REF:	2007-2-INF-197 v2	Creado:	CERT2
Difusión:	Público	Revisado:	TECNICO
Fecha:	12.03.2008	Aprobado:	JEFEAREA

INFORME DE CERTIFICACION del ASF v4.1.5

Expediente: 2007-2 ASF v4.1.5

Referencias:

EXT-291	Solicitud de Certificación ASF V4.1.
EXT-478	ASF-ETR, ASF 4.1.5 Evaluation Technical Report,19-02-2008, Versión 5.0, EPOCHE & ESPRI.
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.

Informe de certificación del producto ASF (Advanced Signature Framework), versión 4.1.5, según la solicitud de referencia [EXT-291], de fecha 23/02/2007, y evaluado por el laboratorio EPOCHE & ESPRI, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-478] de acuerdo a [CCRA], recibido el pasado 21/02/2008.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

INDICE

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Resumen

Este documento constituye el Informe de Certificación para el expediente de la certificación del producto ASF (Advanced Signature Framework), versión 4.1.5.

La plataforma de firma ASF constituye una solución completa para la integración de la Firma Electrónica Avanzada en la infraestructura informática de una entidad u organización. Una de sus características diferenciadoras es la posibilidad de operar simultáneamente con más de una Autoridad de Certificación (CA), liberando al resto de los sistemas de la complejidad añadida que supone la compatibilidad multi-CA.

Fabricante: TB-Solutions Advanced Technologies S.L.

Patrocinador: TB-Solutions Advanced Technologies S.L.

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

Laboratorio de Evaluación: EPOCHE & ESPRI.

Perfil de Protección: ninguno.

Nivel de Evaluación: EAL3+ (ALC-FLR.1).

Fortaleza de las Funciones: no aplica, CC v3.1

Fecha de término de la evaluación: 21-02-2008.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL3+ (aumentado con ALC_FLR.1) 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 EAL3, definidas por los Criterios Comunes v3.1 [CC-P3] y la Metodología de Evaluación v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto ASF v4.1.5, se propone la resolución estimatoria de la misma.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Resumen del TOE

La plataforma de firma ASF constituye una solución completa para la integración de la Firma Electrónica Avanzada en la infraestructura informática de una entidad u organización. Una de sus características diferenciadoras es la posibilidad de operar simultáneamente con más de una Autoridad de Certificación (CA), liberando al resto de los sistemas de la complejidad añadida que supone la compatibilidad multi-CA.

Las principales funciones de seguridad ofrecidas por la plataforma ASF para garantizar la salvaguarda de las transacciones electrónicas son las siguientes:

• **Autenticación**. Permite la identificación fiable de usuarios remotos. La herramienta básica utilizada para ello es el certificado digital X.509v3.

• **Integridad**. La Firma Electrónica Avanzada de documentos digitales permite verificar que éstos no han sido modificados por un tercero tras la generación de los mismos.

• **No Repudio**. El sistema almacena en una base de datos las copias de los documentos firmados, de forma que éstas puedan ser utilizadas, si ello es necesario, como prueba de autoría.

• **Confidencialidad**. La generación de documentos cifrados permite garantizar que únicamente los destinatarios de los mismos pueden acceder a su contenido.

La plataforma ASF proporciona una solución de principio a fin para garantizar la seguridad de las comunicaciones, disponiendo para ello de funcionalidades que permiten el cifrado, la firma, el fechado, y la transmisión de documentos electrónicos de un modo seguro.

Para ello, ASF contempla todos los procedimientos necesarios para la creación de documentos firmados y/o cifrados, la validación y el control de la vigencia de los certificados utilizados, el registro de la información de firma necesaria para garantizar el no repudio, así como el establecimiento de políticas de firma.

El Target Of Evaluation (TOE) está constituido por un subconjunto de los servicios que proporcionan la funcionalidad completa de la plataforma de firma ASF.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL3, más las requeridas para el componente adicional, ALC_FLR.1, según la parte 3 de CC v3.1 r1.

