por parte del firmante y genera tanto firma electrónica avanzada (AdES) como firma electrónica cualificada o reconocida (QES), y construido para ser usado en un entorno operacional seguro como un sistema confiable de firma en servidor.

El conjunto de componentes que conforman el TOE posibilita la generación de firmas en servidor, de manera que una organización pueda fácilmente establecer un sistema de firma seguro, centralizando los procesos de firma de documentos de sus usuarios. Facilita la gestión del ciclo de vida de los certificados, la asociación entre los usuarios y sus claves, así como el cumplimiento del propósito de uso de dichas claves.

Se establece en todo momento el control exclusivo por parte de los usuarios de sus claves de firma, asegurando el vínculo entre usuario y clave/certificado y protegiendo las claves privadas de firma de forma tal que únicamente puedan ser utilizadas dentro del entorno operativo y por los propietarios legítimos de dichas claves.

**Fabricante**: Sistemas Informáticos Abiertos, S.A..

**Patrocinador**: Sistemas Informáticos Abiertos, S.A..

**Organismo de Certificación**: Centro Criptológico Nacional (CCN).

**Laboratorio de Evaluación**: Epoche & Espri S.L.U..

**Perfil de Protección**: No aplica.

**Nivel de Evaluación**: CC v 3.1 R5 EAL4 + ALC_FLR.1 + AVA_VAN.5.

**Fecha de término de la evaluación**: 01/03/2019.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 (aumentado con ALC_FLR.1 y AVA_VAN.5) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Epoche & Espri S.L.U. asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4 + ALC_FLR.1 + AVA_VAN.5, definidas por los Common Criteria v 3.1 (CC_P1, CC_P2, CC_p3) y el CEM

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto **SIAVAL SafeCert Manager, versión 3**, se propone la resolución estimatoria de la misma.

## *RESUMEN DEL TOE*

SIAVAL SafeCert Manager es un software de firma electrónica en servidor, que asegura el control exclusivo de las claves de firma por parte del firmante y genera tanto firma electrónica avanzada

(AdES) como firma electrónica cualificada o reconocida (QES), y construido para ser usado en un entorno operacional seguro como un sistema confiable de firma en servidor.

El conjunto de componentes que conforman el TOE posibilita la generación de firmas en servidor, de manera que una organización pueda fácilmente establecer un sistema de firma seguro, centralizando los procesos de firma de documentos de sus usuarios. Facilita la gestión del ciclo de vida de los certificados, la asociación entre los usuarios y sus claves, así como el cumplimiento del propósito de uso de dichas claves.

Se establece en todo momento el control exclusivo por parte de los usuarios de sus claves de firma, asegurando el vínculo entre usuario y clave/certificado y protegiendo las claves privadas de firma de forma tal que únicamente puedan ser utilizadas dentro del entorno operativo y por los propietarios legítimos de dichas claves.

La forma de interactuar con el TOE es mediante dos interfaces vía webservices, una de uso administrativo y otra de firma, a través de las cuales las aplicaciones invocarán a las operaciones del TOE. Estas interfaces aseguran el control de acceso mediante la autenticación, en todo momento, de los usuarios que acceden a dichos servicios y realizando la autorización en función de perfiles que determinarán el ámbito y uso de las operaciones.

La interfaz de uso administrativo se utilizará para el aprovisionamiento y activación de las cuentas de los usuarios firmantes en el sistema. De manera que, a través de esta interfaz, la organización establecerá y gestionará a los usuarios firmantes, así como sus claves y certificados activos en el sistema.

A la interfaz de firma se accederá desde aquellas aplicaciones de creación de firma de la organización que se integren con el sistema para posibilitar la firma de documentos. El acceso a estos servicios se accederá autenticando a las aplicaciones solicitantes de la firma, de manera que se establezca un canal seguro entre la aplicación de firma y el TOE. A través de este canal seguro, el usuario, en el momento de la firma, establecerá las credenciales de autenticación a su clave de firma a través de un sistema multicanal, proporcionando una clave secreta que únicamente él conoce, y un segundo factor de autenticación como puede ser una contraseña dinámica de un solo uso o una comprobación biométrica.

