REF:	2009-30-INF-515 v1	Creado:	CERT2
Difusión:	Expediente	Revisado:	TECNICO
Fecha:	18.08.2010	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2009-30
Datos del solicitante: EIN 26-3272415 - Authenware Corp.

Referencias:

EXT-942	Solicitud de Certificación Authentest v2.2.1.
EXT-995	AUT-ETR, Informe Técnico de Evaluación Authentest Server, 24-05-2010, Versión 2.0, EPOCHE & ESPRI.
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.
SOGIS	European Mutual Recognition Agreement of IT Security Evaluation Certificates version 3.0, Jan 2010.

Informe de certificación del producto Authentest Server v1.2.6, según la solicitud de referencia [EXT-942], de fecha 09/12/2009, y evaluado por el laboratorio EPOCHE & ESPRI, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-995] de acuerdo a [CCRA] y [SOGIS], recibido el pasado 24/05/2010.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

INDICE

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen

Este documento constituye el Informe de Certificación para el expediente de la certificación del producto Authentest Server v1.2.6.

El TOE certificado es un conjunto de funcionalidades y subsistemas que provee el producto Authentest para proteger al servicio de verificación biométrica de ataques que impidan su normalfuncionamiento.

En general el producto Authentest provee un servicio de verificación de identidad mediante biometría comportamental basada en el ritmo de tecleo de los usuarios que operan a través de aplicaciones externas al TOE. Si bien su principal aplicación es la autenticación mediante nombre de usuario y contraseña, Authentest está preparado para trabajar con cualquier dato o campo que se desee validar biométricamente. Por ejemplo, frases de paso, el nombre de usuario, etc.

Fabricante: Authenware Corp.

Patrocinador: Authenware Corp.

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: EAL2+ ALC_FLR.1

Fecha de término de la evaluación: 24-05-2010.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2+ (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 EAL2, 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 Authentest Server v1.2.6, se propone la resolución estimatoria de la misma.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen del TOE

El TOE es un conjunto de funcionalidades y subsistemas que provee Authentest para proteger al servicio de verificación biométrica de ataques que impidan su normal funcionamiento.

Las funcionalidades del TOE incluyen:

· la capacidad de repeler los ataques de denegación de servicio y de repetición ilegítima de ingresos ya recibidos (ataques de repetición o replay attacks)

· la capacidad de controlar el acceso al servicio web de verificación biométrica desde software externo que se conecte con el certificado digital adecuado.

· la capacidad de importar los certificados digitales que serán tomados como válidos en el momento de acceso.

· la capacidad de cifrar los patrones biométricos mediante la utilización del algoritmo AES con el fin de preservar su confidencialidad.

· la capacidad de generar registros de auditoría sobre las operaciones críticas del producto.

· la capacidad de consultar los registros de auditoría para su adecuado análisis.

· la capacidad de almacenar afuera del TOE tanto la base de datos de patrones biométricos de comportamiento e ingreso como los registros de auditoría, permitiendo así al cliente aplicar su infraestructura y políticas de seguridad y auditoría vigentes.

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL2, más las requeridas para el componente adicional ALC_FLR.1, según la parte 3 de CC v3.1 r3.

Requisitos funcionales de seguridad

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

La funcionalidad de seguridad del producto se limita a satisfacer los requisitos funcionales, según la parte 2 de CC v3.1 r3, siguientes:

