REF:	2009-16-INF-524 v1	Creado:	CERT2
Difusión:	Expediente	Revisado:	TECNICO
Fecha:	20.08.2010	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2009-16
Datos del solicitante: A-82958075 MNEMO EVOLUTION & INTEGRATION SERVICES

Referencias:

EXT-928	Solicitud de Certificación PROCESA V1.7.
EXT-992	PRO-ETR, Informe Técnico de Evaluación PROCESA ENGINE 1.7.3, 31-03-2010, Versión 3.0, 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 PROCESA ENGINE v1.7.3, según la solicitud de referencia [EXT-928], de fecha 16/07/2009, y evaluado por el laboratorio EPOCHE & ESPRI, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-992] de acuerdo a [CCRA] y [SOGIS], recibido el pasado 31/03/2010.

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

INDICE

RESUMEN **3**
RESUMEN DEL TOE 5
REQUISITOS DE GARANTÍA DE SEGURIDAD 6
REQUISITOS FUNCIONALES DE SEGURIDAD 6
IDENTIFICACIÓN **7**
POLÍTICA DE SEGURIDAD **7**
HIPÓTESIS Y ENTORNO DE USO **8**
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS 8
FUNCIONALIDAD DEL ENTORNO 11
ARQUITECTURA **11**
DOCUMENTOS **15**
PRUEBAS DEL PRODUCTO **16**
CONFIGURACIÓN EVALUADA **16**
RESULTADOS DE LA EVALUACIÓN **17**
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES **17**
RECOMENDACIONES DEL CERTIFICADOR **18**
GLOSARIO DE TÉRMINOS **18**
BIBLIOGRAFÍA **19**
DECLARACIÓN DE SEGURIDAD **19**

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 PROCESA ENGINE v1.7.3.

PROCESA es un producto BPMS (Business Processes Management System) especialmente diseñado para la construcción y ejecución de procesos de Administración Electrónica y de Tramitación Electrónica, sobre la base del concepto de reutilización de servicios. Utiliza las tecnologías BPM y SOA para la construcción de sistemas de información basados en procesos, en los cuales cada tarea es ejecutada por la combinación de la ejecución de los distintos tipos de servicios accesibles desde el servidor que está realizando la ejecución del proceso.

Es necesario distinguir entre PROCESA como producto y el objeto de evaluación (TOE):

· PROCESA: un producto basado en SOA que contiene una gestor BPM, los servicios necesarios para su administración y ejecución y herramientas para la creación e interacción con los procesos e instancias.
· TOE: el objeto de evaluación que consiste en el módulo PROCESA Engine, el núcleo principal de PROCESA, y que engloba el motor de BPM y la aplicación SOA junto con todos los servicios de administración y ejecución.

PROCESA Engine es una aplicación basada en una arquitectura orientada a servicios que permite la gestión del ciclo de vida de procesos, tareas y acciones encargadas de ser ejecutadas por ciertas personas o grupo de personas ofreciendo sus funcionalidades en base a servicios web.

Fabricante: Mnemo Evolution & Integrations Services, S.A.

Patrocinador: Mnemo Evolution & Integrations Services, S.A.

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: EAL1+ALC_FLR.1+ASE_SPD.1+ASE_REQ.2+ASE_OBJ.2

Fecha de término de la evaluación: 30-03-2010.

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

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1+ (aumentado con ALC_FLR.1+ASE_SPD.1+ASE_REQ.2+ASE_OBJ.2) 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 EAL1, 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 PROCESA ENGINE v1.7.3, 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 núcleo de PROCESA es el objeto de evaluación (TOE), y se corresponde con el módulo **PROCESA Engine,** entre cuyas características destacan las siguientes:

o Es un servicio inteligente de BPM-workflow sobre objetos reutilizables, mediante arquitecturas SOA e invocación de servicios web.

o Permite la construcción de una Plataforma de Servicios para el diseño de sistemas de información basados en flujos de procesos y árboles de tramitación complejos, para los cuales el número de caminos, el volumen de tareas por cada camino y la probabilidad de cambio en las especificaciones funcionales y técnicas asociadas a cada tarea son muy elevados.

o Aplicación práctica de las tecnologías BPM, SOA y utilización de estándares (XML, WebServices, XPDL, BPEL, etc.).

o Diseñado teniendo en cuenta requisitos de construcción de sistemas globales e interoperables (eAdministración).

o Integrable de forma natural en estrategias SOA corporativas en las que se incluyen tecnologías de terceros.