Los usuarios firmantes podrán tener asociadas varias claves con sus correspondientes certificados, de manera que podrán utilizar en cada aplicación de creación de firma la clave requerida en cada momento.

El TOE, mediante configuración, podrá establecer diferentes políticas sobre diferentes aspectos de seguridad:

1. Bloqueo/suspensión de las claves tras n fallos de intentos de autenticación en el momento de la firma o cambio de contraseña por parte del usuario firmante.

2. Activación del uso del certificado durante periodos de tiempo.

## *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 el componente adicional ALC_FLR.1 + AVA_VAN.5, según los CC v3.1 R5.

| **Clase** | **Familia/Componente** |
|---|---|
| ASE | INT.1<br>CCL.1<br>SPD.1<br>OBJ.2<br>ECD.1<br>REQ.2<br>TSS.1 |
| AGD | OPE.1<br>PRE.1 |
| ALC | CMC.4<br>CMS.4<br>DEL.1<br>DVS.1<br>LCD.1<br>TAT.1<br>FLR.1 (aumentado) |
| ADV | FSP.4<br>ARC.1<br>TDS.3<br>IMP.1 |
| ATE | COV.2<br>DPT.1<br>FUN.1<br>IND.2 |
| AVA | VAN.5 (aumentado) |

## *REQUISITOS FUNCIONALES DE SEGURIDAD*

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según los CC v3.1 R5.

| **Clase** | **Familia/Componente** |
|---|---|
| FAU | GEN.1 Operaciones del TOE<br>GEN.1 Operaciones de los usuarios firmantes<br>GEN.2 Identificación del usuario de la operación<br>SAR.1 Revisión de los datos de auditoría de operaciones del TOE<br>SAR.1 Revisión de los datos de auditoría de operaciones del usuario firmante<br>SAR.2 Acceso restringido a los datos de auditoría del TOE<br>SEL.1 selección de los datos de auditoría de operaciones del TOE<br>SEL.1 selección de los datos de auditoría de operaciones de los usuarios firmantes<br>STG.3 Archivado de datos de auditoría del TOE<br>SAA.1<br>ARP.1 |
| FCO | NRO.1 CSR Generación del certificado |
| FCS | COP.1 descifrado / cifrado simétrico de datos<br>COP.1 descifrado fichero configuración HMAC<br>COP.1 verificación fichero configuración HMAC<br>COP.1 cálculo / verificación HMAC<br>CKM.1 descifrado/cifrado simétrico de datos<br>CKM.3 clave protección fichero de configuración HMAC<br>CKM.3 almacén comunicación segura ProxySFDA<br>COP.2 generación de SCD/SVD (extendido)<br>COP.2 activación del SCD en firma/autenticación (extendido)<br>COP.2 cambio de contraseña (extendido) |
| FIA | UAU.2 |

| | |
|---|---|
| | UAU.5 Para los usuarios firmantes en las operaciones de firma y cambio de contraseña<br>UID.2<br>AFL.1 Usuarios firmantes en la operación de firma/cambio de contraseña |
| FDP | ACC.2 Acceso a los servicios web SFP<br>ACC.1 Operaciones de los usuarios firmantes SFP<br>ACF.1 Acceso a los servicios web SFP<br>ACF.1 Operaciones de los usuarios firmantes SFP<br>ETC.2 Exportación CSR<br>ITC.1 Histórico de contraseñas<br>ITC.1 Asociación de certificado<br>SDI.1<br>SDC.1 (extendido)<br>UDC.1 (extendido) |
| FPT | RPL.1 |
| FMT | MSA.1 ADMIN-OWNER<br>MSA.1 CREATE_KEY<br>MSA.1 CHANGE_PASSWORD_SERVICE<br>SMF.1<br>MTD.1 Consulta datos de auditoria |
| FTP | ITC.1 Aplicación de Registro<br>ITC.1 Aplicación de Creación de Firma<br>ITC.1 Base de datos<br>ITC.1 Componente ProxySFDA |

