Alliberament SISTRA: Mòdul de signatura

Codi: DSI-LIBSISTRA-SIGNATURA

FULL DE CONTROL DE DOCUMENT

DOCUMENT/ARXIU

Títol: Alliberament SISTRA: Mòdul de signatura	Nom arxiu/s: **SISTRA-PLUGINSIGNATURA**
Codi: **DSI-LIBSISTRA-SIGNATURA**	Suport lògic: **Word**
Data: setembre 2010	
Versió: **2**	

REGISTRE DE CANVIS

Versió	Pàgines	Motiu del canvi
1	9	Creació del document.
2	9	Separació entre el format intern a l'hora d'emmagatzemar/recuperar signatures de BD i el format extern en l'API de servei web.

DISTRIBUCIÓ DEL DOCUMENT

Nom	Personal

CONTROL DEL DOCUMENT

PREPARAT	REVISAT/APROVAT	ACCEPTAT	ACCEPTAT
Rafael Sanz	José Vicente Juan Pérez	**Jeroni Navarrete**	**Bernat Albertí**

Emplenau-ho amb el nom, la signatura i la data.

Només per a clients

ÍNDEX

1. Objecte

L'objecte d'aquest document és definir les accions que s'han de dur a terme perquè la plataforma SISTRA permeti l'ús de les implementacions de signatura de la DGIDT i d'@firma.

2. Mòduls de signatura

2.1. Signatura DGIDT

Solució basada en una API java de signatura que oculta els detalls d'implementació de la signatura digital.

Per realitzar la signatura en clients web, s'ha de construir una miniaplicació que utilitzi aquesta API de manera que:

- mostri en un desplegable els certificats instal·lats.
- mostra una caixa de text per introduir el pin.
- botó que inicia el procés de signatura.

Per segellar les signatures digitals a la DGIDT, cal emprar el sistema de custòdia de documents signats de la DGIDT (en procés de posada en producció). Tots els documents signats s'emmagatzemen en aquest sistema de custòdia.

2.2. @firma

Proporciona dos tipus de serveis segons el client:

- Client web: solució basada en applet (applet instal·lador + applet signador + fitxers javascripts). A la pàgina web no apareix l'applet i, quan es pitja el botó de signatura, apareix una finestra per seleccionar el certificat i, posteriorment, sol·licita el pin.
- Servidor d'aplicacions: s'ofereixen els serveis web per a aplicacions següents. Per utilitzar aquest serveis d'aplicacions cal que estiguin registrades i cal indicar en cada invocació al serveis web l'ID d'aplicació. Els serveis que s'ofereixen són:
    - signatura digital (signatura delegada: es registra certificat aplicació en servidor @firma i se li indica que se signi amb aquell certificat).
    - verificació de signatures.
    - consulta dades certificats.

L'operació d'afegir un segell de temps a una signatura digital es du a terme des de la plataforma d'@firma, és a dir, des del servidor, mai des del client. Per tant, només podem generar signatures amb segell de temps si empram el servei FirmaServidor. El format en el qual es torna la signatura es denomina XAdES-T.

3. Operativa de signatura a la plataforma SISTRA

3.1. Signatura en client web

En el frontal web es duen a terme els processos següents:

- Signatura de formularis i annexos
- Signatura de tràmits
- Signatura de justificants de recepció

3.2. Signatura en servidor

A la part servidor s'han de dur a terme els processos següents:

- Validació de signatures generades en client.
- Signatura de justificants de registre per l'API de registre telemàtic.
- Emmagatzematge de les signatures en el REDOSE.
- Generació d'un arxiu que emmagatzema una signatura digital perquè el ciutadà el pugui descarregar.

4. Solució proposada

4.1. Signatura en client web

En el frontal web es distingiran dos modes de funcionament (DGIDT o @firma) de manera que es configurarà la pàgina segons aquest mode, ja que l'operativa i l'aspecte visual difereix en cada cas.

Elements que cal configurar depenent del mode de funcionament:

- Càrrega d'applets / js
- Textos explicatius de signatura

Aquest desenvolupament es durà a terme dins de les tasques de l'alliberament de la plataforma desenvolupades per la DGIDT.

