REF: 2012-10-INF-1315 v1	Creado: CERT8
Difusión: Expediente	Revisado: CALIDAD
Fecha: 31.03.2014	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2012-10 MFED

Datos del solicitante: W00014596A RCI Banque, S.A., Sucursal en España

Referencias:

[EXT-1703] Solicitud de Certificación de MFED

[EXT-2425] Informe Técnico de Evaluación de MFED

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto MFED, según la solicitud de referencia [EXT-1703], de fecha 01/06/2012, evaluado por el laboratorio Epoche & Espri S.L.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-2425], recibido el pasado 24/02/2014.

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

ÍNDICE

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

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto Módulo de Firma Electrónica de Documentos, versión 2.18.

El TOE es un módulo diseñado para llevar a cabo la gestión y firma de documentos en formato PDF generados por la Alianza Renault-Nissan, tales como contratos de financiación con RCI Banque realizados en concesionarios.

Fabricante: RCI Banque S.A. Sucursal España.

Patrocinador: RCI Banque S.A. Sucursal España.

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

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

Perfil de Protección: Ninguno.

Nivel de Evaluación: Common Criteria v3.1 r3.

CEM v3.1 r3.

EAL1+ (ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2).

Fecha de término de la evaluación: 24/02/2014.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 (ampliado con ASE_SPD.1, ASE_OBJ.2 y ASE_REQ.2) 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 EAL1 (ampliado con ASE_SPD.1, ASE_OBJ.2 y ASE_REQ.2), definidas por los Common Criteria v3.1 r3 ([CC_P1], [CC_P2] y [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 Módulo de Firma Electrónica de Documentos v2.18, se propone la resolución estimatoria de la misma.

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

RESUMEN DEL TOE

Se trata de un módulo que permite la firma de contratos de financiación, prestaciones y servicios, u otros tipos de documentos utilizados en la actividad de RCI y empresas de la Alianza Renault-Nissan.

El TOE hace uso de un dispositivo de captura de firmas (tableta WACOM 520U) para capturar las firmas de los intervinientes. Esta captura de firmas se realiza con el fin de llevar a cabo un posterior uso de las mismas para adjuntarlas al correspondiente documento PDF.

El TOE realiza la gestión de la comunicación entre las partes cliente y el componente servidor tanto para enviar documentos a firmar, como para recuperar documentos previamente firmados. El procedimiento de firma se gestiona en el componente servidor, e incluye tanto el firmado de los intervinientes sobre el documento a firmar, como la inclusión de un sello de tiempo proveniente de una TSA, y la firma digital de dicho documento, sus firmas y el sello de tiempo, por parte de la plataforma de firmas ASF.

La plataforma de firmas tiene como objetivo confirmar la validez del certificado electrónico (no revocación) con el que se va a firmar el documento, la consulta a la TSA para recoger el sello de tiempo y la custodia final de los documentos firmados.

El TOE permite que la firma de documentos se realice en diferentes instantes, de forma que se puedan ir incorporando nuevas firmas a lo largo del tiempo hasta el cierre del proceso completo de firma, que culmina con la adición del sello de tiempo y la firma del emisor del contrato por parte de ASF.

En el proceso de firma, se pueden pasar varios documentos a firmar, aunque cada uno será firmado por separado.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, más las requeridas por los componentes adicionales ASE_SPD.1, ASE_OBJ.2 y ASE_REQ.2 según [CC_P3].

Clase	Familia/Componente
Security Target evaluation	ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_REQ.3 ASE_SPD.1 ASE_TSS.1
Guidance documents	AGD_OPE.1 AGD_PRE.1

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

Life-cycle support	ALC_CMC.1 ALC_CMS.1
Development	ADV_FSP.1
Tests	ATE_IND.1
Vulnerability assessment	AVA_VAN.1

REQUISITOS FUNCIONALES DE SEGURIDAD

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

Clase	Familia/Componente	
FAU	GEN.1	Audit data generation
FDP	POM.1 ITI.1 RIP.1	Process order management Intra-TOE trusted information Subset residual information protection
FMT	SMF.1	Specification of management functions

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

IDENTIFICACIÓN

Producto: Módulo de Firma Electrónica de Documentos versión 2.18.

Declaración de Seguridad: Declaración de Seguridad para Módulo de Firma Electrónica de Documentos de RCI Banque España, versión 1.5, Noviembre 2013.

Perfil de Protección: ninguno.

Nivel de Evaluación: Common Criteria v3.1 r3

CEM v3.1 r3

EAL1+ (ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2).