## IDENTIFICACIÓN

**Producto**: SIAVAL SafeCert Manager, versión 3.

**Declaración de Seguridad:** SIAVAL SafeCert – Declaración de Seguridad v3.0, Febrero 2019.

**Perfil de Protección**: No aplica.

**Nivel de Evaluación**: Common Criteria v3.1 R5, EAL4 + ALC_FLR.1 + AVA_VAN.5.

## POLÍTICA DE SEGURIDAD

El uso del producto SIAVAL SafeCert Manager, versión 3, 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 síntesis, se establece la necesidad de implementar políticas organizativas relativas a los siguientes aspectos.

- **P.Q-CERTIFICATE:** Certificado cualificado
- **P.Q-SIGNATURE:** Firmas electrónicas
- **P.REGISTRY_PROCESS:** Proceso de registro
- **P.ACCESS_CONTROL_SCA:** Control de acceso de las aplicaciones de creación de firma
- **P.CONFIGURATION_TOE:** Configuración del TOE
- **P.VALIDATION-HMAC:** Validación periódica de los HMAC generados en base de datos
- **P.SECURE-HSM:** Alto nivel de seguridad del HSM
- **P.ROL_ACCESS_EXCLUSIVE:** Perfiles de acceso excluyentes
- **P.ARCHIVE-DATA-AUDIT:** Archivado de datos de auditoría
- **P.BACKUP/RECOVERY-DATA-SYSTEM:** Backup/Recovery de los datos del sistema
- **P.SECURE-ALGORITHMS-SIGN:** Algoritmos seguros para la firma

## 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.

- **A.TRUSTED_TSP:** Trusted Service Provider confiable (TSP)

- **A.TRUSTED_SCA:** Aplicación de creación de firma de confianza (SCA)
- **A.SECURE_ENVIRONMENT:** Entorno seguro
- **A.MGMT_SEND-OTP&SFDA:** Gestión de sistemas para envío de OTPs y Gestores de SFDAs externos
- **A.MGMT_BBDD:** Gestión de BBDD de configuración
- **A.MGMT_HSM:** Gestión de HSM de la organización
- **A.CONTROL_SFDA_DATA&HARDWARE:** Control de los datos y/o hardware de acceso por SFDA del firmante
- **A. .TRUSTED_USERS:** Usuarios capacitados y de confianza

## *ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS*

Las siguientes amenazas no suponen un riesgo explotable para el producto SIAVAL SafeCert Manager, versión 3, 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 relacionan a continuación.

- **T.ACCESS_CONTROL:** Acceso no autorizado a los servicios del TOE
- **T. SIGNATURE-SUPPLANT_USER:** Uso ilegítimo de los datos de creación de firma (SCD)
- **T.DTBS-FORGERY:** Falsificación de los datos a firmar (DTBS o DTBSR)
- **T.SIGNATURE-FORGERY:** Falsificación de la firma digital
- **T.SIGNER_AUTHENTICATION-DIVULG:** Acceso a los datos de autenticación
- **T.HACK_MANINTHEMIDDLE:** Ataques de tipo “man in the middle”
- **T.SCD-DIVULG:** Divulgación de los datos de creación de firma (SCD)
- **T.MODIFY_USER_DATA:** Modificación no autorizada de los datos de trabajo de los usuarios
- **T.MODIFY_CONFIGURATION_DATA:** Modificación no autorizada de los datos de configuración del TOE

- **T.OTP-STOLEN:** El atacante obtiene una OTP durante la generación, almacenamiento o transferencia a un titular
- **T.MODIFY_AUDIT_DATA:** Modificación de los datos de auditoría
- **T. DATA_NOT_GENERATED_BY_TOE:** Datos no generados por el TOE

### *FUNCIONALIDAD DEL ENTORNO*

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

Se relacionan, a continuación, los objetivos que se deben cubrir por el entorno de uso del TOE.