4.2. Signatura en servidor

A la part servidor, es defineix una interfície genèrica de signatura per dur a terme les operacions de servidor. Per això, s'han de definir dues implementacions o plugins per a cada mode de signatura.

El plugin per a la signatura DGIDT ha de ser implementat dins de les tasques de l'alliberament de la plataforma desenvolupades per la DGIDT.

El plugin per a la signatura amb @firma ha ser implementat per algun dels organismes que l'utilitzin.

5. Interfície plugin de signatura

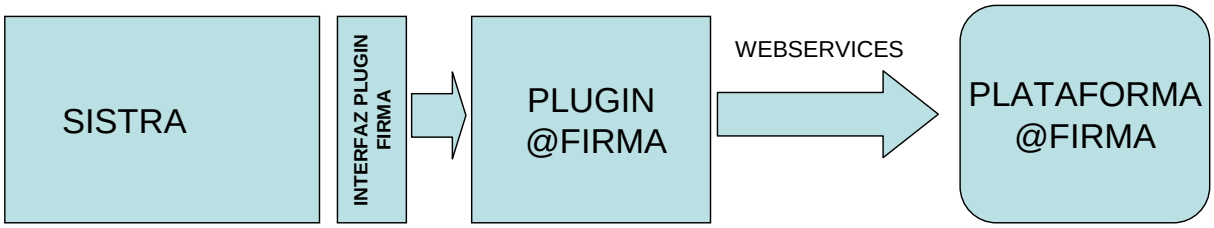
La interfície del plugin de signatura per a les operacions de signatura en servidor és la següent:

Mètode	Descripció	Paràmetres	Resultat
getProveedor	Obté proveïdor de signatura.	No en té.	DGIDT o @firma.
Firmar	Realitza una signatura digital.	datos: dades per signar. nombreCertificado: certificat que s'ha d'utilitzar. parámetros: paràmetres específics proveïdor	FirmaIntf: signatura digital.
verificarFirma	Verifica una signatura.	datos: dades signades. FirmaIntf: signatura digital.	*true* / *false.*
parseFirmaFromHtmlForm	Crea una signatura a partir de la cadena de dades que es rep des del formulari HTML.	signatureHtmlForm: Cadena de signatura rebuda des del formulari HTML.	FirmaIntf: signatura digital.
parseFirmaFromBytes	Crea una signatura a partir d'un array de bytes que es recupera de BD.	Firma: Bytes amb el contingut de la signatura. formatoFirma: format de la signatura.	FirmaIntf: signatura digital.
parseFirmaToBytes	Serialitza la signatura en un byte array per emmagatzemar en BD.	Firma: dades de la signatura.	Byte array amb la signatura.
parseFirmaFromWS	Crea una signatura a partir d'un array de bytes que prové de l'API de web services.	Firma: Bytes amb el contingut de la signatura. formatoFirma: format de la signatura.	FirmaIntf: signatura digital.
parseFirmaToWS	Serialitza la signatura en un byte *array* per usar-la en l'API de web services.	Firma: dades de la signatura.	Byte array amb la signatura.
parseFirmaToFile	Serialitza la signatura digital en un fitxer descarregable per l'usuari.	datosFirmados: dades signatura.	FicheroFirma: dades del fitxer generat.

6. Implementació plugin de signatura

6.1. Plugin @firma

El plugin d'@firma ha d'implementar internament les cridades necessàries als web services de la plataforma d'@firma per donar suport a les operacions definides.



La implementació d'@firma permet l'ús de diversos formats de signatura (CMS, XMLDsig, CADES, XADES, etc.). Per això, s'emmagatzema en el RDS la signatura i el format d'aquesta, per després poder recuperar-la correctament (mètode parseFirmaFromBytes).

S'aconsella que per a la signatura en servidor (la que ofereix el plugin) s'utilitzi un format que generi un segellat de la signatura (per exemple, XAdES-T).

A la part client, com que no es pot generar segell de temps, s'utilitzarà en principi el format CMS (per defecte en @firma). Els formats disponibles en client són CMS (per defecte) i CADES-BES.