MANUAL DE INSTALACIÓN Y USO DEL WEBSERVICEIGNER

Arturo Martín Lladó

3digits S.L.

Tabla de contenido

Manual de instalación y uso del WebServiceSigner	1
Instrucciones de instalación/desinstalación	3
Instrucciones de uso	4
Un pequeño ejemplo.....	5

INSTRUCCIONES DE INSTALACIÓN/DESINSTALACIÓN

Para la instalación de este nuevo signer basta con copiar el JAR (junto al JAR de AXIS y sus dependencias) en el directorio donde se encuentran el resto de signers habitualmente (<JRE>/lib/signaturacaib). A continuación listamos los archivos necesarios para la instalación:

- signaturacaib.webServiceSigner-<VERSIÓN>.jar
- axis.jar (versión 1.4)
- commons-discovery.jar (dependencia AXIS)
- jaxrpc.jar (dependencia AXIS)
- saaj.jar (dependencia AXIS)

Una vez exista el JAR en el directorio signaturacaib, al cargarse el API de firma en alguna ejecución la clase CAIBSigner detectará el recurso e intentará instanciar un objeto de la clase WebServiceSigner para su uso.

Para la desinstalación de este signer basta con borrar el JAR que contiene la clase WebServiceSigner, mencionado anteriormente. Los demás JARs podrían borrarse también a no ser que sean necesarios para, por ejemplo, su uso con el cliente de VALCERT para comprobar el estado de validez de certificados, que también se hace vía webservice (usando el API de AXIS).

INSTRUCCIONES DE USO

Para usar este signer hay que indicarle 3 parámetros, establecidos como propiedades del sistema. Estos son:

- **es.caib.signatura.provider.impl.webServiceSigner.urlWS:** URL de "escucha" del webservice del cual obtendremos certificados y firmas, el cual forma parte de la aplicación IBKeySigner. Una URL de ejemplo sería: <https://<servidor>:8443/ibkey-signer-web/services/SignAndVerifyWS>.
- **es.caib.signatura.provider.impl.webServiceSigner.username:** nombre de usuario de la aplicación que quiere acceder al webservice (se supone que dado de alta desde la zona de administración de la aplicación IBKeySigner).
- **es.caib.signatura.provider.impl.webServiceSigner.password:** contraseña asociada al nombre de usuario del punto anterior.

IMPORTANTE: Además de estas tres propiedades de sistema, es necesario que exista el archivo DGTICkeystore (localizado en el directorio <JRE>/lib/signaturacaib) y que contenga el certificado raíz del emisor del certificado usado por el servidor web donde está instalado el webservice de firma. Por ejemplo, si el servidor web Jetty donde se aloja el webservice de firma tiene como certificado SSL uno emitido por Camerfirma, dentro del archivo DGTICkeystore deberá existir el certificado raíz de dicha autoridad certificadora. Si no se cumple esta condición, la conexión SSL desde el ordenador con el API de firma hacia el ordenador servidor de firma **no funcionará**.

UN PEQUEÑO EJEMPLO

He aquí un pequeño programa de muestra, el cual establece las 3 propiedades de sistema necesarias, carga el API de firma, invoca el método de obtener certificados disponibles y, si los hay, muestra su nombre en la salida estándar:

```
System.setProperty("es.caib.signatura.provider.impl.webServiceSi
gner.username", "usuarioApp");
System.setProperty("es.caib.signatura.provider.impl.webServiceSi
gner.password", "1234");
System.setProperty("es.caib.signatura.provider.impl.webServiceSi
gner.urlWS", "https://epreinfl11.caib.es:8443/ibkey-signer-
web/services/SignAndVerifyWS");

// Content-type para las pruebas
String contentType = "application/signaturaTest";

SignerFactory sf = new SignerFactory();
Signer signer = sf.getSigner();

System.out.println("Usando API de firma versión " +
signer.getAPIVersion());

String[] certs = signer.getCertList(contentType);

if (certs.length > 0) {
    for (int i = 0; i < certs.length; i++)
        System.out.println(certs[i]);
}
```