



Plataforma @firma

Novedades de la versión 5.3.1 del núcleo de la plataforma

Versión: v01r003

Fecha: 27/07/2010

Queda prohibido cualquier tipo de explotación y, en particular, la reproducción, distribución, comunicación pública y/o transformación, total o parcial, por cualquier medio, de este documento sin el previo consentimiento expreso y por escrito de la Junta de Andalucía.

| | | | |
|---|---|--|---|
|  | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

HOJA DE CONTROL

| | | | |
|---------------------------|---|-------------------------|------------|
| Título | Novedades de la versión 5.3.1 del núcleo de la plataforma | | |
| Entregable | Novedades de la versión 5.3.1 del núcleo de la plataforma | | |
| Nombre del Fichero | Novedades_afirma_5_3_1_v01r003 | | |
| Autor | José Ignacio Cortés Santos <josei.cortes@juntadeandalucia.es> (Servicio de Coordinación de Administración Electrónica) | | |
| Versión/Edición | v01r003 | Fecha Versión | 27/07/2010 |
| Aprobado por | | Fecha Aprobación | 27/07/210 |

REGISTRO DE CAMBIOS

| Versión | Causa del Cambio | Responsable del Cambio | Área | Fecha del Cambio |
|---------|------------------------|------------------------|------|------------------|
| v01r00 | Versión inicial | SCAE | - | 20/07/2010 |
| v01r001 | Revisión del documento | SCAE | - | 21/07/2010 |
| V01r002 | Revisión del documento | SCAE | - | 23/07/2010 |
| V01r003 | Revisión del documento | SCAE | - | 27/07/2010 |

CONTROL DE DISTRIBUCIÓN

| Nombre y Apellidos | Cargo | Área | Nº Copias |
|--------------------------|------------------|---------|-----------|
| Manuel Perera Domínguez | Jefe de Servicio | SCAE | 1 |
| Juan José López Portillo | - | TELVENT | 1 |

Este documento se publicará en la web de soporte de administración electrónica de la Junta de Andalucía, en la dirección <https://ws024.juntadeandalucia.es>

| | | | |
|---|---|--|---|
|  | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

1. 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 Development Kit (JDK) 1.5. Hasta la fecha el entorno de ejecución habitual de la plataforma era Jboss 4.0.2.

Entre las características más destacadas de la versión 4.2.1. GA de JBoss destacan la incorporación de JDK 1.5 en lugar de la versión JDK 1.4.2 y una mejor gestión de los nodos que componen los clusters.

La información acerca de los cambios incorporados en esta versión de JBoss está disponible en la siguiente dirección: http://sourceforge.net/project/shownotes.php?release_id=523619

Este cambio tecnológico proporciona una mayor estabilidad a la plataforma, así como un mejor rendimiento, especialmente en las librerías que controlan el cluster. 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.
- 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.
- Se categorizan como “info” las trazas de búsqueda de la aplicación a partir del certificado firmante.

| | | | |
|---|---|--|---|
|  | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

2. CARACTERÍSTICAS FUNCIONALES RESUMIDAS

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

Módulo de Firma

- Se añaden nuevos formatos de firma de servidor: formato ODF (Open Document Format), así como la firma de PDF.
- Se incorpora la validación de firmas en formato 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, enviándose el documento a firmar en la misma petición de firma lo que permite realizar una firma de servidor en una sola fase.

Módulo DSS

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

Módulo de Auditoría

- Nueva versión del módulo de auditoría para evitar el pesado procesado de logs habitual hasta ahora.
- Los mensajes y eventos se tratan ahora en tiempo real de una forma más actualizada. También se dispone de una tarea de respaldo para asegurar la persistencia de los datos en caso de problemas con la base de datos.

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.

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.

| | | | |
|---|---|--|---|
|  | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

Otras mejoras

- Mejoras en el “mapeo” de certificados, añadiendo campos lógicos y “mapeo” de campos multivaluados. Ahora se pueden utilizar expresiones regulares para el “mapeo” de certificados .
- Supresión de la tarea periódica de procesado de logs.
- Mejoras en el módulo de Administración.
- Creación de nuevas alarmas.
- Mejoras con respecto a las posibles desincronizaciones del cluster.
- Optimización de acceso a los almacenes de certificados JKS.
- Mejoras en la importación y exportación de políticas.