-Requisitos de aseguramiento: Clase ASE - Security Target Evaluation

ASE_INT.1 ST introduction
ASE_CCL.1 Conformance claims
ASE_SPD.1 Security problem definition
ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition
ASE_REQ.2 Derived security requirements
ASE_TSS.1 TOE summary specification

-Requisitos de aseguramiento: Clase ADV - Development

ADV_FSP.3 Functional specification with complete summary
ADV_ARC.1 Security architecture description
ADV_TDS.2 Architectural design

-Requisitos de aseguramiento: Clase AGD - Guidance Documents

AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

-Requisitos de aseguramiento: Clase ALC - Life-Cycle Support

ALC_CMC.3 Authorisation controls
ALC_CMS.3 Implementation representation CM coverage
ALC_DEL.1 Delivery procedures
ALC_DVS.1 Identification of security measures
ALC_FLR.1 Basic flaw remediation
ALC_LCD.1 Developer defined life-cycle model

-Requisitos de aseguramiento: Clase ATE - Tests

ATE_COV.2 Analysis of coverage
ATE_DPT.1 Testing: basic design
ATE_FUN.1 Functional testing
ATE_IND.2 Independent testing - sample

-Requisitos de aseguramiento: Clase AVA - Vulnerability Assessment

AVA_VAN.2 Vulnerability analysis

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los requisitos funcionales, según la parte 2 de CC v3.1 r1, siguientes:

FDP_ACC.2 Complete access control
FDP_ACF.1 Security attribute based access control

FMT_MSA.1 Management of security attributes
FMT_MSA.3 Static attribute initialisation
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FIA_UID.2 User identification before any action
FIA_UAU.2 User authentication before any action
FIA_UAU.5 Multiple authentication mechanisms
FIA_UAU.7 Protected authentication feedback

FCS_CKM.1 Cryptographic key generation
FCS_CKM.2 Cryptographic key distribution
FCS_CKM.3 Cryptographic key access
FCS_CKM.4 Cryptographic key destruction
FCS_COP.1 Cryptographic operation

FAU_GEN.1 Audit data generation
FAU_SAR.3 Selectable audit review

FDP_ITT.1 Basic internal transfer protection
FDP_ITT.3 Integrity monitoring

FPT_ITT.1 Basic internal TSF data transfer protection
FPT_ITT.3 TSF data integrity monitoring

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Identificación

Producto: Advanced Signature Framework (ASF) v4.1.5.

Declaración de Seguridad: Declaración de Seguridad para Advanced Signature Framework v4.1.5, v1.9 Enero 2008.

Perfil de Protección: ninguno.

Nivel de Evaluación: CC v3.1 r1 EAL3+ (ALC-FLR.1).

Fortaleza de las Funciones: no aplica en CC v3.1.

Política de seguridad

El uso del producto ASF v4.1.5, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de las políticas como dispositivo de firma se encuentra en la declaración de seguridad. En síntesis, se establece la necesidad de implementar políticas organizativas relativas a:

Política 01: Documentación guía de instalación y uso

En el momento de la entrega del TOE se proporcionará la documentación guía de instalación y de uso necesaria para que el propietario del TOE sepa cómo instalarlo y gestionarlo de modo seguro. La documentación será inequívoca y contendrá la suficiente información para garantizar la instalación y operación seguras del TOE.

Política 02: Aplicación de procedimientos por administrador TOE

El administrador del sistema seguirá todos los procedimientos y normas establecidas en la documentación guía que se le entregará, definiendo y manteniendo los permisos de acceso establecidos para los archivos críticos del TOE. Éstos son los archivos de auditoría, las trazas de eventos del servidor de aplicaciones (en los que podría aparecer información sensible acerca de las conexiones a base de datos) y el archivo en el que se encuentra la clave secreta con la que se cifran las contraseñas almacenadas.

Política 03: Revisión de auditorías

Existirá un auditor interno del TOE, diferente del administrador del sistema,

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

que será el encargado de revisar periódicamente el HMAC de cada archivo de auditoria, para comprobar así que dichos ficheros no han sido modificados. Además, el auditor interno del TOE asegurará que los datos auditados se archivan regularmente, para de esta forma prevenir posibles problemas de sobrecarga en los almacenes de registros de auditoría.