**OE.RESTRICTED_ACCESS:** Acceso restringido. El TOE estará instalado en un servidor físico y en un servidor de aplicaciones ubicados en un entorno seguro y controlado por administradores de confianza los cuales serán los encargados de gestionar el acceso físico al TOE, tanto a sus ficheros de configuración como a los ficheros ejecutables del TOE. Así mismo, la base de datos utilizada por el TOE para almacenar los datos de configuración, datos de trabajo de usuario y datos de auditoría, deberá tener el control de acceso suficiente para evitar el acceso de agentes externos que pudieran realizar modificaciones que alteren el correcto funcionamiento del TOE.

**OE.SECURE_COMMUNICATIONS**: Comunicaciones seguras. Las comunicaciones que se establecen a los servicios del TOE serán siempre establecidos a través de mecanismos seguros. La conexión desde los clientes al TOE se realizará a través de una conexión http sobre SSL/TLS; de esta manera las aplicaciones clientes se aseguran que se conectan a un servidor seguro, puesto que deberán confiar en el certificado correspondiente del servidor. Así mismo, las comunicaciones que se realicen desde el TOE a los diferentes componentes necesarios para su funcionamiento, como son, BBDD, Pasarela de envío de OTPs y gestores de SFDA externos, se realizarán también bajo una comunicación segura mediante protocolo SSL/TLS y la comunicación al HSM se realizará sin que se produzca comunicación exterior al ser este un módulo PCI instalado en la misma máquina que el TOE y acceder a él mediante los mecanismos PKCS#11 sin producirse comunicación por red.

**OE.SVD-VALIDATION:** Autenticidad de la SVD. El TSP (Trusted Service Provider) comprobará la validez de la SVD utilizando la prueba de posesión exportada desde el TOE (CSR o firma de la clave pública) antes de suministrar un certificado apropiado para esa SVD.

**OE.SCD-SVD-UNICITY:** Unicidad de los datos de creación de firma. El HSM garantizará la calidad criptográfica de un par SCD/SVD que se crea como adecuado para la firma electrónica. El SCD utilizado para la creación de firma prácticamente puede darse sólo una vez y no puede ser reconstruido a partir de la SVD. En ese contexto, lo de que 'prácticamente puede darse sólo una vez' significa que la probabilidad de que haya SCDs iguales es insignificante.

**OE.CERTIFICATE-GENERATION:** Generación de certificados. La Autoridad de Registro solicitará al TSP, que genere unos certificados de acuerdo a lo que se indica en Directiva: Art.2: 9, Art.2: 10, Anexo I y eIDAS: Art.3: 14, Art.3: 15, Anexo I y que incluyan, entre ellos: el nombre del firmante, la SVD que coincida con el SCD generada a través del TOE y controlado por el firmante, la firma del TSP.

**OE.AUTHENTICATION_DATA-PROTECTION**: Protección de los datos de autenticación introducidos por el usuario. El sistema que solicita los datos al usuario asegurará la confidencialidad e integridad de los mismos hasta que sean enviados al TOE. Por ejemplo: la contraseña estática del usuario, así como la OTP se mantendrán confidenciales y no se revelarán a terceros.

**OE.DTBS-CORRECT**: La SCA envía al sistema los DTBS correctos. El firmante utilizará un Sistema de Creación de Firma confiable que:

- genera el DTBS/R de los datos que ha sido presentado como DTBS y que el firmante tiene la intención de firmar en una forma que sea apropiada para el TOE.
- envía el DTBS/R al TOE utilizando un canal que asegura la confidencialidad y la integridad DTBS/R.
- se aplica la firma producida por el TOE a los datos, obteniendo la firma final del usuario.