POLÍTICA DE SEGURIDAD

El uso del producto Módulo de Firma Electrónica de Documentos v2.18, 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:

Política 01: OSP.Auditoría

El TOE deberá generar auditoría para las acciones que intervienen en los procesos completos de firma.

Política 02: OSP. ProcesoFirma

Los documentos firmados por todos los intervinientes se deberán enviar a una entidad externa donde se sellarán con una marca de tiempo y se firmarán digitalmente.

Política 03: OSP.Gestión

El TOE deberá implementar funcionalidad de gestión relacionada con los procesos completos de 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.

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

Hipótesis 01: A.Configuración

Tanto los puestos clientes como los servidores centrales donde se ejecuta el TOE (servidores Web, de aplicaciones, LDAP y base de datos), y los otros sistemas con los que interactúa (@baco, Plataforma ASF, Archivo Digital) están bien configurados, y no son una fuente de ataque

Hipótesis 02: A.Físico

Todo el sistema global, a excepción de los puestos clientes y los dispositivos de captura de firma, están en un CPD securizado.

Hipótesis 03: A.Personal

Los administradores de los sistemas centrales, tanto de RCI como de Renault, son de confianza.

Hipótesis 04: A.Autenticación

El entorno operacional del TOE es el encargado de autenticar al usuario del puesto cliente con que se opera.

Hipótesis 05: A.Integridad

La integridad de los documentos y sus firmas es mantenida por el entorno operacional.

Hipótesis 06: A.PKI

La custodia de la PKI utilizada para la generación de certificados firmados por la CA del grupo Renault está gestionada por personal confiable, y sólo se generarán certificados si su uso final es conocido y aceptado.

Hipótesis 07: A.DMZ

La parte servidor del TOE y su entorno está desplegado en una red DMZ segura en la que todas las comunicaciones con Internet son manejadas por un reverse proxy y las comunicaciones con la Intranet se autorizan a nivel IP:Puerto. Se utilizan servidores intermedios para las comunicaciones de tal manera que éstas nunca son directas. Toda comunicación entre elementos dentro de la DMZ se considera segura. Tanto la configuración de la red como la asignación y utilización de los pares IP:puerto en los nodos conectados a la misma es responsabilidad del grupo de seguridad de Renault y no constituye una fuente de ataque.

Hipótesis 08: A.Generación

El entorno operacional del TOE es el encargado de generar los documentos a firmar y asegurar su envío de forma única al TOE para cada proceso completo de firma

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto Módulo de Firma Electrónica de Documentos v2.18, aunque los agentes que realicen

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

ataques tengan potencial de ataque correspondiente a *Basic* de EAL1, 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.

Amenaza 01: T.Acceso

Un usuario sin autenticar logra acceso a la red donde está desplegado el TOE y obtiene información de documentos, firmas y descriptores de firmas.

Amenaza 02: T.ModificaSecuencia

Cualquier agente modifica la secuencia de operaciones y hace que un documento incompleto sea firmado digitalmente por ASF, y pasado a documento completo.

Amenaza 03: T.FirmaNoAutorizada

Cualquier agente inserta una firma en un documento en proceso de firma, sin que dicha firma provenga directamente de un interviniente con el procedimiento habitual.

Amenaza 04: T.DocumentoFalso

Cualquier agente envía al TOE un documento falso a ser firmado, y el TOE procesa dicho documento como válido y realiza un proceso completo de firma.

Amenaza 05: T.ModificaDocumento

Cualquier agente modifica un documento, sus firmas o el descriptor de firmas durante el proceso completo de firma.

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.

Objetivo entorno 01: OE.FirmaDigital

El entorno operacional proporcionará una marca de tiempo de una fuente confiable y un mecanismo para realizar firmas digitales a los documentos firmados por todos sus intervinientes.

Objetivo entorno 02: OE.Integridad

El entorno operacional garantizará la integridad de los documentos y sus firmas.

Objetivo entorno 03: OE.Autenticación

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Email: organismo.certificacion@cni.es

El entorno operacional será el encargado de autenticar a los usuarios de los puestos clientes.

Objetivo entorno 04: OE.Personal

Los administradores de los sistemas centrales tanto de RCI como de Renault son de confianza.

Objetivo entorno 05: OE.Configuración

Los puestos cliente y los servidores centrales donde se ejecuta el TOE están bien configurados.