Política 04: Cualificación de los usuarios del TOE

Los usuarios del TOE deberán estar suficientemente cualificados para realizar sus funciones. El propietario del TOE proporcionará a los usuarios y administradores del mismo el entrenamiento y formación necesarios para que adquieran el conocimiento y la experiencia requeridos para la utilización del sistema de manera segura.

Política 05: Disposición de datos de usuario y privilegios de acceso

El propietario del TOE garantizará la confidencialidad y protección de los datos de autenticación de los usuarios del mismo. Ningún usuario podrá acceder al sistema sin acreditarse previamente con ellos. Asimismo, en el momento en el que un usuario sea dado de alta se le asignará un rol, en función del cual tendrá unos permisos asociados para realizar determinadas acciones. El propietario del TOE habrá de cerciorarse de que estas acciones corresponden realmente con aquellas operaciones para las que el usuario esté realmente autorizado.
Asimismo, el propietario del TOE deberá gestionar los keystores definidos para almacenar las claves privadas utilizadas para firmar las peticiones o para procedimientos de autenticación, de manera que las contraseñas de acceso a los almacenes estén libres de accesos indebidos y almacenadas en un lugar seguro. Además, estos keystores deben ser de tipo JCEKS para que de esta forma las claves privadas en ellos depositadas puedan almacenarse cifradas.
El propietario del TOE se asegurará igualmente de que existan procedimientos apropiados para asegurar la destrucción de los datos de autenticación, así como la eliminación de los privilegios asociados, una vez que el acceso haya sido eliminado o bien en el caso de que las reglas de control de acceso hayan sido redefinidas. Esto se aplica tanto a los administradores como a los usuarios del TOE.

Política 06: Restricción de acceso al TOE

El propietario del TOE será el responsable de asignar las debidas restricciones de acceso al mismo para cada una de las aplicaciones registradas en el sistema. De esta forma, se definirán los usuarios autorizados a acceder al TOE mediante cada aplicación. Asimismo, deberán asignarse restricciones de acceso a los módulos OCSPResponder y TSAServer.

Política 07: Seguimiento de política de seguridad

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Existe una Política de Seguridad Organizacional del Sistema, en la que se identifican y documentan adecuadamente los riesgos y amenazas al sistema, así como los objetivos de seguridad deseados, proporcionando unas pautas a seguir para garantizar los servicios y propiedades de seguridad declarados. Asimismo, en dicha política se especifica un plan de actuación ante posibles contingencias o incidentes no deseados. Todos los usuarios del TOE, y especialmente los administradores del mismo, deberán estar al corriente de dicha política de seguridad organizacional y cumplir los requisitos en ella marcados.

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.

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.

Hipótesis 01: Administrador del sistema confiable

Se supone que el equipo en el que se encuentran instalados tanto los archivos de propiedades utilizados para la configuración del sistema como los archivos de servidor en los que puede aparecer información sensible (por ejemplo, la relativa a las conexiones a bases de datos) tendrá su acceso restringido, de forma que el administrador del sistema será la única entidad que dispondrá de los permisos necesarios para acceder a los mencionados archivos. Además, se supone que dicho administrador no actuará de manera malintencionada ni proporcionará permisos de acceso indebidos.

Hipótesis 02: Administrador de la auditoría

Se supone que existirá un administrador de archivos de auditoría que revisará periódicamente dichos archivos en busca de posibles intentos de ataque al TOE. En el caso de encontrar algún intento de ataque, el administrador de archivos de auditoría realizará las acciones que defina el usuario del producto.

Hipótesis 03: Administrador de la base de datos

Se supone que el administrador de la base de datos será confiable, que

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

no otorgará a la misma permisos de acceso indebidos (ni de lectura ni de escritura), así como que mantendrá en secreto los datos de las conexiones establecidas.

Hipótesis 04: Usuarios del TOE responsables

El personal que administra, gestiona y utiliza el Objeto de Evaluación será suficientemente competente para desarrollar sus funciones, de forma que no realizará un uso incorrecto del TOE, a la vez que respetará la seguridad y confidencialidad de los datos sensibles contenidos en el mismo.
Para ello, se supone que dicho personal poseerá el conocimiento necesario acerca de principios básicos de seguridad computacional. Asimismo, se presume que dicho personal leerá, entenderá y seguirá la documentación que le sea relevante para el desempeño de sus funciones.