- **FAU_GEN.1** AUDIT DATA GENERATION
- **FAU_SAR.1**_WEB-SERVICES AUDIT REVIEW
- **FAU_SAR.1**_ADMIN AUDIT REVIEW
- **FAU_SAR.1**_SSH AUDIT REVIEW
- **FAU_SAR.3** SELECTABLE AUDIT REVIEW
- **FDP_ACC.2**_WEB-SERVICES COMPLETE ACCESS CONTROL
- **FDP_ACC.2_PORTAL_ADMINISTRACION** COMPLETE ACCESS CONTROL
- **FDP_ACF.1_WEB-SERVICES** SECURITY ATTRIBUTE BASED ACCESS CONTROL
- **FDP_ACF.1_PORTAL_ADMINISTRACION** SECURITY ATTRIBUTE BASED ACCESS CONTROL
- **FMT_MSA.1_PORTAL_ADMINISTRACION** MANAGEMENT OF SECURITY ATTRIBUTES
- **FMT_MSA.1_WEB-SERVICES** MANAGEMENT OF SECURITY ATTRIBUTES
- **FMT_MSA.3_PORTAL_ADMINISTRACION** STATIC ATTRIBUTE INITIALIZATION
- **FMT_MSA.3_WEB-SERVICES** STATIC ATTRIBUTE INITIALIZATION
- **FMT_SMR.1** SECURITY ROLES
- **FMT_SMF.1** SPECIFICATION OF MANAGEMENT FUNCTIONS
- **FIA_UAU.2_ WEB-SERVICES** USER AUTHENTICATION BEFORE ANY ACTION
- **FIA_UAU.1_PORTAL_ADMINISTRACION** TIMING OF AUTHENTICATION
- **FIA_UID.2_WEB-SERVICES** USER IDENTIFICATION BEFORE ANY ACTION
- **FIA_UID.1_PORTAL_ADMINISTRACION** TIMING OF IDENTIFICATION
- **FPT_ITC.1** INTER-TSF CONFIDENTIALITY DURING TRANSMISSION
- **FTP_ITC.1** INTER-TSF TRUSTED CHANNEL
- **FPT_RPL.1** REPLAY DETECTION
- **FCS_CKM.1** CRYPTOGRAPHIC KEY GENERATION
- **FDP_ITC.1_IMPORTACION_CERTIFICADOS** IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES
- **FDP_ITC.1** CIFRADO_PATRONES_BIOMETRICOS IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES
- **FCS_COP.1_AES _CIFRADO_SISTEMA_FICHEROS** CRYPTOGRAPHIC OPERATION
- **FCS_COP.1_AES _CIFRADO_PATRONES_BIOMETRICOS** CRYPTOGRAPHIC OPERATION
- **FCS_COP.1_RSA** CRYPTOGRAPHIC OPERATION

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- **FPT_TST.1** TSF TESTING
- **FTA_TAB.1_PORTAL_ADMINISTRACION** DEFAULT TOE ACCESS BANNERS
- **FRU_RSA.1** MAXIMUM QUOTAS

Identificación

Producto: Authentest Server v1.2.6.

Declaración de Seguridad: A_clt_01_v06_Declaración de seguridad, numero de versión 06, 10/05/2010.

Perfil de Protección: ninguno.

Nivel de Evaluación: CC v3.1 r3 EAL2+ (ALC_FLR.1).

Política de seguridad

El uso del producto Authentest Server v1.2.6, 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:

P1. El entorno de uso del TOE garantizara la existencia de los siguientes roles y capacidades:

Administrador de consola: puede realizar la activación del producto y su configuración básica.

Usuario Authentest: puede realizar la configuración de los parámetros del entorno de red, arrancar o detener el servicio JBoss, configurar el URL del web-service, configurar la distribución de teclado del sistema operativo del TOE, cambiar su propia password, cambiar las reglas de firewall y administrar los certificados digitales utilizados por el web-service.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Aplicación web-service remota: invoca la funcionalidad de autenticación basada en el comportamiento humano a través de los métodos del servicio web ofrecidos por el TOE así como el resto de los métodos que permiten la gestión de los usuarios de las aplicaciones remotas y sus respectivos patrones biométricos. Puede ser cualquier entidad externa, como un servidor de aplicaciones o un proxy, que en todo caso se autentica por certificado e invoca los servicios web.

Roles para el portal web:

Administrador de grupo: cuenta con los privilegios necesarios para administrar usuarios y aplicaciones que pertenezcan al grupo de aplicaciones que administra.

Administrador de portal: este usuario es el que cuenta con los privilegios para crear grupos de aplicaciones, usuarios administradores de grupo, otros usuarios administradores de portal, lectura de toda la actividad, ver registros de auditoría del portal, cambiar el nivel de seguridad de Authentest Server , aplicaciones y usuarios, y activar o desactivar el modo de funcionamiento silencioso.