Las principales funciones de seguridad ofrecidas por el producto para garantizar la seguridad, trazabilidad y auditoría de los procedimientos, tareas y acciones ejecutadas son las siguientes:

o **Autenticación:** Permite la autenticación de los usuarios y aplicaciones remotas. La herramienta utiliza para ello la identificación mediante usuario y contraseña.

o **Trazabilidad:** Almacena información de todos los eventos que ocurren en el sistema permitiendo de ésta forma realizar el seguimiento completo de la ejecución de los procesos.

o **Auditoría:** Asociado a cada evento que se produce en el sistema se almacena información relativa al usuario o aplicación que provocó dicho evento en el sistema.

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

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 para los componentes adicional es de ALC_FLR.1 + ASE_SPD.1 + ASE_REQ.2 + ASE_OBJ.2, según la parte 3 de CC v3.1 r3.

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto –tal y como se recoge en su declaración de seguridad- se limita a satisfacer los requisitos funcionales, según la parte 2 de CC v3.1 r3, siguientes:

REQUISITOS DE CONTROL DE ACCESO

- FDP_ACC.2 Complete Access control
- FDP_ACF.1 Security attribute based access control
- FMT_MSA.3 Static attribute initialization
- FMT_MSA.1 Management of security attributes
- 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.4 Single-use authentication mechanisms

REQUISITOS RELATIVOS A AUDITORÍA DE EVENTOS

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association

REQUISITOS RELATIVOS A CONFIDENCIALIDAD DE LAS CONTRASEÑAS

- FCS_COP.1 Cryptographic operation
- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key destruction

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

Identificación

Producto: PROCESA ENGINE v1.7.3.

Declaración de Seguridad: "Declaración de seguridad para PROCESA Engine v1.7.3", Versión 1.6, 15-03-2010.

Perfil de Protección: ninguno.

Nivel de Evaluación: CC v3.1 r3 EAL1+ ALC_FLR.1 + ASE_SPD.1 + ASE_REQ.2 + ASE_OBJ.2.

Política de seguridad

El uso del producto PROCESA ENGINE v1.7.3, 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: 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, incluido el acceso físico.

Política 02: 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 que, en este caso, son aplicaciones cliente de los servicios del TOE. Ninguna aplicación podrá acceder al sistema sin acreditarse previamente.

Asimismo, en el momento en el que una aplicación sea dada 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.
El propietario del TOE se asegurará igualmente de que existan procedimientos apropiados para asegurar la destrucción de los datos de autenticación, así como la

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

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 aplicaciones clientes del TOE.

Política 03: Configuración segura de conexiones externas del TOE

Todas las conexiones externas que necesite el TOE han de ser configuradas siempre de tal manera que se garantice la seguridad de las mismas. Por ejemplo, en el caso del LDAP, la conexión se realizará basada en SSL.

Política 04: Revisión de auditorías

Existirá un auditor interno del TOE, diferente del administrador del sistema, que será el encargado de revisar periódicamente el archivo de auditoría. 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.

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.

Hipótesis de uso 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.
De la misma manera, se supone que los administradores de la base de datos y LDAP serán confiables, que no otorgará permisos de acceso indebidos (ni de lectura

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

ni de escritura), así como que mantendrá en secreto los datos de las conexiones establecidas.

Hipótesis de uso 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 de Entorno 01: Entorno seguro y confiable

Se supone que la máquina en la que se instale el producto PROCESA se encuentra correctamente configurada en lo referente al software base, sistema operativo y servidor de aplicaciones, de forma segura y confiable siguiendo las guías y configuraciones seguras en lo referente a su instalación y configuración.

También se supone que el acceso “físico” a la máquina en la que se instale el producto PROCESA está restringido al usuario (o usuarios) administradores. Se supone que este usuario respetará la seguridad y confidencialidad de los datos sensibles que presentes en la máquina (configuración, auditorías…).

Hipótesis de Entorno 02: Conexión entidades externas segura

La interconexión entre el motor de ejecución de procesos PROCESA Engine y las entidades externas se realizará de forma segura y confiable garantizando la integridad de la información intercambiada entre ambas partes.

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 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.