Hipótesis 05: Datos de usuario

El personal que administra, gestiona y utiliza el TOE será suficientemente responsable para evitar que sus contraseñas de acceso sean accesibles a personas o entidades no autorizadas. Además, dicho personal deberá asegurarse de poder disponer de estas contraseñas cuando éstas se le requieran para llevar a cabo la autenticación. Lo mismo habrá de ser tenido en cuenta para el caso de los certificados digitales con los que se realizan autenticaciones de cliente en la consola. Respecto a las claves privadas almacenadas en los keystores de aplicaciones cliente, se supone que el personal encargado de gestionar los keystores será lo suficientemente responsable como para mantener las contraseñas de acceso a los mismos libres de accesos indebidos y almacenadas en lugar seguro.

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para el producto ASF v4.1.5, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a “Basic” de EAL3, 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.

Amenazas cubiertas:

Amenaza 01: Obtención de las claves privadas

Un atacante podría conseguir el acceso a alguna de las claves privadas de los certificados almacenados si lograse vulnerar las medidas de seguridad

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

que las protegen, comprometiendo de esa forma la confidencialidad de las mismas.

Amenaza 02: Uso no autorizado de las claves privadas

Un atacante podría utilizar las claves privadas almacenadas y registradas para uso de una determinada aplicación, realizando con ellas operaciones que no le estuvieran permitidas.

Amenaza 03: Lectura de contraseñas almacenadas en base datos

El administrador de la base de datos podría acceder a la totalidad de las contraseñas almacenadas en ella, puesto que dispone de permiso de lectura para toda la base de datos. Al encontrarse las contraseñas cifradas, el administrador podría descifrarlas si fuese capaz de vulnerar el algoritmo criptográfico de cifrado utilizado para protegerlas.

Amenaza 04: Obtención de la clave secreta

Durante el proceso de intercambio de la clave secreta, un agente externo podría interceptar la información negociada mediante un ataque de tipo “man-in-the-middle” y posteriormente leer la clave secreta. Si esto ocurriese, el atacante sería capaz de descifrar la información intercambiada entre el TOE y la aplicación usuaria, la cual debería ser confidencial.

Amenaza 05: Violación de la integridad de los archivos de auditoria

La violación de la integridad de los archivos de auditoría podría no ser detectada una vez que los ficheros de auditoría más antiguos hubiesen sido archivados en un almacén externo gestionado por personal ajeno a la administración del TOE.

Amenaza 06: Suplantación de identidad en las respuestas de los webservices

Un atacante podría interceptar una petición realizada al TOE por una aplicación cliente y responder a ésta suplantando la identidad del TOE.

Amenaza 07: Modificación de las respuestas de los webservices

Durante el proceso de envío de la respuesta del TOE a una petición realizada por una aplicación cliente, dicha respuesta podría ser interceptada y modificada por un atacante.

Amenaza 08: Violación del Servicio TOE

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Los intentos por parte de un atacante de realizar operaciones no permitidas (introduciendo parámetros erróneos, realizando ataques de repetición, etc.) capaces de comprometer la confidencialidad, integridad, disponibilidad y/o autenticidad del TOE podrían no ser detectados.

Amenaza 09: Uso no autorizado del Servicio TOE

Un atacante podría realizar invocaciones a los servicios del TOE sin estar autorizado a ello, comprometiendo con ello la confidencialidad y la disponibilidad del mismo.

Amenaza 10: Integridad de peticiones realizadas a OCSPs y TSAs

Un atacante podría interceptar y modificar la petición realizada por el TOE a una Autoridad de Sellado de Tiempos (TSA) y/o Servidor de Estados (OCSP) sin que dicha modificación fuese detectada.

Amenaza 11: Integridad de respuestas de entidades externas al TOE

Un atacante podría interceptar y modificar la respuesta del TOE a una petición de una TSA, un servidor OCSP o una Autoridad de Certificación sin que dicha modificación fuese detectada.

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 producto son los siguientes:

Objetivo entorno 01: Acceso restringido

El entorno operacional del TOE debe permitir el acceso al TOE o partes del TOE únicamente al personal autorizado al mismo.

