REF: 2014-56-INF-1500 v1	Creado: CERT10
Difusión: Público	Revisado: CALIDAD
Fecha: 16.07.2015	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2014-56 SIAVAL SafeCert v2.4

Datos del solicitante: A82733262 Sistemas Informáticos Abiertos

Referencias:

[EXT-2654] Solicitud de Certificación de SIAVAL SafeCert v2.4

[EXT-2772] Informe Técnico de Evaluación de SIAVAL SafeCert v2.4

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto SIAVAL SafeCert v2.4.02-20150611-1657, según la solicitud de referencia [EXT-2654], de fecha 15/12/2014, evaluado por el laboratorio Epoche & Espri S.L.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-2772], recibido el pasado 19/06/2015.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

ÍNDICE

RESUMEN **3**
RESUMEN DEL TOE 3
REQUISITOS DE GARANTÍA DE SEGURIDAD 5
REQUISITOS FUNCIONALES DE SEGURIDAD 6
IDENTIFICACIÓN **8**
POLÍTICA DE SEGURIDAD **8**
HIPÓTESIS Y ENTORNO DE USO **8**
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS 8
FUNCIONALIDAD DEL ENTORNO 11
ARQUITECTURA **15**
ARQUITECTURA LÓGICA 15
ARQUITECTURA FÍSICA 16
DOCUMENTOS **17**
PRUEBAS DEL PRODUCTO **17**
CONFIGURACIÓN EVALUADA **18**
RESULTADOS DE LA EVALUACIÓN **19**
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES **20**
RECOMENDACIONES DEL CERTIFICADOR **21**
GLOSARIO DE TÉRMINOS **21**
BIBLIOGRAFÍA **21**
DECLARACIÓN DE SEGURIDAD **21**

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto **SIAVAL SafeCert Manager v 2.4.02-20150611-1657**.

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.

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 las claves, su asociación entre los usuarios, 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 claves, protegiendo la clave privada de firma de forma tal que únicamente pueda ser utilizada dentro del entorno operativo y por su propietario legítimo.

Fabricante: SIA Sistemas Informáticos Abiertos S.A.
Patrocinador: SIA Sistemas Informáticos Abiertos S.A.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: EPOCHE & ESPRI

Perfil de Protección: No aplica

Nivel de Evaluación: CC v 3.1 R4 EAL4 + ALC_FLR.1 + AVA_VAN.5

Fecha de término de la evaluación: 19/07/2015

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 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 la Metodología de Evaluación [CEM]

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto **SIAVAL SafeCert Manager v 2.4.02-20150611-1657**, 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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 las claves, su asociación entre los usuarios, 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 claves, protegiendo la clave privada de firma de forma tal que únicamente pueda ser utilizada dentro del entorno operativo y por su propietario legítimo.

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 WebService vía SOAP 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 activas en el sistema.

A la interfaz de firma WebService vía SOAP y mediante mensajes binarios Hessian, 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 una contraseña dinámica de un solo uso que se le enviará a su teléfono móvil vía SMS.

Los usuarios firmantes podrán tener asociadas varias claves, 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:

- 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.

- Activación del uso de las claves durante periodos de tiempo.

Características principales de seguridad del TOE

Las características de seguridad fundamentales del TOE se resumen en:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- Control de Acceso: Se establece control de acceso para todas las operaciones realizadas en el TOE de manera que solamente los usuarios autorizados puedan realizar las operaciones para las que tienen permisos.
- Protección de las claves de firma: Se asegura en todo momento la protección de las claves de firma de los firmantes, de manera que solamente puedan ser utilizadas dentro del entorno operativo del TOE y no puedan ser divulgadas para su uso ilegítimo.
- Control Exclusivo de la clave de firma: La clave de firma se asocia al firmante de manera que éste tenga el control exclusivo para su activación en el momento de la firma.
- Firma segura: Se asegura todo el ciclo del proceso de firma, desde el momento en que desde la aplicación de creación de firma se solicita al TOE una firma, tanto en la transmisión de los datos a firmar al TOE, como en la generación de la firma, así como en la devolución de la firma a la aplicación. Así mismo, la firma generada tiene la fortaleza necesaria para que pueda verificarse su integridad.
- Comprobación de la configuración: Se asegurará, en todo momento, el acceso a la configuración que se encuentra en la base de datos, verificando que de los datos configurados hayan sido generados por el TOE.
- Autenticación multicanal: Se efectúa una autenticación multicanal con secreto estático y contraseña dinámica (OTP) mediante envío de SMS al usuario en la operación de firma, asegurando en todo momento la identidad del firmante.
- Datos de auditoría: Se registran datos de auditoría de todas las operaciones realizadas por los usuarios firmantes en el uso de sus claves de firma.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, según [CC_P3].