**OE.TOE-CONFIGURATION**: Configuración TOE de acuerdo a las recomendaciones suministradas. Se proporcionarán todos los manuales suficientes para que el sistema se configure de manera completa y segura.

**OE.SEND_OTP-MGMT:** Administración y configuración segura del sistema de envío de OTPs y SFDAs externos. La gestión y configuración del sistema de envío de OTPs y los gestores de SFDAs externos al TOE se realizará de manera segura y solamente por las personas autorizadas.

**OE.SIGNER-ACTIVATION_ACCOUNT**: Activación de la cuenta por el firmante. La Autoridad de Registro comprobará la identidad del firmante de manera segura y solicitará la activación de la cuenta del usuario en el sistema. La RA se encargará de solicitar al firmante de manera segura que establezca la contraseña estática que protegerá su SCD. La RA asegurará la integridad y confidencialidad de dicha contraseña hasta su envío al TOE.

**OE.SECURE-BACKUPS/RECOVERY-DATA-SYSTEM**: Backup y Recovery de los datos del sistema. Se gestionarán y mantendrán los backups de los sistemas externos al TOE de manera segura, asegurando la confidencialidad e integridad de los mismos. Se determinará periódicamente la realización de un backup de todos los datos y elementos del Sistema que se necesiten respaldar para que, tras un fallo del sistema, pueda restaurarse a un estado operativo igual al que existía previo al fallo. Mediante la guía operativa del producto se determinará cuáles de todos los datos son necesarios realizar respaldo, por ejemplo:

- Base de datos
- Claves de entorno: claves y ficheros de configuración operativas
- Configuración de entorno: configuración de conexión a base de datos
- Configuración de acceso al HSM y clave maestra que reside en el HSM

Igualmente se determinará el procedimiento para realizar un recovery del sistema a partir del backup realizado. Este backup se ciñe al Reglamento (UE) Nº 910/2014 (eIDAS) Anexo II Art. 4 que establece que se podrán duplicar los datos de creación de firma para el propósito de realizar una copia de seguridad con el mismo nivel de protección que el original.

**OE.SECURE-HSM**: Alto nivel de seguridad del HSM utilizado: El HSM utilizado por el sistema proporcionará un alto nivel de seguridad, por ejemplo:

- Cumpla los requisitos del EN 419211;
- O cumpla los requisitos identificados en CEN/TS 419221-2, CEN/TS 419221-3 o CEN/TS 419221-4;
- O sea, un sistema confiable que sea evaluado como EAL 4 o superior en cumplimiento con la ISO/IEC 15408, o con un criterio de seguridad equivalente o superior;
- O cumpla los requisitos identificados en ISO/IEC 19790:2006, nivel 3 o superior.
- O cumpla FIPS PUB 140-2, nivel 3.

**OE.VALIDATION-HMAC:** Validación periódica de los HMAC generados en base de datos: Se establecerá una validación periódica de la tarea de validación de HMAC para detectar posibles modificaciones no autorizadas en los datos de trabajo del usuario y/o configuración del TOE.

**OE.DOCUMENTATION-SIGNER:** Documentación para la formación de usuarios firmantes. Se dispondrá de manuales y procedimientos de uso para que los usuarios firmantes utilicen el entorno operativo de manera segura, sepan proceder ante situaciones como pérdida/cambio del móvil a través del cual recibirán las contraseñas dinámicas y mantengan su contraseña estática de manera que no pueda ser conocida por terceros.

**OE.ROL_ACCESS_EXCLUSIVE:** Perfiles de acceso excluyentes. Para el correcto uso del control de acceso y que los usuarios no puedan realizar todas las operaciones sobre el TOE y sobre el entorno operacional, se determina que:

- Los usuarios con el perfil "Security Officer" no podrán tener al mismo tiempo el perfil "System Auditor"
- Los usuarios con el perfil "System Administrator" y/o "System Operator" no podrán tener al mismo tiempo el perfil de "System Auditor" y/o "Security Officer".