Objetivo entorno 06: OE.Físico

Todo el sistema global, a excepción de los puestos clientes y los dispositivos de captura de firma, están soportados por un entorno seguro.

Objetivo entorno 07: OE.PKI

La custodia de la PKI utilizada para la generación de certificados firmados por la CA del grupo Renault estará gestionada por personal confiable, y sólo se generarán certificados si su uso final es conocido y aceptado.

Objetivo entorno 08: OE.DMZ

La parte servidor del TOE y su entorno se desplegará en una red DMZ segura en la que todas las comunicaciones con Internet serán manejadas por un reverse proxy y las comunicaciones con la Intranet se autorizarán a nivel IP:Puerto. Se utilizarán servidores intermedios para las comunicaciones de tal manera que éstas nunca serán directas. Tanto la configuración de la red como la asignación y utilización de los pares IP:puerto en los nodos conectados a la misma es responsabilidad del grupo de seguridad de Renault y no constituye una fuente de ataque.

Objetivo entorno 09: Generación

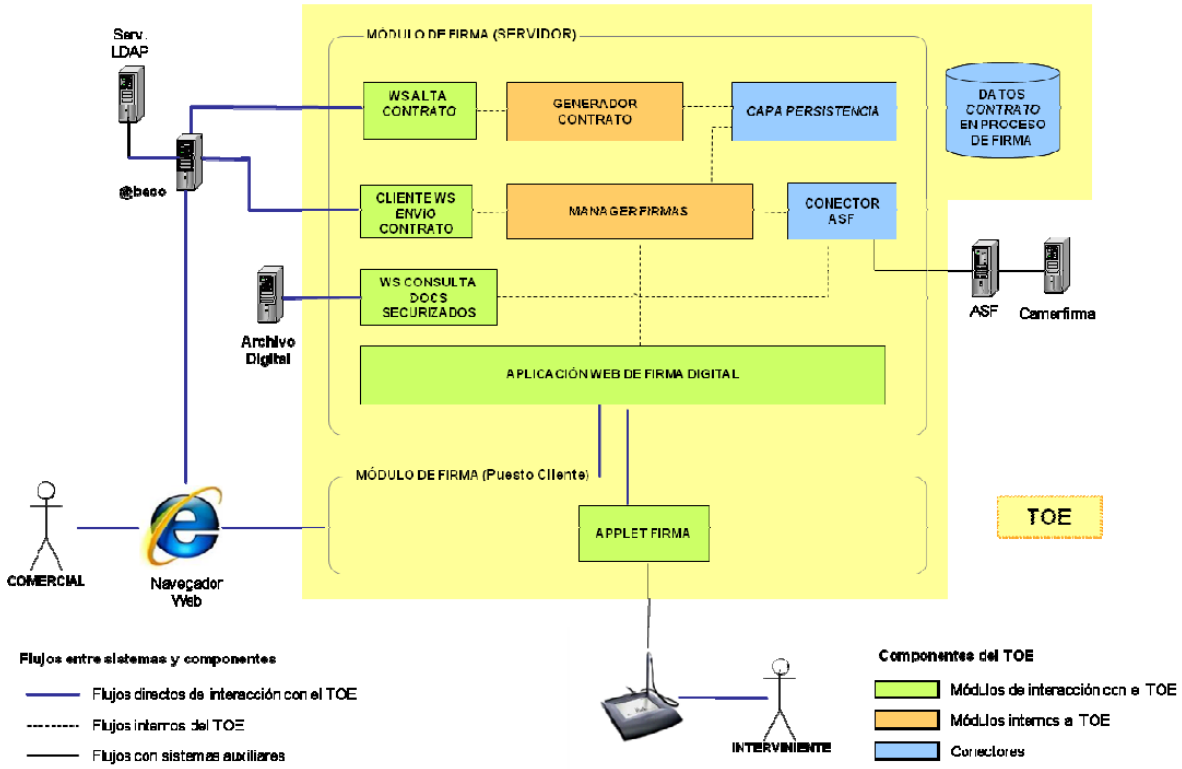
La generación y el del envío de los documentos a firmar será realizada por el entorno y sólo se realizará dicho envío una única vez para cada proceso completo de firma.

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 FÍSICA

El TOE tiene una arquitectura cliente-servidor que se muestra en la siguiente figura.



ARQUITECTURA LÓGICA

Los componentes software de los que consta el TOE son:

Elemento	Descripción
tabletas.jar	Fichero applet para la gestión de la firma con la tableta.
ContratoDigitalweb.war	Conjunto de manuales de instalación y operación para Módulo de Firma Electrónica de Documentos.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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.