Clase	Familia/Componente
ASE	INT.1 CCL.1 SPD.1 OBJ.2 ECD.1 REQ.2 TSS.1
AGD	OPE.1 PRE.1
ALC	CMC.4

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

	CMS.4 DEL.1 DVS.1 LCD.1 TAT.1 FLR.1 (aumentado)
ADV	FSP.4 ARC.1 TDS.3 IMP.1
ATE	COV.2 DPT.1 FUN.1 IND.2
AVA	VAN.5 (aumentado)

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según [CC_P2].

Clase	**Familia/Componente**
FAU	GEN.1 Operaciones del TOE GEN.1 Operaciones de los usuarios firmantes GEN.2 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 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 SAA.1 ARP.1
FCO	NRO.1
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 COP.1 Firma petición envío plataforma SMS COP.1 Verificación firma de respuesta plataforma SMS COP.2 Activación del SCD en firma COP.2 Cambio de contraseña

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

	COP.2 Generación de SCD/SVD CKM.1 CKM.3 Clave protección fichero de configuración HMAC CKM.3 Almacén clave de firma/verificación plataforma de envío de SMS
FIA	UAU.2 UAU.5 UID.1 AFL.1
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 ITC.1 Histórico de contraseñas ITC.1 Asociación de certificado SDI.1 SDC.1 UDC.1
FPT	RPL.1
FMT	MSA.1 ADMIN-OWNER MSA.1 CREATE_KEY MSA.1 CHANGE_PASSWORD_SERVICE MTD.1 SMF.1
FTP	ITC.1 Aplicación de Registro ITC.1 Aplicación de Creación de Firma ITC.1 Base de datos ITC.1 Plataforma envío SMS

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

IDENTIFICACIÓN

Producto: SIAVAL SafeCert Manager, versión 2.4.02-20150611-1657

Declaración de Seguridad: SIAVAL SafeCert – Declaración de Seguridad v 1.3, Junio 2015

Perfil de Protección: no aplica

Nivel de Evaluación: Common criteria v 3.1 R4, EAL4 + ALC_FLR.1 + AVA_VAN.5

POLÍTICA DE SEGURIDAD

En la declaración de seguridad se definen las siguientes políticas organizativas:

- P.Q-CERTIFICATE: Certificado cualificado
- P.Q-SIGNATURE: Firmas electrónicas cualificadas
- 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

En la declaración de seguridad se definen las siguientes hipótesis de entorno:

- 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: Gestión de sistemas para envío de OTPs
- A.MGMT_BBDD: Gestión de BBDD de configuración
- A.MGMT_HSM: Gestión de HSM de la organización
- A.CONTROL_TLF_MOVILE: Control del teléfono móvil del firmante
- A.TRUSTED_USERS: Usuarios capacitados y de confianza

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

En la declaración de seguridad se definen las siguientes amenazas:

- T.ACCESS_CONTROL: Acceso no autorizado a los servicios del TOE

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- 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

Se declaran cubiertas de manera combinada por el TOE y el entorno conforme a las siguientes tablas de cobertura:

A) Tabla de mapeo de amenazas cubiertas por el TOE

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

AMENAZAS / OBJETIVOS DE SEGURIDAD	T.ACCESS_CONTROL	T. SIGNATURE-SUPPLANT_USER	T.DTBS-FORGERY	T.SIGNATURE-FORGERY	T.SIGNER_AUTHENTICATION-DIVULG	T.SCD-DIVULG	T.HACK_MANINTHEMIDDLE	T.MODIFY_USER_DATA	T.MODIFY_CONFIGURATION_DATA	T.OTP-STOLEN	T.MODIFY_AUDIT_DATA	T.DATA_NOT_GENERATED_BY_TOE
O.AUTHENTICATION_USER	X											
O.ACCESS_CONTROL	X							X	X		X	
O.CONFIDENTIAL_PRIVATE_KEY						X						
O.SIGNER-SOLECONTROL		X				X						
O.SCD_SVD-CORRESPONDENCE		X										
O.SIGNATURE-SECURE				X								
O.SCD-ANTIREPLAY		X										
O.CONFIGURATION-INTEGRITY					X		X					X
O.USER-DATA-INTEGRITY					X					X		X
O.AUDIT-INTEGRITY												X
O.VERIFICATION-SERVER-SMS					X		X			X		
O.PROTECT-HMAC-KEY												X
O.CIPHER-PASS										X		X
O.DETECT-FUNCTION-SECURITY-SYSTEM												X

B) Tabla de mapeo de amenazas cubiertas por el entorno

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

AMENAZAS / OBJETIVOS DE SEGURIDAD	T.ACCESS_CONTROL	T. SIGNATURE-SUPPLANT_USER	T.DTBS-FORGERY	T.SIGNATURE-FORGERY	T.SIGNER_AUTHENTICATION-DIVULG	T.SCD-DIVULG	T.HACK_MANINTHEMIDDLE	T.MODIFY_USER_DATA	T.MODIFY_CONFIGURATION_DATA	T.OTP-STOLEN	T.MODIFY_AUDIT_DATA	T.DATA_NOT_GENERATED_BY_TOE
OE.RESTRICTED_ACCESS								X	X		X	
OE.SECURE_COMMUNICATIONS			X	X	X		X	X	X	X	X	
OE.SVD-VALIDATION				X								
OE.SCD-SVD-UNICITY				X								
OE.AUTHENTICATION_DATA-PROTECTION		X								X		
OE.DTBS-CORRECT			X									
OE.TOE-CONFIGURATION					X		X			X		
OE.SEND_OTP-MGMT					X					X		
OE.SIGNER-ACTIVATION_ACCOUNT		X										
OE.SECURE-BACKUPS/RECOVERY-DATA-SYSTEM												
OE.SECURE-HSM				X								
OE.VALIDATION-HMAC												X
OE.CERTIFICATE-GENERATION												
OE.DOCUMENTATION-SIGNER					X					X		
OE.ARCHIVE_AUDIT_DATA												
OE.ROL_ACCESS_EXCLUSIVE	X											
OE.SECURE-ALGORITHMS-SIGN				X								

FUNCIONALIDAD DEL ENTORNO

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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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 SMS, se realizarán también bajo una comunicación segura mediante protocolo SSL. 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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

de activación del usuario titular, 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
La gestión y configuración del sistema de envío de OTPs 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 ejecución 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.

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 CEN/TS EN 419 211;
- O cumpla los requisitos identificados en CEN/TS 419 221-2, CEN/TS 419 221-3 o CEN/TS 419 221-4;

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- 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 datos no generados por el TOE en los datos de trabajo del usuario, auditoría 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
Se determinará que 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. 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 o de los requisitos de seguridad del TOE se encuentran en la correspondiente Declaración de Seguridad.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