3. CARACTERÍSTICAS FUNCIONALES DETALLADAS

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

Módulo de Firma

- Se añaden nuevos formatos de firma: ODF (Open Document Format) y PDF.
- Se crea una interfaz WS de firma /multifirma de servidor siguiendo las especificaciones OASIS-DSS.
- Para firmas en formatos XML, se añade la posibilidad de generar firmar de servidor simples en modos "enveloping", "enveloped" y "detached" mediante interfaz OASIS-DSS.
- Se añade una interfaz WS para el registro de la firma en la Plataforma (similar al servicio de firma en dos fases) basada en las especificaciones OASIS – DSS.
- Se añade la validación de firmas ODF y PDF.
- Se ha añadido un servicio de verificación de firma mediante interfaz OASIS – DSS. Este servicio permite también la actualización de firmas registradas o generadas externamente a formatos avanzados.
- Se han añadido nuevos algoritmos de firmas: MD5WithRSA, SHA256WithRSA, SHA512WithRSA.
- Se han añadido nuevos algoritmos de hash: MD5, SHA256, SHA384, SHA512 para firmas en formato XML.
- Se ha modificado el servicio de “Firma de Servidor” para poder incluir el documento a firmar en el mismo mensaje de petición.
- Se incluye un detector de formatos de firma.

| | | | |
|---|---|--|---|
|  | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

- Se añade SMIME y los formatos avanzados a los formatos de entrada válidos (EPES, C, X1, X2, XL, XL1, XL2, A).
- Para la firma en 2 fases, se devuelve el justificante de la misma junto con su formato.
- 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.
- Se admite el formato CMS-T para la extensión de @firma.

Módulo DSS

- Modificación del servicio de firma en 2 fases mediante interfaz DSS para que no realice proceso de upgrade sobre la firma.
- Inclusión en los mensajes de respuesta del servicio de Upgrade los componentes “dss:SignatureType” y “ades:SignatureForm” para indicar el formato de la firma generada.
- Inclusión de identificadores “Warning” para componente “dss:ResultMajor” y “IncompleteUpgradeOperation” para componente “dss:ResultMinor”.

Módulo de Auditoría

- Remodelación del módulo de estadísticas.
- Se añade una herramienta de extracción de datos estadísticos programable mediante la herramienta “cron”
- 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 la base de datos.
- Se incluye un nuevo modo de registro de información de auditoría en el cual cada nodo registra su información una vez ha recogido un número determinado de transacciones finalizadas.
- Se incluye dentro del sistema de estadísticas la información correspondiente a los servicios de Custodia.
- Se modifica la forma de nombrar y gestionar el log diario, de forma que ahora el fichero lleva el identificador de secuencia delante, así como su proceso de custodia. En concreto:
 - El fichero diario.log pasa a denominarse {Identificador de transacción}.diario.log. Con este cambio se permite relacionar este fichero con su transacción de firma. En una

| | | | |
|---|---|--|---|
|  <p>JUNTA DE ANDALUCÍA CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA</p> | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

primera ejecución el fichero diario.log existente será renombrado, en caso de no existir se creará uno con el nuevo formato. Una vez firmado el nombre pasa a denominarse {Identificador de transacción}.diario.log.YYYY-MM-DD.

- Una vez firmado el fichero no se incluye el identificador de custodia en el mismo ya que este se incluye en el nombre del fichero.
- Deja de almacenarse el contenido de los ficheros *.diario.log en el sistema de Custodia; únicamente se registra el resumen del mismo mediante los algoritmos SHA-256 y SHA-512. El Administrador de la Plataforma deberá conservar estos ficheros en algún sistema de almacenamiento para asegurar la trazabilidad de las transacciones generadas por la Plataforma. La firma realizada de este fichero sí es registrada en el sistema de Custodia.
- Como consecuencia del punto anterior, se ha eliminado la posibilidad de descargar del diario.log desde la interfaz gráfica “Cliente de Auditoría”.

Módulo de Custodia

- Se añade Servicio Web para obtener una firma custodiada mediante interfaz OASIS-DSS.
- Se modifica levemente la estructura de la base de datos para poder relacionar identificadores de transacción con identificadores de secuencia.
- Se modifica el uso de los campos tipo BLOB mejorando su rendimiento.

Módulo de Validación

- 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.
- Se añaden mensajes en los archivos de traza con información de cuándo se inician y finalizan las tareas de validación de los certificados almacenados en la Plataforma y de comprobación del estado de revocación de las cadenas de certificación.
- Añadida validación de firmas XAdES-BES y XAdES-T v1.2.2.
- Modificado el módulo de validación de certificados para que registre información de auditoría asociada a las evidencias del estado de revocación.
- Incluida funcionalidad de identificación de peticiones OCSP a partir del certificado firmante.

| | | | |
|---|---|--|---|
|  <p>JUNTA DE ANDALUCÍA CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA</p> | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