Amenaza cubierta:

Amenaza 01: Violación de la confidencialidad de las contraseñas almacenadas en base de datos o ficheros de configuración

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

Un agente externo podría acceder a las contraseñas almacenadas en base de datos o ficheros de configuración y podría recuperar información de acceso a las fuentes de datos de la aplicación.

Amenaza 02: Violación de la integridad en la gestión de roles de proceso

Un agente externo podría modificar sin autorización la asociación de usuarios, grupos o perfiles con roles de proceso si no se controlase el acceso a los servicios de gestión de roles, de modo que, sólo los usuarios autorizados pueden acceder a dichos servicios.

Amenaza 03: Violación de la integridad en la gestión del ciclo de vida de los procesos

Un agente externo podría realizar sin autorización la ejecución, parada, suspensión o continuación de procesos desplegados, así como el despliegue o repliegue de procesos dentro del motor de ejecución de procesos, sólo los usuarios autorizados pueden acceder a dichos servicios.

Amenaza 04: Violación de la integridad en la gestión del ciclo de vida de las tareas

Un agente externo podría realizar sin autorización la ejecución, parada, suspensión o continuación de tareas asociadas a los procesos desplegados dentro del motor de ejecución de procesos, sólo los usuarios autorizados pueden acceder a dichos servicios.

Amenaza 05: Violación de la integridad de los servicios de acceso a datos

Un agente externo podría realizar sin autorización la ejecución de los servicios que acceden a los datos manejados por los procesos de forma que pudiera crear, alterar, borrar o consultar información de los procesos sin autorización.

Amenaza 06: Violación de la integridad de los servicios de administración

Un agente externo podría realizar sin autorización la ejecución de los servicios de administración de forma que pudiera crear, alterar, borrar o consultar información de los parámetros de configuración del motor de ejecución de procesos sin autorización.

Amenaza 07: Violación de la integridad de los servicios de gestión documental

Un agente externo podría realizar sin autorización la ejecución de los servicios de gestión documental de forma que pudiera crear, alterar, borrar o consultar documentos asociados a los procesos que se encuentran en ejecución.

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

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: Garantizar el entorno seguro y confiable

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

Objetivo entorno 02: Garantizar la conexión a entidades externas segura

El entorno operacional del TOE (LDAP) debe asegurar que las conexiones sean seguras a través del uso de cifrado y autenticación en las comunicaciones.

Objetivo entorno 03: Revisión de auditorías

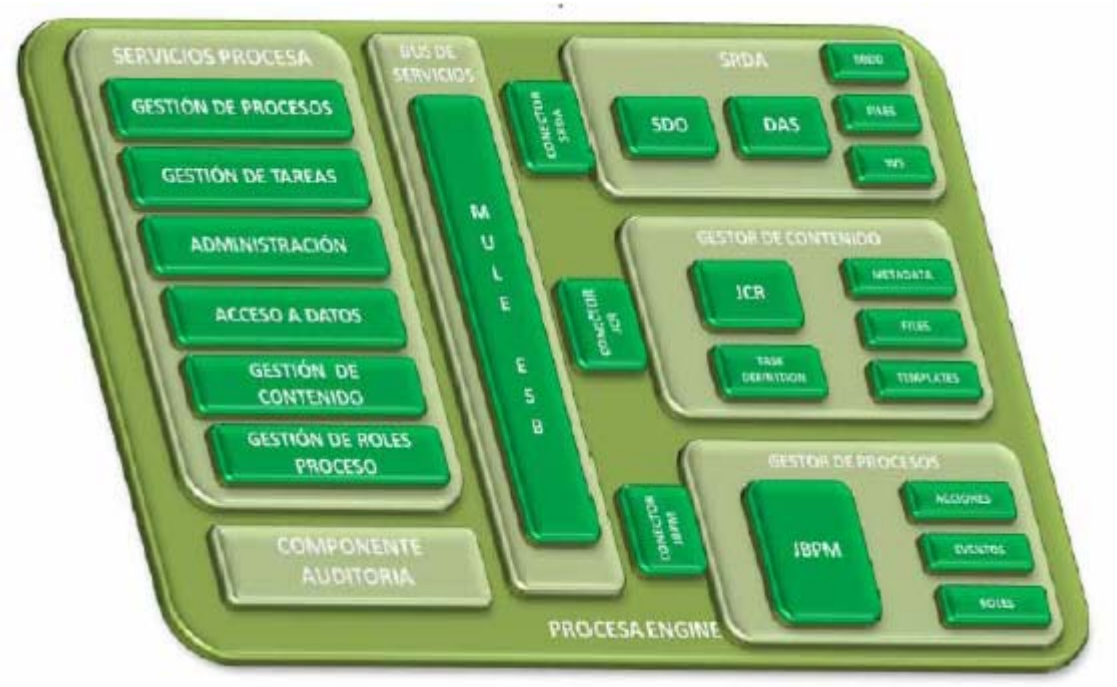
El entorno operacional del TOE debe garantizar la realización de auditorías periódicas que permitan la detección de posibles intentos de violación al TOE, para de esta forma poder tomar las medidas oportunas, definidas por el propietario del TOE, en el caso de que dichos intentos sean identificados.