ARQUITECTURA

ARQUITECTURA LÓGICA

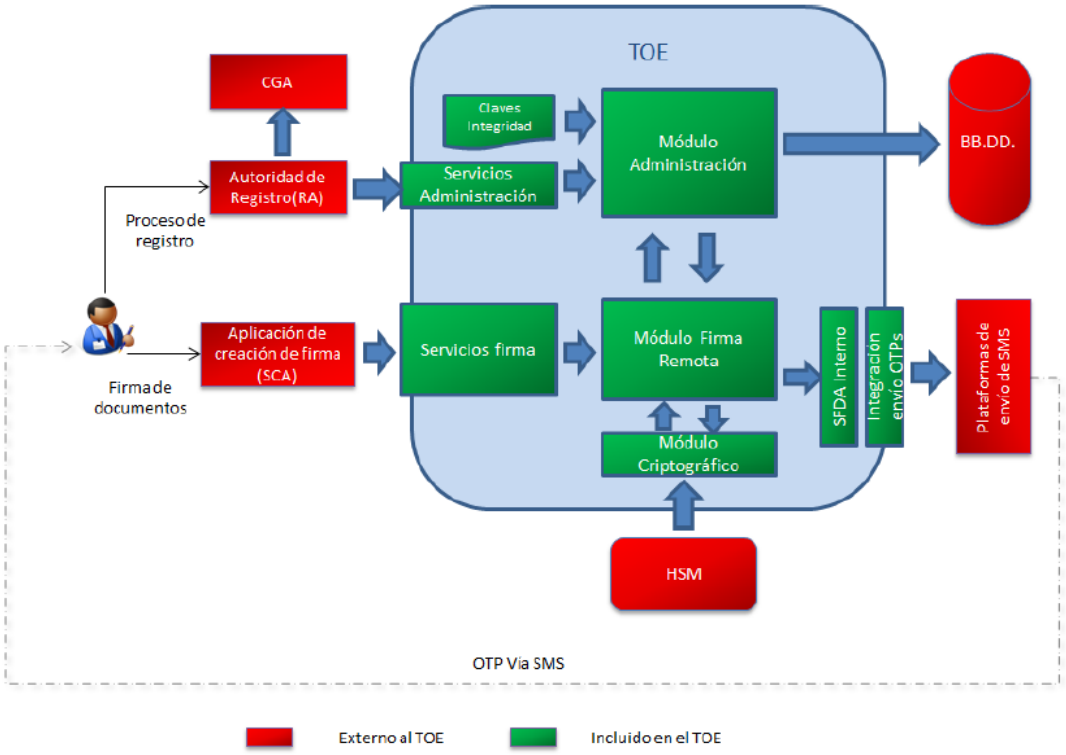
El TOE es un subconjunto de los componentes que conforman la solución global aportada por el producto.

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 envío de OTPs a los titulares.
- Componentes de integración con Plataformas de Segundo Factor de Autenticación.
- 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:

C/ Argentona nº 20
Email: organismo.certificacion@cni.es



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 2.4.02 20150611-1657*** 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.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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 v 1.3, Junio 2015

Listado de manuales del TOE:

- SIAVAL_SafeCert v2.4.02-Manual_de_Instalación v3.0
- SIAVAL_SafeCert v2.4.02-Manual_de_Integración v3.0
- SIAVAL SafeCert v2.4.02-Manual de operaciones v1.1
- SIAVAL SafeCert v2.4.02-Manual de configuración segura v1.1
- Soporte Técnico - Procedimiento Resolución de Incidencias v1.2

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_2.xsd, XMLExtra_1.xsd, MonitorRSS_1.xsd, MonitorRSS_Result_1.xsd, Commons_Types_2.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"**, 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 evaluador ha considerado la totalidad de casos de prueba del fabricante y una estrategia adecuada al tipo del TOE para el desarrollo del plan de pruebas independiente. La documentación entregada describe el comportamiento de las TSFIs, y esta información ha sido aplicada por el evaluador para desarrollar este

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

plan de pruebas. El evaluador, además, ha considerado toda la información proveniente de los requisitos funcionales de seguridad descritos en la declaración de seguridad, así como toda la información contenida en la especificación funcional y documentos de diseño.

