Liberación SISTRA: módulo Firma

Código: DSI-LIBSISTRA-FIRMA

HOJA DE CONTROL DE DOCUMENTO

DOCUMENTO/ARCHIVO

Título: Liberación SISTRA: módulo Firma	Nombre Archivo/s: **SISTRA-PLUGINFIRMA-001.doc**
Código: **DSI-LIBSISTRA-FIRMA**	Soporte lógico: **Word**
Fecha: 09/03/2009	
Versión: **1**	

REGISTRO DE CAMBIOS

Versión	Páginas	Motivo del cambio
1	9	Creación del Documento

DISTRIBUCIÓN DEL DOCUMENTO

Nombre	Personal

CONTROL DEL DOCUMENTO

PREPARADO	REVISADO/ APROBADO	ACEPTADO	ACEPTADO
Rafael Sanz	José Vicente Juan Pérez	**Jeroni Navarrete**	**Bernat Alberti**

Cumplimentar con el nombre, la firma y la fecha ***Sólo para clientes***

INDICE

1. Objeto

El objeto de este documento es definir las acciones a realizar para permitir que la plataforma SISTRA permita el uso de las implementaciones de firma de la DGTIC y de @firma.

2. Módulos de firma

2.1. Firma DGTIC

Solución basada en un API java de firma que oculta los detalles de implementación de la firma digital.

Para realizar la firma en clientes Web se ha de construir un applet que utilice esta API de forma que:

- muestre en un desplegable los certificados instalados
- muestra una caja de texto para introducir el pin
- botón que inicia el proceso de firma

Para el sellado de firmas digitales en la DGTIC se ha de emplear el sistema de custodia de documentos firmados de la DGTIC (en proceso de puesta en producción). Todos los documentos firmados se almacenarán en este sistema de custodia.

2.2. @Firma

Proporciona dos tipos de servicios según el cliente:

- Cliente Web: solución basada en applet (applet instalador + applet firmador + ficheros javascripts). En la página web no aparecería el applet y cuando se pulsara el botón de firma aparecerá una ventana para seleccionar el certificado y que posteriormente solicitará el pin.
- Servidor aplicaciones: se ofrecen los siguientes servicios web para aplicaciones. Para utilizar estos servicios la aplicación debe estar registrada y se debe indicar en cada invocación al servicio web el id de aplicación. Los servicios ofertados son:
    - firmado digital (firma delegada: se registra certificado aplicación en servidor @firma y se le indica que se firme con ese certificado)
    - verificación de firmas
    - consulta datos certificados

La operación de añadir un sello de tiempo a una firma digital se realiza desde la plataforma de @FIRMA, es decir, desde el servidor nunca desde el cliente. Por tanto, solamente podemos generar firmas con sello de tiempo si utilizamos el servicio FirmaServidor. El formato en el que se devuelve la firma se denomina XAdES-T

3. Operativa de firma en la plataforma SISTRA

3.1. Firma en cliente web

En el frontal web se realizan los siguientes procesos:

- firma de formularios y anexos
- firma de trámites
- firma de acuses de recibo

3.2. Firma en servidor

En la parte servidor se han de realizar los siguientes procesos:

- validación de firmas generadas en cliente
- firma de justificantes de registro por el api de registro telemático
- almacenamiento de las firmas en el REDOSE
- generación de un archivo que almacena una firma digital para que se lo pueda descargar el ciudadano

4. Solución propuesta

4.1. Firma en cliente web

En el frontal web se distinguirán dos modos de funcionamiento (DGTIC ó @firma) de forma que se configurará la página según este modo, ya que la operativa y el aspecto visual difiere en cada caso.

Elementos a configurar dependiendo el modo de funcionamiento:

- carga applets / js
- textos explicativos de firma

Este desarrollo se llevará dentro de las tareas de la liberación de la plataforma desarrolladas por la DGTIC.

4.2. Firma en servidor

En la parte servidor se define un interfaz genérico de firma para realizar las operaciones de servidor. Para ello se deberán definir dos implementaciones o plugins para cada modo de firma.

El plugin para la firma DGTIC será implementada dentro de las tareas de la liberación de la plataforma desarrolladas por la DGTIC.

El plugin para la firma con @Firma deberá ser implementada por alguno de los organismos que lo utilicen.

5. Interfaz plugin de firma

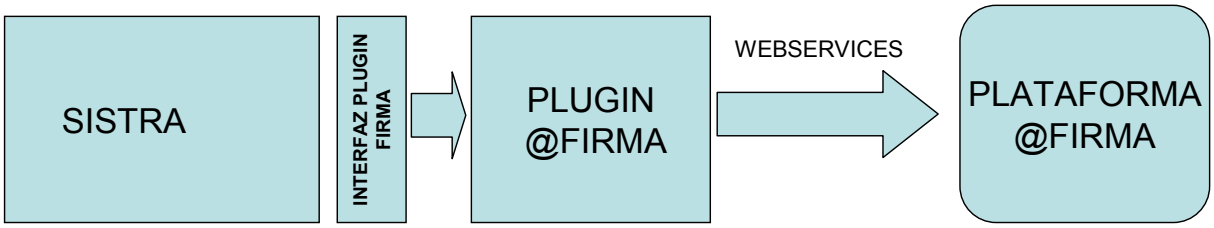
El interfaz del plugin de firma para las operaciones de firma en servidor es el siguiente:

Método	Descripción	Parámetros	Resultado
getProveedor	Obtiene proveedor de firma	No tiene	DGTIC ó @FIRMA
Firmar	Realiza una firma digital	datos: datos a firmar nombreCertificado: certificado a utilizar parámetros: parámetros específicos proveedor	FirmaIntf: firma digital
verificarFirma	Verifica una firma	datos: datos firmados FirmaIntf: firma digital	true / false
parseFirmaFromHtmlForm	Crea una firma a partir de la cadena de datos que se recibe desde formulario HTML	signatureHtmlForm: Cadena de firma recibida desde el formulario HTML	FirmaIntf: firma digital
parseFirmaFromBytes	Crea una firma a partir de un array de bytes	firma: bytes con el contenido de la firma formatoFirma: formato de la firma	FirmaIntf: firma digital
parseFirmaToBytes	Serializa la firma en un byte array para almacenar en BBDD	Firma: datos de la firma	Byte array con la firma
parseFirmaToFile	Serializa la firma digital en un fichero descargable por el usuario	datosFirmados: datos firmados	FicheroFirma: datos del fichero generado

6. Implementación plugin de firma

6.1. Plugin @firma

El plugin de @firma deberá implementar internamente las llamadas necesarias a los webservices de la plataforma de @firma para dar soporte a las operaciones definidas.



La implementación de @firma permite el uso de varios formatos de firma (CMS, XMLDsig, CADES, XADES, etc.). Por ello se almacenará en el RDS junto a una firma el formato de la misma, para luego poder recuperarla correctamente (método parseFirmaFromBytes).

Se aconseja que para la firma en servidor (la ofrecida por el plugin) se utilice un formato que genere un sellado de la firma (p.e. XAdES-T).

En la parte cliente al no poderse generar sello de tiempo se utilizará en principio el formato CMS (por defecto en @firma). Los formatos disponibles en cliente son CMS (por defecto) y CADES-BES.