Arquitectura

Arquitectura Lógica:

EL TOE se corresponde con el módulo “PROCESA ENGINE” cuyos componentes se detallan en la siguiente figura:

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



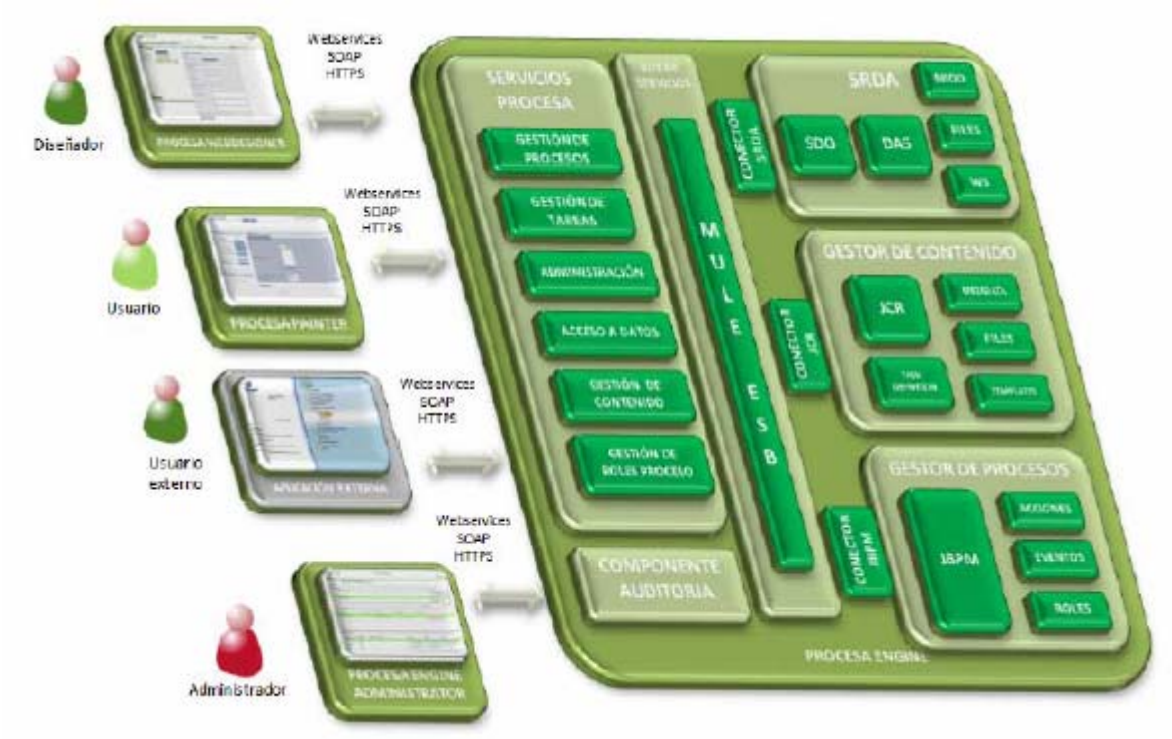
Todos los componentes que componen el módulo PROCESA Engine han sido objeto de evaluación, siendo los componentes denominados **Componente Auditoria** y **Servicios PROCESA (**Servicios del TOE) el interfaz exterior dado que se tratan de los componentes que participan en el acceso a las funcionalidades expuestas por el motor de ejecución de procesos.

Los Servicios del TOE que han sido objeto de evaluación son:

- Servicios de gestión del ciclo de vida de los procesos.
- Servicios de gestión del ciclo de vida de las tareas.
- Servicios de administración
- Servicios de gestión del acceso a datos.
- Servicios de gestión de contenido.
- Servicios de gestión de roles de proceso.