Otras mejoras

- 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. Así, por ejemplo, se podrá “mapear” el NIF desde el asunto del certificado.
- Se pueden exportar los datos obtenidos en las estadísticas a un documento PDF.
- Se ha modificado el interfaz gráfico de usuario del módulo de auditoría para que contemple los cambios realizados en el módulo de estadística.
- 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.
- Se mejora la interfaz de usuario de la administración, incorporando indicadores de ejecución y ayudas contextuales.
- Nueva Alarma 27: Se lanza la alarma en caso de experimentarse problemas al obtener el contenido de algún almacén de certificados del cluster, lo que puede provocar la desincronización de los nodos del cluster.
- Nueva Alarma 28: Se lanza la alarma en caso de que el nodo Master reciba una configuración del cluster con una versión inferior a la local. Esto implica una configuración errónea del cluster que provoca que el nodo Master imponga su configuración al cluster con obligación por parte del resto de nodos de aceptarla para evitar que se desincronicen los nodos.
- Nueva Alarma 29: Se lanza la alarma en caso de que un nodo no haya podido actualizar su configuración local con la recibida del cluster. Esto implica que hasta la siguiente sincronización el nodo afectado no tenga la misma configuración que el resto de nodos que componen el cluster, produciéndose una desincronización.
- Se permite configurar manualmente la disponibilidad de una TSA.
- 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).
- 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.
- Se añade soporte para campos multivaluados en certificados digitales X.509.
- Se elimina el chequeo de parámetros para los servicios de administración delegada.
- Debido a la migración a JBOSS 4.2.1.GA en general y JRE 1.5 en particular, se actualizan gran parte de las librerías utilizadas.

| | | | |
|---|---|--|---|
|  <p>JUNTA DE ANDALUCÍA CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA</p> | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

- Se suprime la tarea de procesado de log al resultar innecesario ya que los mensajes se procesan en tiempo real.
- Se actualizan los scripts SQL debido a los cambios introducidos en el módulo de 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 la 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.
- Se incorpora la posibilidad de establecer un proxy para utilizar 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.
- Se categorizan a “info” las trazas de búsqueda de la aplicación a partir del certificado firmante.
- Se realiza la firma de los mensajes SOAP de respuesta de tipo “Fault”.
- Se modifican las pantallas donde aparece el número de versión de la plataforma, para mostrar la versión 5.3.1.
- Se elimina el desplegable correspondiente al Cliente de Monitorización, y se eliminan las dependencias internas a este mismo.

4. MANTENIMIENTO CORRECTIVO

Además de las nuevas funcionalidades incluidas en esta versión, se han corregido una serie de problemas y errores detectados en la versión anterior de la Plataforma.

- Se ha corregido un error en el proceso de firma en bloques por el que las firmas de servidor que realiza la Plataforma de los documentos implicadas no tenían en cuenta el formato de firma especificado y siempre se realizaban en formato CMS. No obstante, la firma del bloque por parte del usuario mediante el cliente de firma sí realizaba ésta en el formato especificado. Actualmente, las firmas de servidor de una firma en bloque se realizan en el formato solicitado.

| | | | |
|---|---|--|---|
|  <p>JUNTA DE ANDALUCÍA CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA</p> | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

- Se ha modificado el servidor OCSP para que no genere información de auditoría ni estadística en el caso de recibir una petición no autorizada.
- Se modifica el servidor OCSP para que admita la validación de múltiples certificados, sin la restricción de que todos ellos hayan sido emitidos por el mismo PSC.
- Se corrige un comportamiento del OCSP Responder por el cual, no se utilizaba como lista de confianza de certificados de firma de OCSP el almacén de confianza definido a tal efecto.
- Se corrige la respuesta dada en caso de recibir una petición WS sin las credenciales cuando son necesarias.
- Se corrige un error, por el cual al obtener información de ciertas extensiones concretas de un certificado proporcionaba una respuesta incorrecta.
- No se importaba correctamente una configuración que tuviera PSCs sin tipos de certificados declarados.
- Corregido un error detectado en la verificación del hash firmado en firmas CMS con contrafirmas.
- Corregido error al procesar “mapeo” de expresión regular y modificada pantalla "Mostrar Mapeos Tipo de Certificado" para que muestre los “mapeos” de tipo expresión regular.
- Se corrigen algunos comportamientos anómalos del tipo de mapeo “COMPLEJO” con respecto a la búsqueda de caracteres en cadenas.
- Se corrige un comportamiento incorrecto al realizar una búsqueda dentro de una CRL de cierto certificado (proviene de un error de las librerías IAIK).
- Se corrige un error por el que al eliminar cualquier PSC, se eliminaban sus tipos de certificados asociados a las distintas políticas, pero no el propio PSC ni sus PSCs descendentes.
- Corregido error al verificar firmas ASN. 1 con más de un firmante en el que alguno no tenía sello de tiempo.
- Corregido error detectado cuando un fichero XML incluye una contrafirma de distinto formato a la firma original.
- Corregido error que hacía que no apareciera en la Herramienta de Auditoría el servicio “Obtencion de Transacciones por Referencia”.
- Se corrige un mal funcionamiento cuando un certificado presentaba en el subject AltName un OID con valor nulo.
- Ahora se muestra la etiqueta "descripción" al dar de alta un campo lógico.