P2. El TOE generará trazas de auditoría de actividad del servicio de autenticación y relativas a la funcionalidad del TOE, para la integración en los sistemas de gestión del usuario con el TOE.

P3. El TOE identificará su versión y la condición de producto certificado en la consola y página principal del portal web, así como advertirá de las responsabilidades sobre el uso del producto utilizado o configurado de manera insegura.

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 no pudieran asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

H1. Como todos los métodos biométrico comportamentales (Por ej.: reconocimiento de la voz o la firma) la fiabilidad del algoritmo, en lo que a falsos negativos o

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

rechazos erróneos se refiere, depende fuertemente de la colaboración del usuario de la aplicación remota, que deberá seguir las siguientes recomendaciones equivalentes a cuando se va a firmar un cheque y se quiere evitar el rechazo del banco por no reconocer la firma como legitima:

Tipear naturalmente, evitando forzar una velocidad mayor o menor a la habitual durante el
entrenamiento del patrón biométrico y en los sucesivos ingresos.

En el momento de ingresar los datos observados biométricamente evitar realizar otra actividad que pueda alterar la naturalidad del ritmo habitual (hablar por teléfono, tipear con una sola mano, etc.)

Utilizar palabras que resulten naturales y reconocidas que impliquen un tipeo natural.

En caso de utilizar números tener presente que el patrón biométrico de tipeo varía si se utiliza una vez el teclado numérico y otra vez los números arriba de las letras.

Siempre que sea posible, utilizar la misma máquina y entorno. Mismo teclado, sistema operativo, navegador (en caso de aplicaciones Web), etc.

H2. La generación y distribución de los certificados y claves para el servidor de aplicaciones se realiza mediante una tercera entidad externa de confianza, con el nivel de seguridad acorde a cada instalación en particular.

H3. Los servidores de aplicación remotos que consumen los servicios de Authentest son
responsables de garantizar la confidencialidad e integridad de los certificados con los que se realiza la autenticación.

H4. La fiabilidad en el uso e integración de los servicios de Authentest en los servidores de aplicaciones remotos dependen de la seguridad y buenas prácticas de dichas entidades externas. Por lo anterior se considera como confiables a los servidores de aplicación remotos.

H5. El acceso físico al servidor está restringido a los administradores de Authentest, usuario administrador de consola y usuario Authentest, que son considerados como usuarios confiables en todas sus operaciones. Así también los usuarios administradores de Authentest, usuario administrador del portal y usuario administrador de grupo, que ingresan a través del portal de administración, son considerados como usuarios confiables en todas sus operaciones.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

H6. La fiabilidad en el uso de Authentest depende de la seguridad y buenas prácticas implementadas en el sistema de gestión de bases de datos externo, en donde se almacenan los patrones de comportamiento biométrico. Por lo anterior se considera que dicho sistema es
configurado.

H7. El sistema operativo deberá estar configurado de manera que realice correctamente la política de control de acceso a la aplicación “Server Administration”.

Aclaraciones sobre amenazas no cubiertas

La siguiente amenaza no supone un riesgo explotable para el TOE, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a “Basic” de EAL2, 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.

Amenaza cubierta:

T1. Un agente externo a la administración del sistema no autorizado, compromete la confidencialidad del patrón de comportamiento biométrico.

T2. Un agente externo a la administración del sistema no autorizado, compromete la confidencialidad de los parámetros de configuración del TOE degradando la seguridad del mismo en su servicio.

T3. Un agente externo en una red no confiable deniega el servicio de identificación comportamiento utilizando técnicas y ataques de denegación de servicios remotas, imposibilitando el acceso al servicio por parte de los usuarios de Authentest, utilizando firmas de comportamiento falsas o mediante replay attack.

Funcionalidad del entorno.

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

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Los objetivos que se deben cubrir por el entorno de uso del producto son los siguientes:

OE1. El entorno de uso deberá garantizar la fiabilidad del algoritmo de autenticación basado en el comportamiento, comunicando fehacientemente a todos los usuarios las siguientes recomendaciones:

Teclear naturalmente, evitando forzar una velocidad mayor o menor a la habitual durante el entrenamiento del patrón biométrico y en los sucesivos ingresos.