- Declaración de Seguridad para Módulo de Firma Electrónica de Documentos de RCI Banque España, versión 1.5, Noviembre 2013.
- Manual de operación para Módulo de Firma Electrónica de Documentos de RCI Banque España versión 1.4, Noviembre 2013.
- Manual de instalación para Módulo de Firma Electrónica de Documentos de RCI Banque España versión 1.3, Noviembre 2013.

PRUEBAS DEL PRODUCTO

El evaluador ha diseñado y ejecutado un plan de pruebas independiente para verificar la funcionalidad de la totalidad de requisitos definidos en la declaración de seguridad e interfaces descritas en la especificación funcional, con resultado satisfactorio.

El evaluador también ha realizado pruebas de penetración con el fin de comprobar la existencia de vulnerabilidades obvias con un potencial de ataque *BASIC*, obteniendo un resultado satisfactorio. Para el diseño de estas pruebas de penetración se ha tenido en cuenta:

- Vulnerabilidades públicas e inherentes a la tecnología teniendo en cuenta el tipo de TOE.
- Especificación de requisitos de seguridad.
- La especificación de interfaces externos y pruebas funcionales sobre los mismos.

Para la realización de dichas pruebas, el evaluador ha verificado la instalación y ha considerado que el TOE está desplegado y configurado conforme a la declaración de seguridad y se encuentra en un estado conocido.

CONFIGURACIÓN EVALUADA

El fabricante ha proporcionado al laboratorio una instalación funcional del TOE en un entorno virtualizado para la realización de las pruebas. El evaluador ha verificado la instalación y ha considerado que el TOE está desplegado y configurado conforme a la declaración de seguridad y se encuentra en un estado conocido, considerándola por tanto válida para la realización de las pruebas.

El evaluador ha realizado los pasos indicados para obtener la versión del TOE en operación, y ha verificado que es la misma versión que la descrita en la declaración de seguridad.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

Los requisitos software y hardware son los que se indican a continuación. Así, para el funcionamiento del producto Módulo de Firma Electrónica de Documentos v2.18 es necesario disponer de los siguientes componentes software:

Para los puestos Cliente:

- Sistema Operativo Windows XP o Windows 7.
- Navegadores: Internet Explorer v7 o superior o Mozilla Firefox v9 o superior.
- Plugin Flash v11 o superior.
- Tableta digitalizadora WACOM 520-U y drivers.
- JVM versión 6 o superior.
- Microsoft Visual C++ 2005 o superior.

Para el servidor

- Sistema operativo: Solaris 10.
- Servidor web Apache 2.0.59 o superior.
- Servidor de aplicaciones J2EE WebSphere application server CE v.2.1.0.1.
- Java JRE v.1.6.20 o superior.
- Plataforma ASF de TB Solutions v.51.17 o superior.
- Puesto de venta RCI (@baco) v.1.04.267 o superior.
- Archivo digital.
- Camerfirma (Conexión SSL a sus servidores).
- LDAP SUN One DS 5.2P4.

En cuanto a los componentes hardware, el único requisito es que soporten los elementos software detallados previamente.

RESULTADOS DE LA EVALUACIÓN

El producto Módulo de Firma Electrónica de Documentos v2.18 ha sido evaluado en base a la “Declaración de Seguridad para Módulo de Firma Electrónica de Documentos de RCI Banque España, versión 1.5, Noviembre 2013”.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 más los componentes extendidos ASE_SPD.1, ASE_OBJ.2 y ASE_REQ.2 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 EAL1+ (ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2), definidas por Common Criteria [CC-P3] y la Metodología de Evaluación [CEM] en su version 3.1 r3.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

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.

- Tanto la red como los puestos cliente de acceso al TOE deben estar configurados acorde a la declaración de seguridad.
- El personal que hace uso del mismo debe estar adecuadamente preparado y familiarizado con los procesos de firma.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Módulo de Firma Electrónica de Documentos v2.18, 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, R3 Final, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R3 Final, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R3 Final, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R3 Final, July 2009.

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

DECLARACIÓN DE SEGURIDAD

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la "Declaración de Seguridad para Módulo de Firma Electrónica de Documentos de RCI Banque España, versión 1.5, Noviembre 2013".

También se encuentra disponible para su descarga en la web del Organismo de Certificación *http://www.oc.ccn.cni.es*.

ENAC
CERTIFICACIÓN
Nº 45/C-PR110

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