Objetivo entorno 02: Formación

El entorno operacional del TOE debe asegurar que todos los usuarios humanos del TOE (i.e., personas físicas) hayan recibido previamente la formación e instrucción adecuadas para permitirles trabajar con el TOE siguiendo todos los procedimientos que impliquen el funcionamiento seguro del mismo.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Objetivo entorno 03: Proporcionar todos los entregables necesarios

El entorno operacional del TOE debe garantizar que la entrega del mismo se haga acompañada de toda la información y documentación guía necesarias para una correcta instalación y uso del TOE.

Objetivo entorno 04: Revisión de auditorías

El entorno operacional del TOE debe garantizar la realización de auditorías periódicas que permitan la detección de posibles intentos de violación al TOE, para de esta forma poder tomar las medidas oportunas, definidas por el propietario del TOE, en el caso de que dichos intentos sean identificados.

Objetivo entorno 05: Formación en política de seguridad

En el entorno operacional del TOE debe existir un responsable encargado de formar a los administradores y usuarios del mismo, para asegurarse de que éstos conocen las políticas de seguridad del TOE y de que las aplican.

Objetivo entorno 06: Gestión de los datos de autenticación

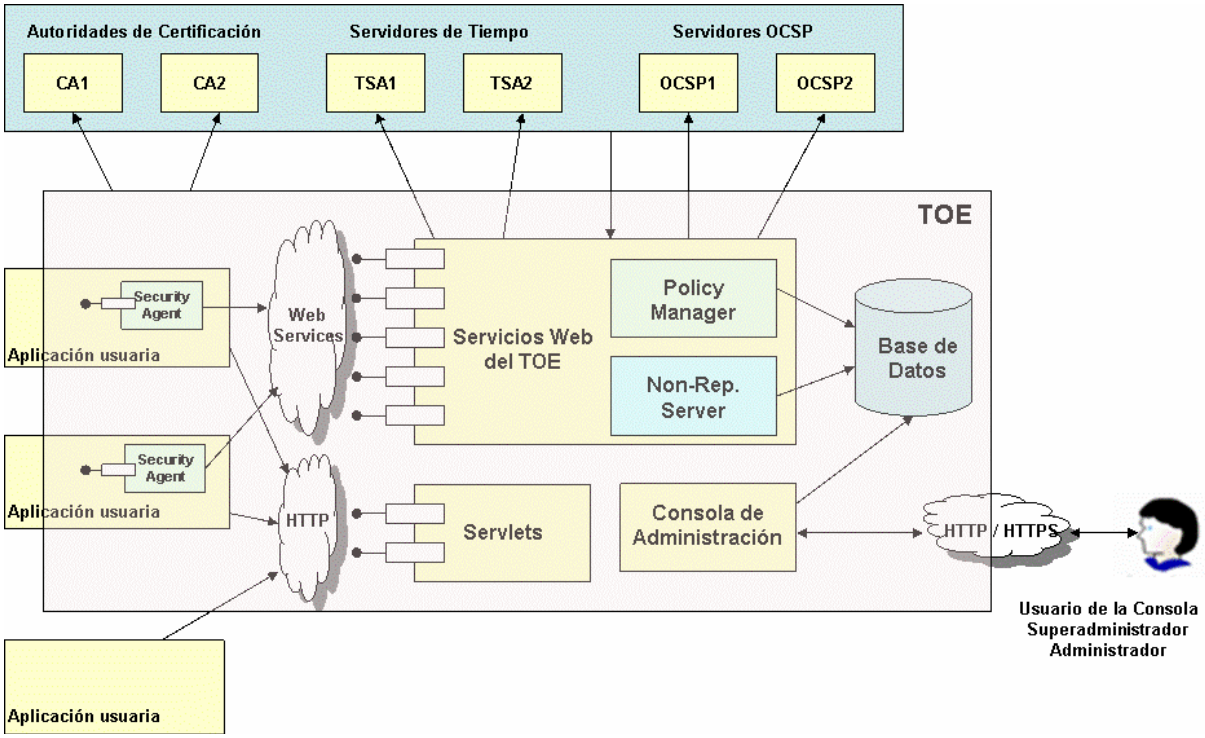
El entorno operacional del TOE debe garantizar la confidencialidad de los datos de autenticación de los distintos usuarios, así como la destrucción de los mismos en caso de su redefinición.
Asimismo, el entorno operacional del TOE debe garantizar que las restricciones de acceso no tendrán asociados certificados cuya seguridad pueda haberse visto comprometida.