En el momento de ingresar los datos observados biométricamente evitar realizar otra actividad que pueda alterar la naturalidad del ritmo habitual (hablar por teléfono, tipear con una sola mano, etc.)

Utilizar palabras que resulten naturales y reconocidas que impliquen un tecleo natural.

En caso de utilizar números tener presente que el patrón biométrico de tipeo varía si se utiliza una vez el teclado numérico y otra vez los números arriba de las letras.

Siempre que sea posible, utilizar la misma máquina y entorno. Mismo teclado, sistema operativo, navegador (en caso de aplicaciones Web), etc.

OE2. El entorno de uso deberá garantizar la generación y distribución de los certificados y claves para el servidor de aplicaciones que se realiza mediante una tercera entidad externa de confianza con el nivel de seguridad acorde a cada instalación en particular.

OE3. El entorno de uso deberá garantizar la confidencialidad e integridad de los certificados con los que se realiza la autenticación. El cliente deberá garantizar la generación de los certificados con herramientas externas al TOE y copiarlos al TOE utilizando protocolo SSH. El cliente deberá garantizar la generación y distribución segura de de los certificados necesarios para invocar el web-service del TOE.

OE4. El TOE deberá tener comunicación con el cliente que consumirá el web-service en una red de datos separada de la red del cliente. En caso de no contar con una red separada debe de aislarse en un segmento de VLAN. A esta red de datos podrá también conectarse el servidor de base de datos, servidor de log (syslog) remoto y el equipo desde donde se podrá administrar el TOE mediante ssh y/o Portal de Administración. El acceso al TOE para su administración deberá realizarse desde un equipo conectado a la red de datos. En todos los casos se recomienda disponer de un solo punto de acceso a la red, sea la red de cliente o red de datos, e implementar mecanismos de filtrado que se basen en una política de denegación por defecto.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

OE5. El cliente deberá garantizar que el acceso físico al servidor está restringido a los administradores de Authentest, como así también que estos puedan ser considerados confiables (usuario administrador de consola, usuario Authentest, usuario administrador del portal y usuario administrador de grupo).

OE6. El entorno de uso deberá garantizar que el sistema de gestión de bases de datos externos, en donde se almacenan los patrones de comportamiento biométrico sea confiable y este bien configurado.

OE7. El entorno de uso deberá garantizar que el sistema operativo este configurado de manera que realice correctamente la política de control de acceso a la aplicación “Server Administration”.

Arquitectura

Arquitectura Lógica:

El TOE Authentest Server 1.2.6, es una parte del producto Authentest 1.2.6, cuya funcionalidad de seguridad está orientada a la protección de la funcionalidad biométrica que proporciona el producto.

El producto Authentest provee un servicio de verificación de identidad mediante biometría comportamental basada en el ritmo de tipeo de los usuarios que operan a través de aplicaciones externas al TOE. Si bien su principal aplicación es la validación biométrica al momento de la autenticación mediante nombre de usuario y contraseña, Authentest está preparado para trabajar con cualquier dato o campo que se desee validar biométricamente. Por ejemplo, frases de paso, solo el nombre de usuario, etc.

Authentest devuelve, a través de la consulta a un servicio web estándar, si la persona que ha tipeado es quien dice ser o no (0 o 1) acompañado por el porcentaje de confianza sobre esta afirmación. Para tomar esta decisión, Authentest compara el ingreso actual contra un patrón biométrico comportamental que incluye tres dimensiones principales:

1) El ritmo de tipeo (Tiempos de intervalo entre dos teclas y tiempos de detención de cada una)

2) Información del entorno habitual (IP, Sistema operativo, Navegador, etc.)

3) Comportamiento oculto o inconsciente tales como si el usuario legítimo utiliza la tecla <Tab> o el mouse para pasar del campo usuario a la contraseña, que días de la semana y a qué hora es esperable su ingreso, etc.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Las características principales de seguridad del TOE se pueden resumir:

1. capacidad de repeler los ataques de denegación de servicio y de repetición ilegítima de ingresos ya recibidos (ataques de repetición o replay attacks);
2. capacidad de controlar el acceso al servicio web de verificación biométrica desde software externo que se conecte con el certificado digital adecuado;

3. capacidad de importar los certificados digitales que serán tomados como válidos en el momento de acceso;

4. capacidad de cifrar los patrones biométricos mediante la utilización del algoritmo AES con el fin de preservar su confidencialidad.