El plan de pruebas del evaluador tiene en cuenta:

1. Pruebas de todos los SFRs definidos a través de los TSFIs del TOE.
2. Incremento de la cobertura de los casos de prueba para cada interfaz, variando los parámetros de entrada en búsqueda de parámetros críticos o que provoquen un mal comportamiento.
3. Selección de los TSFIs/subsistemas que son testeados en función de:
   - Importancia de los TSFIs y los subsistemas.
   - Tipos de TSFIs y los subsistemas.
   - Número de TSFIs y los subsistemas.

Para la selección de los casos de pruebas, se han utilizado los siguientes criterios: búsqueda de parámetros críticos en la interacción con las TSFIs y los subsistemas, prueba de los requisitos ejercitados por las TSFIs, realización de pruebas exhaustivas en las TSFIs de mayor importancia, y en aquellas que son sospechosas de mal comportamiento ante determinados parámetros de entrada.

También se han realizado casos de prueba con parámetros de las TSFIs y de los subsistemas que pudieran tener especial relevancia en el mantenimiento de la seguridad del TOE.

El plan de pruebas independiente desarrollado por el evaluador está orientado a probar todos los SFRs, y la funcionalidad de cada SFR incluido en la declaración de seguridad ha sido considerada. Para la realización de todos los casos de prueba se han ejercitado interfaces externos que permiten probar adecuadamente los SFRs definidos.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados. No se ha presentado ninguna desviación.

CONFIGURACIÓN EVALUADA

Aunque **SIAVAL SafeCert Manager v 2.4.02-20150611-1657** soporta otras plataformas, las pruebas para llevar a cabo la evaluación del TOE se han realizado sobre la siguiente plataforma:

- Hardware:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- Máquina servidor donde reside el TOE: Dell PowerEdge R320 4 CPU's Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz.
- HSM: Luna PCI (PED) Key Export With Cloning Mode K6Model.
- Máquina servicios externos al TOE: PC genérico con procesador Intel 64 bits.

- 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: CentOS release 6.3 de 64 bits.
  - Servidor de aplicaciones: Apache Tomcat 7.0.47.
  - Base de Datos: PostgreSQL 9.3.
  - Cliente HSM: Luna PCI 5.0.
  - Java Runtime Enviroment en servidor del TOE: JDK 1.7.0.45 con JCE Unlimited Strength.
  - Consola web de administración: SIAVAL/SafeCert Console v2.4.02 20150611-1657.
  - Aplicación de creación de firma que invoca a los servicios de firma del TOE (SCA).
  - Aplicación de registro (RA).
  - Aplicación de creación de certificados (CGA).
  - Plataforma de envío de SMS simulada para el envío de OTPs

RESULTADOS DE LA EVALUACIÓN

El producto **SIAVAL SafeCert Manager v 2.4.02-20150611-1657** ha sido evaluado en base a la **SIAVAL SafeCert – Declaración de Seguridad v 1.3, Junio 2015**.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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 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 criterios de evaluación Common Criteria [CC_P3] y la Metodología de Evaluación [CEM].

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

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).

Estos OTPs son enviados a los usuarios/titulares de los certificados mediante SMSs. Esto implica que los OTPs son enviados haciendo uso de la infraestructura de envío de SMSs la cual se sabe insegura.

Durante la evaluación, el envío de los SMSs ha sido simulado, haciendo uso de un elemento que registraba en un fichero local las OTPs generadas por el TOE para su envío. En este sentido, la seguridad relativa al envío de los SMSs ha quedado fuera del ámbito de la evaluación, pero no deja de ser un elemento muy importante en la seguridad del sistema. Así pues, se considera de vital importancia controlar como se implementa el envío y recepción de los SMSs.

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. A este respecto, el producto presenta la opción de anular la utilización del segundo factor de autenticación (SFDA - OTP) e incluso de obviar el PIN de acceso a la clave privada de los titulares. 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto **SIAVAL SafeCert Manager v 2.4.02-20150611-1657**, 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, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.

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 – Declaración de Seguridad v 1.3, Junio 2015

C/ Argentona nº 20
Email: organismo.certificacion@cni.es