El entorno lógico operacional se describe en la siguiente figura:

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



En esta arquitectura se diferencian dos casos, dependiendo de quién invoca los servicios del TOE. Estos son los siguientes:

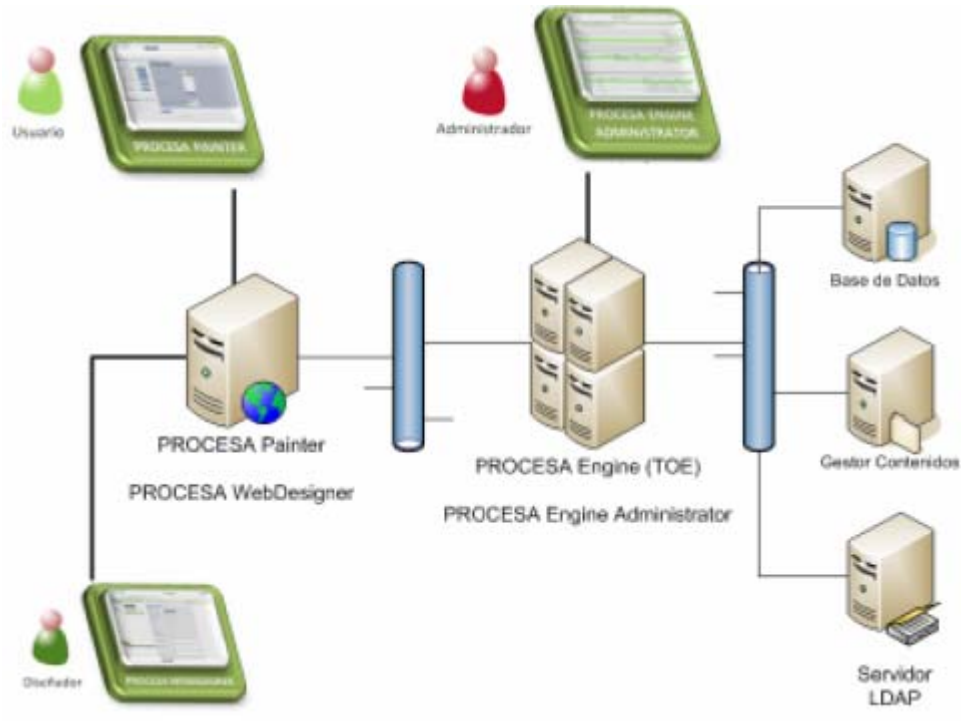
o **Administrador del sistema:** Para configurar el TOE, el administrador del sistema utiliza el módulo PROCESA Engine Administrator. En la configuración evaluada, la comunicación entre este tipo de usuario y la consola de administración se realiza mediante el protocolo HTTPS. El módulo PROCESA Engine Administrator utiliza siempre los servicios de administración del TOE por lo que se le puede considerar como una aplicación externa más con los mismos requisitos de identificación y seguridad que el resto de las aplicaciones externas.

o **Aplicaciones externas:** Las aplicaciones externas, así como el resto de los módulos que componen PROCESA, pueden interactuar con el Servicio del TOE, pero no con la consola de administración. En la configuración evaluada, los servicios del TOE están desplegados como servicios Web y las invocaciones se realizan vía HTTPS encapsulando mensajes SOAP en formato XML y haciendo uso de las cabeceras de seguridad de servicios Web (UsernameToken y timestamp).

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

Arquitectura Física:

Desde un punto de vista físico, el TOE se aloja en un máquina que se integra en una infraestructura que se detalla en la siguientes figura:



Los requisitos software y hardware, se indican a continuación. Estos elementos no forman parte del TOE:

• **Servidor de aplicaciones**. El servidor de aplicaciones ha de soportar una máquina virtual Java J2SE 1.5.0. ó superior. Servidor Aplicaciones compatible J2EE 1.4 o superior (JBoss 4.2.X o superior, Weblogic 9 o superior, Websphere 6.1 o superior, OAS 10g o superior) con mínimo 2 procesadores y 2GB RAM.

• **Servidor de portal**. El servidor de portales ha de soportar una máquina virtual Java J2SE 1.5.0. ó superior. Servidor Portal compatible con el estándar JSR-168 (JBoss Portal 2.6.X +, Weblogic Portal 9.2+, Websphere Portal 6.1+, Oracle Portal 10g+) con mínimo 2 procesadores y 2GB RAM.