5. capacidad de generar registros de auditoría sobre las operaciones críticas del producto.

6. capacidad de consultar los registros de auditoría para su adecuado análisis.

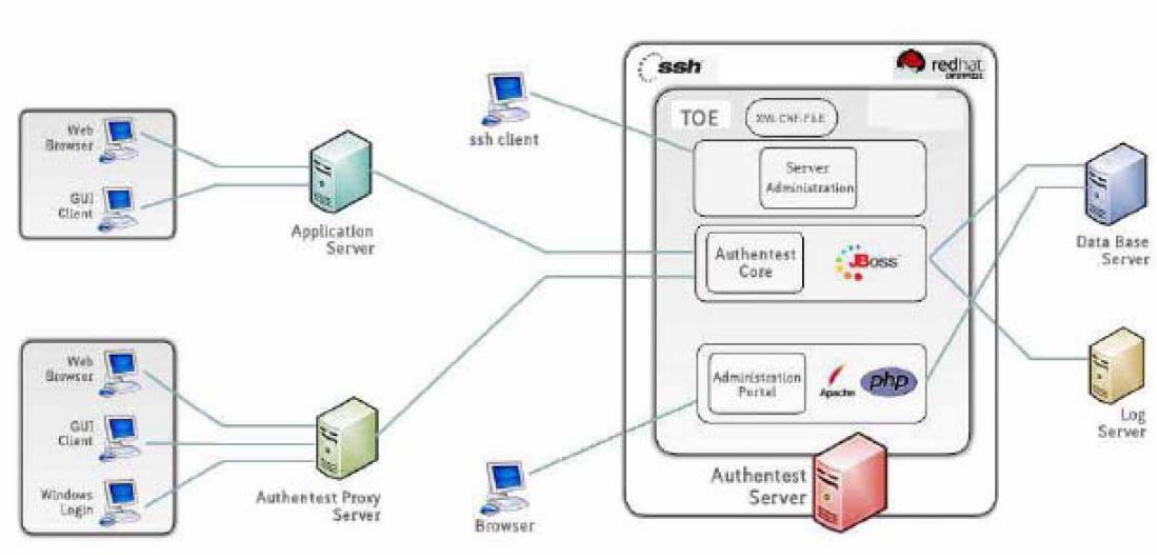
7. capacidad de almacenar fuera del TOE tanto la base de datos de patrones biométricos de comportamiento e ingreso, como los registros de auditoría.

Arquitectura Física:

Authentest server es una aplicación software y por lo tanto todo el hardware o firmware queda excluido desde el punto de vista de componentes externos.

En la siguiente figura se pueden ver los elementos que forman parte del entorno y los que forman parte del TOE. Desde el punto de vista físico, el TOE incluye JBOSS (despliega el fichero .war que contiene Authentest core que implementa los servicios web), Apache y PHP (incluye el módulo Administration Portal, conjunto de scripts en php que implementan la funcionalidad del portal web de administración) y los scripts que se ejecutan en la consola y que conforman la aplicación “Server Administration”.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
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.

o A_clt_01_v06_Declaración de seguridad, numero de versión 06, 10/05/2010.

o A_svc_07_v05_Authentest Operating System – RedHat 54 v.05 Mayo 2010

o A_svc_10_v02_Authentest Activation (AGD) v.03 Mayo 2010

o A_svc_08_v06_Authentest Activation v.06 Mayo 2010

o A_adm_01_v03_Authentest Server Administration v.04 Mayo 2010

o A_svc_02_v04_How to Create Authentest Signature Builder v.04 Mayo 2010

o A_svc_05_v04_Security Level Configuration v.04 Abril 2010

o A_adm_02_v05_Authentest Admin Portal User Guide v.05 Mayo 2010

o A_svc_04_v03_Authentest Service Network Structure, v 03 Mayo 2010

o A_svc_03_v06_API Webservice Authentest CORE

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Pruebas del producto

El evaluador ha seleccionado un subconjunto de pruebas y una estrategia apropiada para el TOE entregado por el fabricante. La documentación de la especificación funcional del TOE describe el comportamiento de las TSFIs y el evaluador ha aplicado esa información a la hora de desarrollar sus pruebas.

