Nuevas características de la versión 5.3.1 de @firma

CARACTERÍSTICAS TÉCNICAS

Tecnológicamente, el cambio más importante en esta versión es la adaptación al uso de @firma con una nueva versión de Jboss, en concreto la versión 4.2.1.GA, y en consecuencia su uso con la revisión de Java Runtime Environment (JRE) 1.5.

Esto permite ejecutar la Plataforma en JRE 1.5 con todas las garantías. Actualmente @firma utiliza la versión de Jboss 4.0.2 y JRE 1.5, aunque sólo está certificada para la JRE 1.4.2.

Este cambio tecnológico proporciona una mayor estabilidad a la plataforma, así como un mejor rendimiento.

En concreto:

• Debido a la migración a JDK 1.5 y a JBOSS 4.2.1.GA, se han actualizado gran parte de las librerías a las nuevas versiones.
• Se suprime el procesado de log al resultar innecesario ya que los mensajes se procesan en tiempo real.
• Se actualizan los scripts SQL debido principalmente a los cambios introducidos en auditoría.
• Se mejora el gestor de exportación de políticas pudiendo escoger la versión de la plataforma destino en la que se realizará la importación.
• Se controla la identificación del usuario tanto en la administración como en auditoría, gestionando el número de reintentos y el establecimiento de la contraseña.
• Se han añadido botones de ayuda en los módulos de Administración y Auditoría. Esta ayuda consiste en una página HTML con los manuales respectivos de Administración y Auditoría.
• Se incorpora la posibilidad de establecer el proxy a usar en las conexiones externas que realice la plataforma.
• Se adapta el mapeo de los certificados para contemplar el tratamiento de los campos multivaluados.
• Se actualizan y mejoran los esquemas de los servicios web.
• Se añaden trazas de log para detectar si una petición OCSP viene firmada o no.
• Categorizado a “info” las trazas de búsqueda de la aplicación a partir del certificado firmante.

CARACTERÍSTICAS FUNCIONALES RESUMIDAS

A continuación se desglosan las características principales de cada uno de los módulos funcionales que componen la Plataforma:

1. **Módulo de Firma.**

- Se añaden nuevos formatos de firma: en formato ODF (Open Document Format), así como la firma de PDF.
- Validación de los nuevos formatos de firma: ODF y PDF.
- Creación de servicios de firma y verificación de las mismas según las especificaciones OASIS-DSS.
- Nuevos algoritmos de firma y resúmenes admitidos en firmas basadas en XML.
- Eliminar la necesidad de registrar el documento en la Plataforma para firmas de servidor.

Nuevas características de la versión 5.3.1 de @firma

2. **Módulo DSS**

- Creación de este nuevo módulo en @firma para implementar las firmas y verificaciones a tra´ves de las especificaciones OASIS-DSS (en @firma 5.2 y versiones anteriores no se dispone de este módulo ni de estas capacidades).

3. **Módulo de Auditoría**

- Nueva versión del módulo de auditoria para evitar el pesado procesado de logs que se venía haciendo hasta ahora.
- Los mensajes y eventos se tratan ahora en tiempo real de una forma más óptima.

4. **Módulo de Custodia**

- Creación de servicio web para recuperar firmas mediante interfaz OASIS-DSS.
- Optimización en el uso de los campos BLOB en base de datos.

5. **Módulo de Validación**

- Posibilidad de configurar librerías externas para conexiones HTTP y LDAP.
- Validación de firmas XADES-BES y XADES-T v.1.2.2.
- Mejoras funcionales en la validación de certificados y registro en el módulo de auditoría.

6. **Otras mejoras funcionales**

- Mejoras en el mapeo de certificados, añadiendo campos lógicos y mapeo de campos multivaluados.
- Mejoras en el módulo de administración.
- Creación de nuevas alarmas.
- Mejoras con respecto a las desincronizaciones del cluster.
- Optimización de acceso a los almacenes de certificados JKS.

CARACTERÍSTICAS FUNCIONALES DETALLADAS

A continuación se desglosan las características principales de cada uno de los módulos funcionales que componen la Plataforma:

1. Módulo de Firma.

o Se añaden nuevos formatos de firma: ODF (Documentos OpenOffice) y PDF.

o Se crea interfaz WS de firma/multifirma servidor siguiendo las especificaciones OASIS – DSS.

o Para firmas en formatos XML se añade la posibilidad de generar firmas de servidor simples en modos enveloping, enveloped y detached mediante interfaz OASIS-DSS.

o Se añade interfaz WS para el registro de firma en la plataforma (similar al servicio de firma en 2 Fases) basadas en las especificaciones OASIS – DSS.

o Se añade la validación de firmas ODF (Documentos OpenOffice) y PDF.

o Se ha añadido servicio de verificación firma mediante interfaz OASIS – DSS, este servicio permite también la realización de procesos de upgrade de firmas registradas o generadas externamente.