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

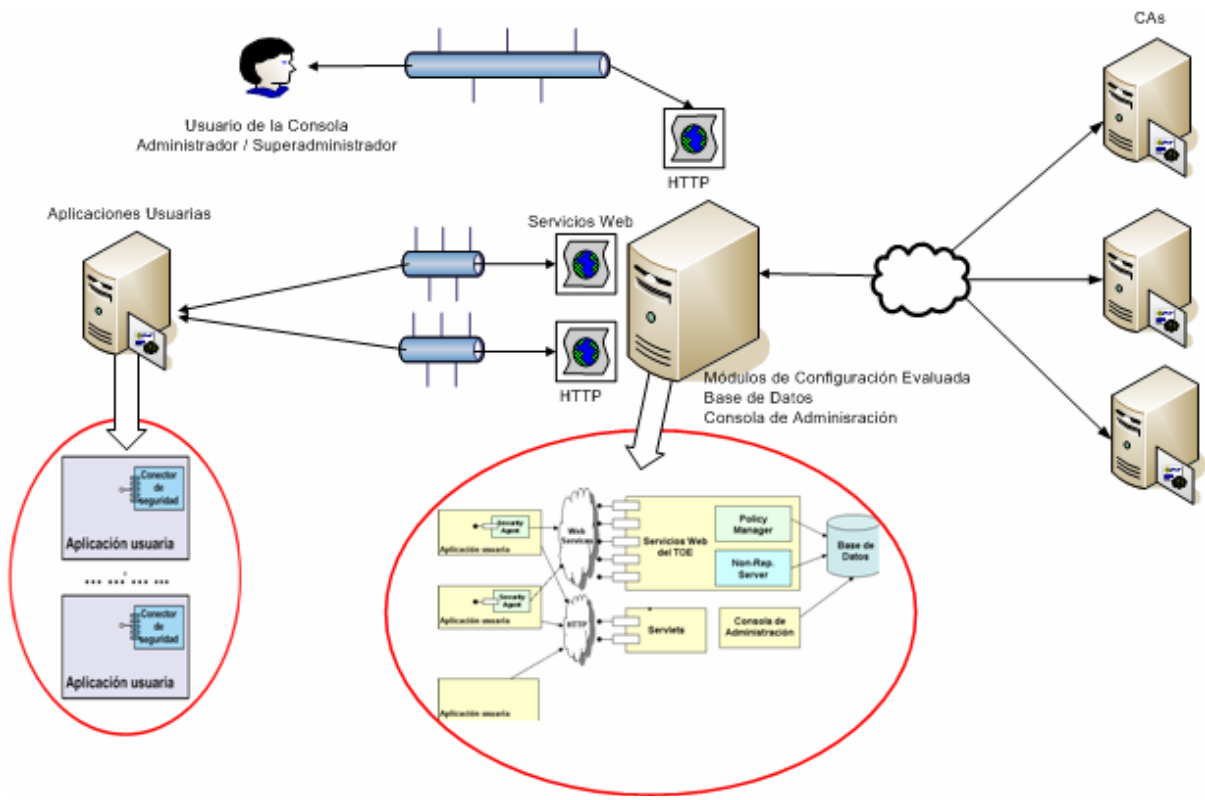
Arquitectura

Arquitectura Lógica:

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es



Arquitectura Física:



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@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 Advanced Signature Framework v4.1.5, v1.9 Enero 2008
- Manual de Usuario Consola de Administración ASF v1.8 Enero 2008
- Manual de Integración Agente de Seguridad JAVA v1.3 Enero 2008
- Manual de Instalación Servicio ASF v1.11 Enero 2008
- Manual de Instalación Base de Datos v1.8 Enero 2008
- Manual de Instalación Consola de Administración v1.9 Enero 2008
- Manual de Instalación Demo ASF v1.8 Enero 2008
- Requerimientos Técnicos Servicio ASF v1.4 Enero 2008
- Configuración Segura de la Versión Evaluada v1.7 Enero 2008
- Guía de Securización del Entorno v1.5 Enero 2008
- Manual_de_Explotación_v1.5 Enero 2008
- Instalación de ASF en Tomcat v1.4 Enero 2008

Pruebas del producto

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todos las pruebas ha sido realizados por el fabricante en sus instalaciones con resultado satisfactorio.