**OE.ARCHIVE_AUDIT_DATA**: Archivado periódico de los datos de auditoría. Se determinará periódicamente la ejecución del proceso de archivado que proporciona el TOE que genera el archivado de los datos de auditoría desde la base de datos a un fichero que se almacenará de forma segura.

**OE.SECURE-ALGORITHMS-SIGN:** Utilización de algoritmos seguros. Se especificarán los algoritmos que cada uno de los elementos del sistema puedan utilizar para cumplir las recomendaciones de la especificación técnica ETSI/TS 119 312. Las aplicaciones de creación de firma utilizarán algoritmos de hashing de SHA-256 o superior. Y la aplicación de registro solicitará generación de claves asimétricas de firma con algoritmo de firma RSA con un tamaño de clave no inferior a 2048 bits.

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: Que invoca al HSM para realizar las operaciones criptográficas de protección de las claves y firma electrónica.

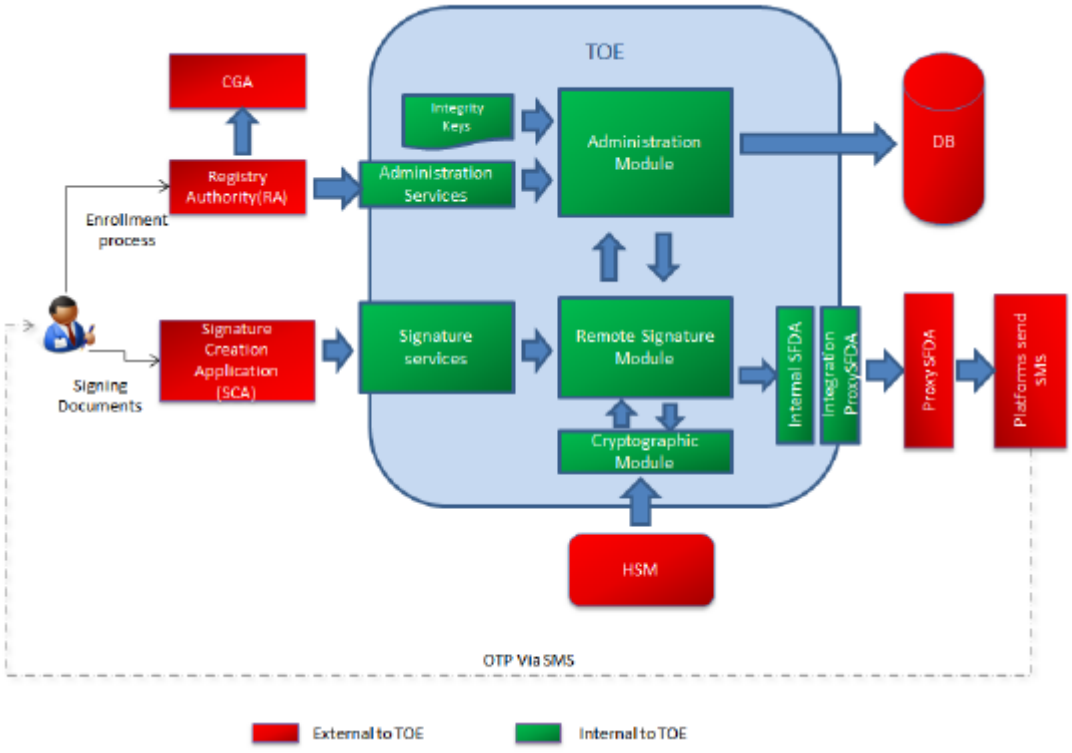
- Servicios web de administración: Que actúan sobre el módulo de administración.