| | | | |
|---|---|--|---|
|  <p>JUNTA DE ANDALUCÍA CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA</p> | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

- Se corrige un problema al mostrar las direcciones de correo en las alarmas, que provocaba que al introducir comas en el texto no se pudieran seleccionar para eliminar o modificar.
- Se corrige el proceso de upgrade para que eleve un error en el caso de no estar disponible la TSA.
- Se corrige un error detectado al generar firmas de servidor con sello de tiempo por el que no se incluía el identificador de transacción como atributo firmado.
- Sustituido el mensaje "Finalizar Firma Servidor CounterSign" en mensaje de Auditoría para Firma de Usuario.
- Se corrige un error por el que el servicio OCSP no funcionaba adecuadamente en todos los casos. El error proviene de la librería 3.14 de IAIK y anteriores.
- Se solventan problemas en la validación de contrafirmas en formato CMS, provocados por la tarea de verificación de los hashes.
- Solucionados problemas en la administración, relacionados con el alta de información adicional de PSCs (URL de la DPC y Domicilio Social).
- Se corrige un problema en la correlación del almacenamiento de las peticiones/respuestas custodiadas con la información de auditoría que ha generado el sistema para dichas peticiones.
- Corregido un problema en el tratamiento de los "saltos de carro" entre elementos en las peticiones WS-XML, por parte del servicio de validación de parámetros incorporado en la versión 5.3.
- Se habilita la firma del identificador de transacción para firmas con sello de tiempo.
- Se "escapan" las entradas de los campos de alias de certificados y de las expresiones regulares de la administración para evitar problemas de interpretación con ciertos caracteres.
- Se elimina el almacenamiento de la configuración en el cluster cada vez que se consultara un método de validación por políticas, ya que resultaba innecesario.
- Se corrige el comportamiento de los mapeos de certificados al encontrarse con el carácter especial '\.
- Se elimina el lanzamiento de la alarma 008 en caso de una petición OCSP con un prestador no dado de alta en la plataforma. En su lugar se lanza una excepción.
- Incluido atributo xml:lang en componente dss:ResultMessage.
- Siguiendo las especificaciones DSS "Profile for Comprehensive Multi-signature Verification Reports" se ha incluido el componente "vr:DigestAlgAndValue" como hijo del elemento "vr:SignatureIdentifier" en la respuesta de verificación de firma.
- Corregido error al tratar de sincronizar la caché de certificados OCSP en el cluster.

| | | | |
|---|---|--|---|
|  <p>JUNTA DE ANDALUCÍA CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA</p> | <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p> <p>Servicio de Coordinación de Administración Electrónica</p> | <p>Novedades de la versión 5.3.1 del núcleo de la plataforma</p> |  |
|---|---|--|---|

- Corregido resultado de validación OCSP certificado no soportado por la política en casos de validación de certificados intermedios (válidos).
- Corregido error al obtener los registros almacenados en la tabla “FirmaAux” del esquema de Auditoría en el caso de consulta para un determinado identificador de secuencia que no tenga asociada información en la tabla “CertificadoAux”.
- Modificado el modo 0 de registro de evento de Auditoría para corregir error de colapso de conexiones de bases de datos.
- Corregido error al validar firma XAdES-T v.1.1.1 en el que se devolvía una respuesta de error “Es necesario indicar para la obtención de información de Firmas XAdES 1.1.1, en el contexto del Core Criptográfico, el documento que contiene la firma”.
- Corregido error detectado al eliminar un Tipo de Certificado en el Módulo de Gestión de PSC de la Herramienta de Administración; se eliminaba el Tipo de Certificado de la Política pero su emisor permanecía en la misma aunque no tuviera Tipo de Certificados admitidos o alguna de sus CA hijas.
- Se corrige un mal comportamiento en el “mapeo” lógico del anagrama fiscal. En la herramienta de administración se indica correctamente cuál es el campo para rellenar con el nombre, cuál el apellido 1 y cuál el apellido 2.
- Se corrige un error por el cual si los elementos MensajeEntrada e InputMessage vienen con un prefijo delante (pej <ns2:MensajeEntrada>) la plataforma devuelve un error con el mensaje "el fichero xml de entrada no está bien formado".
- Se eliminan “saltos de línea” en el mensaje para el registro de evento de error durante una validación de firma CADES-BES.
- Se mejora la gestión de hilos para que finalice correctamente la transacción que lanza la tarea de custodia sin necesidad de esperar a que esta termine.