Para ello se ha tenido en cuenta:

- Trascendencia de los interfaces

- Tipos de interfaces

- Número de interfaces

Para la selección de las pruebas se han utilizado como criterios: la búsqueda de parámetros críticos en la interacción con las TSFIs, realización de pruebas exhaustivas en las TSFIs de mayor importancia y sospechas de mal comportamiento de las TSFIs ante determinados parámetros de entrada.

También se han realizado pruebas con parámetros de las TSFIs que pudieran tener especial relevancia en el mantenimiento de la seguridad del TOE.

En el plan independiente se han definido casos de prueba para todos los requisitos definidos en la declaración de seguridad. Para la realización de todas las pruebas se han ejercitado interfaces visibles desde el exterior.

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.

Configuración evaluada

Para garantizar la seguridad del servicio de autenticación basado en el comportamiento, el TOE implementa los siguientes mecanismos de seguridad que son objeto de evaluación:

Control de acceso al portal de administración

Autenticación fuerte basada en PKI para acceso a los webservices

De manera adicional Authentest registra los eventos principales relativos a la seguridad del servicio.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Cifrado de los patrones de comportamiento, como garantía de su confidencialidad.

Desde el punto de vista físico, el TOE incluye JBOSS (despliega el fichero .war que contiene Authentest core que implementa los servicios web), Apache y PHP (incluye el módulo Administration Portal, conjunto de scripts en php que implementan la funcionalidad del portal web de administración) y los scripts que se ejecutan en la consola y que conforman la aplicación “Server Administration”.

Para realizar las pruebas se ha precisado por el laboratorio de los siguientes elementos externos al TOE:

Sistema operativo RedHat Enterprise 5.4

Openssh Server 4.3

JAVA 1.6.0_07

Una configuración compatible de Hardware con los requerimientos anteriores como por ejemplo la siguiente:

- Procesador doble núcleo 1.5 Ghz o superior
- 4 GB de memoria
- HDD 40 GB o más, SCSI, SATA o SAS.
- Placa de Red compatible con RedHat Enterprise 5.4
- Lector DVD

El entorno del TOE incluye un servidor externo que aloja una base de datos MySQL donde se almacenan datos del TOE y el registro de auditoría.

Resultados de la Evaluación

El TOE Authentest Server v1.2.6 ha sido evaluado frente a la declaración de seguridad “A_clt_01_v06_Declaración de seguridad, numero de versión 06, 10/05/2010”.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL2+** (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 EAL2+, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 r3.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
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.

o Limitar al extremo el acceso al interfaz consola de administración web, únicamente a las personas debidamente autorizadas y desde PCs que carezcan de acceso a Internet o a otras redes potencialmente inseguras.

o Cambiar los passwords por defecto que presenta el TOE por passwords complejos para mitigar la posibilidad de un ataque de fuerza bruta.

o Configurar el firewall del sistema operativo del TOE para denegar el acceso a los puertos que no utilizan SSL, configurando debidamente los keystores para autenticación en cliente de los servicios web, por una persona con la debida competencia técnica.

o Utilizar el TOE y su entorno únicamente bajo una red segura, libre de atacantes.

o Imposibilitar el acceso físico a la máquina que aloja al TOE.

o Securizar debidamente los componentes del entorno, en concreto la base de datos del TOE.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del TOE Authentest Server v1.2.6, se propone la resolución estimatoria de la misma.

Glosario de términos

CC	Common Criteria
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
HW	HardWare

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

IT	Information Technology
OC	Organismo de Certificación
PC	Personal Computer
SW	SoftWare

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@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, r3, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r3, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r3, July 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, July 2009.

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:

“A_clt_01_v06_Declaración de seguridad, numero de versión 06, 10/05/2010”.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es