Nuevas características de la versión 5.3.1 de @firma

o Se ha añadido los algoritmos de firmas MD5WithRSA, SHA256WithRSA, SHA512WithRSA y los de resumen MD5, SHA256, SHA384 y SHA512 para firmas en formato XML.

o Se ha modificado el servicio de Firma de Servidor para poder incluir el documento a firmar en el mismo mensaje de petición.

o Se incluye un detector de formatos de firma.

o Se añade SMIME y los formatos avanzados a los formatos de entrada válidos para @firma 5.3 (EPES, C, X1, X2, XL, XL1, XL2, A). (NO implementa la funcionalidad de firma de estos formatos, solo acepta el tipo.)

o Se devuelve el formato de firma y el justificante para la firma en 2 fases.

o Para aquellos servicios de actualización de firma que tienen como parámetro de entrada un firmante objetivo se devuelve un mensaje de error en el caso de no encontrar el certificado enviado dentro de la firma.

2. **Módulo DSS**

o Modificación del servicio de firma en 2 fases mediante interfaz DSS para que no realice proceso de upgrade sobre la firma.

o Incluido en los mensaje de respuesta del servicio de Upgrade los componentes "dss:SignatureType" y "ades:SignatureForm" para indicar el formato de la firma generada.

o Incluido identificadores "Warning" para componente "dss:ResultMajor" y "IncompleteUpgradeOperation" para componente "dss:ResultMinor".

3. **Módulo de Auditoría**

o Remodelación total del módulo de estadísticas.

o Se añade una herramienta de extracción de datos estadísticos programable mediante la herramienta "cron" de Solaris.

o Modificaciones en el módulo de registro de eventos:

- Tratamiento de mensajes en tiempo real en nuevo modelo de datos.
- Desarrollo de tarea de respaldo para asegurar la persistencia de los mensajes en caso de problemas con BBDD.

4. **Módulo de Custodia**

o Se añade Servicio Web para obtener una firma custodiada mediante interfaz OASIS-DSS.

o Se modifica levemente la estructura de la BBDD para poder relacionar identificadores de transacción con identificadores de secuencia.

o Se modifica el uso/manejo de los campos tipo Blob mejorando su rendimiento.

5. **Módulo de Validación**

o Se permite la parametrización del uso de las librerías externas para las conexiones http y LDAP. De esta forma, se permite la elección de la librería concreta que implementa estas funcionalidades.

o Se añaden mensajes de inicio y fin para las tareas de validación y revocación, y se deja preparado para que sea obligatorio incluirlos para cualquier nueva tarea.

o Añadida validación de firmas XAdES-BES y XAdES-T v1.2.2.

o Se ha quitado la validación de countersignatures frente a firmas XADES ya que sólo funcionaban para 1.3.2.

Nuevas características de la versión 5.3.1 de @firma

o Modificado el módulo de validación de certificados para que registre información de auditoría asociada a las evidencias del estado de revocación.

o Incluida funcionalidad de identificación de peticiones OCSP a partir del certificado firmante.

6. Otras mejoras

o Se añade un nuevo tipo de mapeo de campos lógicos, Expresión Regular que afecta al alta, modificación y visualización de los mapeos de campos lógicos de un certificado.
(Ahora se puede mapear el NIF desde el asunto del certificado, p.e. ANCERT).

o Se pueden exportar los datos obtenidos en las estadísticas a un documento PDF.

o Se ha modificado el interfaz gráfico de usuario del módulo de auditoría para que contemple los cambios realizados en el modulo de estadística.

o Se mejora la seguridad del módulo de administración, restringiendo ciertas acciones críticas en la administración, solicitando de nuevo la contraseña del usuario actual y especificando una política de validación de contraseñas.

o Se mejora la interfaz de usuario de la administración, incorporando indicadores de ejecución y ayudas contextuales.

o Nueva Alarma 27: Se lanza la alarma en caso de experimentarse problemas al obtener el contenido de algún almacén de certificados.

o Se soluciona la desincronización del cluster haciendo más eficiente los algoritmos encargados de resolver los posibles eventos e incluyendo dos nuevas alarmas: 28 y 29.

o Se permite configurar manualmente la disponibilidad de una TSA.

o Se comprueba, previa inserción de cualquier certificado en un almacén, si éste está caducado o aún no es válido (excepto para el almacén de tipos de certificados).

o Incorporación de un nuevo proveedor de gestión de keystores JCE-KS que mejora el acceso a los almacenes de claves JKS, eliminando algunos problemas relacionados con los tiempos de carga de los certificados.

o Se añade soporte para campos multivaluados en certificados digitales X.509.

o Se elimina el chequeo de parámetros para los servicios de administración delegada.