- Módulo de gestión de Segundo Factor de Autenticación (interno).

- 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

## 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 – Declaración de Seguridad v3.0, febrero 2019

Listado de manuales del TOE:

- SIAVAL_SafeCert 3 - Manual_de_Administración v1.0
- SIAVAL_SafeCert 3 - Manual_de_Instalación v1.0
- SIAVAL_SafeCert 3 - Manual_de_Integración v1.0
- SIAVAL SafeCert 3 - Manual de operaciones v1.0
- SIAVAL SafeCert 3 - Manual de configuración segura v1.0
- SIAVAL_SafeCert 3 - Manual_de_Integración_ProxySFDA v1.0
- SIAVAL_SafeCert 3 - Manual_de_Composición v1.0
- Soporte Técnico - Procedimiento Resolución de Incidencias v2.0

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.

## 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 han 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 en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido todas las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más relevantes.

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, versión 3 es necesario disponer de los siguientes componentes software:

- Sistema operativo en el servidor del TOE: CentOS release 6.3 de 64 bits.

- Sistema operativo en el servidor de los servicios externos al TOE: Windows de 64 bits.
- Servidor de aplicaciones: Apache Tomcat 7.0.90.
- Base de Datos: PostgreSQL 9.6.10
- Cliente HSM: Luna PCI 5.2.1
- Java Runtime Enviroment en servidor del TOE: JDK 1.8.0.181 con JCE Unlimited Strength.
- Consola web de administración: SIAVAL SafeCert Console v3
- Componente ProxySFDA: SIAVAL SafeCert ProxySFDA 3 con plataforma de envío de OTPs

En cuanto a los componentes hardware:

- Máquina servidor donde reside el TOE: Dell PowerEdge con Intel(R) Xeon(R).
- HSM: Luna PCI-E Cryptographic Module.
- Máquina servicios externos al TOE: PC o servidor genérico.

## RESULTADOS DE LA EVALUACIÓN

El producto SIAVAL SafeCert Manager, versión 3 ha sido evaluado en base a la Declaración de Seguridad SIAVAL SafeCert – Declaración de Seguridad v3.0, Febrero 2019.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 + ALC_FLR.1 + AVA_VAN.5 presentan el veredicto de "PASA". Por consiguiente, el laboratorio Epoche & Espri S.L.U. asigna el **VEREDICTO de "PASA"** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4 + ALC_FLR.1 + AVA_VAN.5, definidas por los CC v3.1 R5 y el CEM.

## 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 producto es una plataforma de firma en remoto en la que los usuarios disponen de certificados protegidos por el sistema. El acceso y uso de estos certificados para firma y autenticación se controla mediante la información/credenciales proporcionados en el momento del registro y mediante un segundo factor de autenticación que hace uso de OTPs (One Time Passwords).

Por otro lado, el appliance en el que se despliega el TOE es proporcionado ya configurado e instalado por el fabricante. En este sentido, durante las pruebas se ha verificado la existencia de varios elementos instalados en el appliance que pueden llegar a dar acceso al producto y a los datos de la TSF. Se recomienda controlar y securizar la configuración del appliance y de las aplicaciones

en él instaladas, pues un fallo en un elemento del entorno puede desencadenar en una vulnerabilidad grave en el producto.

El producto ha presentado una única configuración evaluada, si bien permite operar con configuraciones diferentes ofreciendo propiedades y mecanismos de seguridad diferentes. Se recomienda poner especial énfasis en la verificación de la configuración aplicada en la puesta en producción en cliente para chequear que todos estos mecanismos de seguridad se encuentran habilitados para el uso del TOE.

## RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto SIAVAL SafeCert Manager, versión 3, 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, 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.

# DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

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

- SIAVAL SafeCert – Declaración de Seguridad v3.0, Febrero 2019

# RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

## *European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)*

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

## *International Recognition of CC – Certificates (CCRA)*

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.