• **Servidor base de datos**. El servidor de base de datos ha de tener

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

disponible un driver de tipo JDBC. Entre otros puede ser Oracle 9i,10g,11g . SQLServer 2000, 2005. MySQL 5.x. DB2 8 o superior.

• **Sistema operativo**. El sistema operativo de los equipos puede ser cualquiera sobre el que se puedan instalar los servidores de aplicaciones anteriormente descritos.

• **Java Runtime Enviroment** J2RE 1.5.0 o superior.

• **Servidor LDAP**. Como servidor LDAP se puede utilizar cualquiera que soporte la especificación LDAP v3.

• **Gestor de contenido**. PROCESA utiliza un gestor de contenido para almacenar los documentos asociados a los procesos que se ejecutan dentro del motor de ejecución de procesos (PROCESA Engine). El gestor de contenidos tiene que soportar el estándar JSR170.

• **Navegadores:**
o Microsoft Internet Explorer v6.0 Service Pack 2 o superior.
o Netscape Comunicator v6 o superior.
o Mozilla v4.1 o superior.
o Firefox 3.0.x o superior.

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 PROCESA Engine v1.7.3", Versión 1.6, 15-03-2010.
- Requerimientos certificación EAL1+ Clase AGD – Operational User Guidance v1.4 Marzo 2010.
- Requerimientos certificación EAL1+ Clase AGD – Preparative Procedures v1.5 Marzo 2010.
- JBOSS Guía de configuración segura.
- Red Hat Enterprise Linux 5 Guía de configuración segura.

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

La configuración de PROCESA ENGINE que se ha decidido evaluar es la siguiente:

· Servidor de aplicaciones. JBoss Enterprise Application Platform 5.0.0.

· Servidor de portal. JBoss Portal Server 2.7.2

· Servidor base de datos. Oracle 10.2.0.5

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

· Sistema operativo: Red Hat Enterprise Linux 5

· Java Runtime Enviroment: JRE 1.6u18

· Navegadores: Mozilla Firefox 3.0.11.

· Servidor LDAP: OpenLDAP

· Gestor de contenidos: Jackrabbit 1.4.5

El despliegue de los servicios web del TOE para permitir el acceso a las aplicaciones externas (usuarias) se realizará utilizando la siguiente configuración:

· Conexión mediante protocolo SSL (https)

· SOAP

· Cabeceras de seguridad web (Web Service Secutiry) para la identificación y autenticación de la aplicación externa (UsernameToken + Timestamp)

Resultados de la Evaluación

El TOE PROCESA ENGINE v1.73 ha sido evaluado frente a la declaración de seguridad “Declaración de seguridad para PROCESA Engine v1.7.3”, Versión 1.6, 15-03-2010.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL1+** (aumentado con ALC_FLR.1 + ASE_SPD.1 + ASE_REQ.2 + ASE_OBJ.2) 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 EAL1+, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 r3.

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.

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

- Procesa Engine se despliega sobre un portal JBOSS. Este portal debe estar correctamente configurado de modo que el acceso a él esté controlado y no permita modificaciones que comprometan la seguridad del producto.

- El producto hace uso de diferentes entidades tales como LDAP, Bases de Datos, Gestor de Contenidos, y aplicaciones, que generalmente van a estar instaladas en máquinas distribuidas por una red local de comunicación. Es conveniente que esta red de comunicación sea cerrada, de modo que sólo puedan acceder a ella usuarios confiables.

- La gestión de cada uno de los componentes con los que interacciona Procesa Engine (LDAP, Bases de Datos, Gestor de Contenidos, y aplicaciones) debe ser controlada y protegida convenientemente.

- La máquina física donde está instalado el producto Procesa Engine debe tener un acceso controlado para garantizar la integridad y confidencialidad de la información que reside en ella.

- No existen garantías de la integridad de la auditoria, por lo que es posible realizar modificaciones de los eventos de auditoria sin que éstas sean detectadas.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del TOE PROCESA ENGINE v1.73, 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
IT	Information Technology
OC	Organismo de Certificación
PC	Personal Computer
SW	SoftWare

ENAC CERTIFICACIÓN Nº 45/C-PR110
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:

“Declaración de seguridad para PROCESA Engine v1.7.3”,
Versión 1.6, 15-03-2010.

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