El proceso 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 los las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido entorno a un 25 % de 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.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

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 representaba un problema para la seguridad, ni suponía 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 de ASF es necesario disponer de los siguientes componentes software:

• **Servidor de aplicaciones**. El servidor de aplicaciones ha de soportar una máquina virtual Java J2SE 1.4.2. o superior.

• **Servidor base de datos**. El servidor de base de datos ha de tener disponible un driver de tipo JDBC.

• **Sistema operativo**. El sistema operativo de los equipos donde se ejecuta ASF ha de permitir la ejecución de una máquina virtual Java J2SE 1.4.2 o superior.

• **Java Runtime Enviroment**. Respecto a la versión del runtime Java (J2SE) sobre el que se ejecutará el servidor de aplicaciones, se recomienda utilizar la máquina virtual JRE 1.5.0 o superior de Sun. Como mínimo, es necesario la J2SE 1.4.2.

• **Navegadores**. Cualquiera de los siguientes es válido.
- o Microsoft Internet Explorer v6.0 Service Pack 2 o superior.
- o Netscape Comunicator v6 o superior.
- o Mozilla v4.1 o superior.

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

Dentro de todas las posibilidades que ofrecen estos requisitos software, la configuración que se ha elegido para su evaluación es la siguiente:

• **Servidor de aplicaciones**. Apache Tomcat 5.5.

• **Servidor base de datos**. SQLServer 2000.

• **Sistema operativo**: Windows XP

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

• **Java Runtime Enviroment**. JRE 1.5.0.12

• **Navegadores**. Microsoft Internet Explorer v6.0.

Resultados de la Evaluación

El producto ASF v4.1.5 ha sido evaluado frente a la declaración de seguridad "Declaración de Seguridad para Advanced Signature Framework v4.1.5", v1.9 de Enero 2008.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL3+** (aumentado con ALC_FLR.1) 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 EAL3, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 r1.

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.

Accesos remotos

- Cerrar el acceso remoto a la aplicación de administración mediante la configuración del servidor de aplicaciones, permitiendo que tan solo aquellos usuarios que se conecten desde localhost, puedan acceder al mismo.

- Cerrar el acceso mediante protocolo http, permitiendo únicamente acceder a la aplicación mediante https.

SQL Server / Windows XP / Internet Explorer

- Configurar SQL Server para que sólo acepte peticiones desde localhost

Apache Tomcat 5.5.25

- Eliminación por completo de los módulos de administración y aplicaciones de ejemplo
- Cambio de la palabra clave y puerto de apagado remoto por uno más complejo

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

Medidas de seguridad

- Obligar mediante medidas IT / Procedurales el cambio de los passwords por defecto en la aplicación: administrador inicial / base de datos...
- Forzar el uso de certificados distintos a los provistos por el fabricante, detallando el proceso de generación de los mismos si es necesario en los manuales de instalación
- Verificar siempre el estado de revocación y nunca usar cachés; forzar que siempre se usen sellos de tiempo

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto ASFv4.1.5, se propone la resolución estimatoria de la misma.

Glosario de términos

ASF	Advanced Signatura Framework
CA	Autoridad de Certificación
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Intelligencia
ETR	Evaluation Technical Report
LDAP	Lightweight Directory Access Protocol
OC	Organismo de Certificación
OCSP	Online Certificate Status Protocol
PKI	Public Key Infraestructure
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

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, r1, September 2007.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r1, September 2007.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r1, September 2007.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r1, September 2007.

Declaración de seguridad

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación de la declaración de seguridad completa de la evaluación: **Declaración de Seguridad para Advanced Signature Framework v4.1.5, v1.9 Enero 2008**.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es