Govern de les Illes Balears
Vicepresidència Econòmica,
de Promoció Empresarial i d'Ocupació
Direcció General d'Innovació
i Desenvolupament Tecnològic

Estándares de firma electrónica

SERVICIO DE SEGURIDAD

Autor: Pere Joseph Rodríguez
Versión 1.0
Fecha de revisión: 5/12/2012
Ubicación: DGIDT

Índice de contenidos

Propiedades del documento

Autores

Nombre	Fecha	Observaciones
Pere Joseph Rodríguez	05/12/12	

Revisiones

Nombre	Fecha	Observaciones
Cristina Miranzo Nebot		

Distribución

Nombre	Fecha	Empresa

Introducción a la firma electrónica

Reglamentos que regulan la firma electrónica en España

La LEY 59/2003, de 19 de diciembre, de firma electrónica junto con la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, establecen un marco jurídico para la utilización de herramientas que aporten confianza en la realización de transacciones electrónicas en redes abiertas, como se el caso de Internet. La firma electrónica surge de la necesidad de conferir seguridad en las comunicaciones por Internet, y comprobar la procedencia e integridad de los mensajes intercambiados, ofreciendo las bases para evitar el repudio, si se adoptan las medidas pertinentes.

La ley establece unas obligaciones y garantías que deben cumplir tanto las autoridades de certificación o entidades emisoras de certificados digitales, como los dispositivos creadores de firmas electrónicas.

Los certificados reconocidos constituyen una pieza fundamental de la llamada firma electrónica reconocida, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

Por otra parte, la ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida. No basta con la firma electrónica avanzada para la equiparación con la firma manuscrita; se preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación.

Autoridades de Certificación y Certificados digitales

Las Autoridades de Certificación (CA) son entidades emisoras de certificados digitales válidos para la firma electrónica reconocida. Están reguladas por las leyes de firma electrónica mencionadas anteriormente, y deben ofrecer como mínimo un servicio de revocación de certificados, donde cualquier persona con un certificado emitido por esta CA pueda solicitar la revocación de su certificado. También deben ofrecer un servicio de consulta del estado de revocación de los certificados para que los receptores de los documentos firmados puedan averiguar la validez del certificado digital.

Validez de los certificados digitales

Los certificados digitales definen un período de inicio y de fin de validez definido en el momento de emisión del certificado, y en caso que la fecha en el momento de firma no se encuentre entre estos períodos, el certificado no se considera válido.

Las Autoridades de certificación ofrecen un servicio de revocación de certificados para aquellos casos en que se quiera invalidar un certificado, aunque no se haya alcanzado el período de fin de validez de este. La revocación se suele solicitar cuando se sospecha que el certificado personal ha sido robado o ha podido ser usado por personas ilegítimas. Los certificados revocados siguen apareciendo como válidos a los usuario a menos que consulten expresamente el estado de revocación de éstos a la CA emisora del certificado.

También hay un período que se llama período de gracia, que se el tiempo entre que se sospecha del uso ilegítimo del certificado, y el tiempo en que se publica el estado de revocación del certificado por parte de la AC.

Propósitos de los certificados digitales

Todos los certificados digitales válidos para firma electrónica tienen definida una política de certificación en la que se establecen , entre otras cosas, los propósitos de uso del certificado personal, y que invalida las firmas realizadas con propósitos que no están admitidos en estas políticas de certificación.

Ciclo de vida de un documento firmado electrónicamente

El ciclo de vida de una firma electrónica típica consta de los siguientes pasos:

- Generación del documento
- Selección del certificado con el que se va a realizar la firma electrónica en el equipo del firmante
- Firma electrónica en el equipo del firmante
- Recepción de la firma por parte del receptor
- Verificación de la firma por parte del receptor
- Almacenamiento (custodia) de la firma electrónica por parte del receptor
- Publicación del documento firmado electrónicamentee para poder ser verificado

Generación del documento

La aplicación generadora del documento a firmar prepara el documento en el formato adecuado a sus necesidades. Debe tenerse en cuenta que si el documento a firmar debe ser presentado a un tercero, que el documento generado debe seguir el formato PDF/A, ya que es un formato legible para las personas, que cumple los requisitos que facilitarán a cualquier lector del documento firmado, que éste pueda ser visualizado independientemente del equipo en el que se visualice.

También podría utilizarse otros formatos en aquellos casos en que no es necesario que el documento firmado sea inteligible por un receptor humano, o en casos excepcionales.

Los documentos firmados electrónicamente no pueden ser verificados cuando estos se presentan de forma impresa, es por ello necesario facilitar un mecanismo que permita al receptor del documento verificarlo de forma electrónica. Conviene que se añada al documento un campo de texto con una dirección de Internet en que la tercera persona, receptora del documento firmado, pueda consultar el documento impreso, y la validez de las firmas de éste.

Hay que tener en cuenta que una vez firmado el documento, éste no puede ser modificado, si no la firma quedaría invalidada, y por lo tanto en aquellos casos en que el documento debe ser verificado por terceras personas, conviene que se añada la dirección de verificación del documento en un proceso anterior a la firma de éste.

Selección del certificado con el que se va a realizar la firma electrónica

Es importante filtrar los certificados con los que se pueden firmar los documentos, ya que si admitiéramos cualquier tipo de certificado, la persona receptora del documento firmado

podría no reconocer la validez de la firma electrónica debido a la no confianza en el certificado del firmante.

La Ley de firma electrónica establece unas normas para el reconocimiento de los certificados admitidos para diferentes usos.

Firma electrónica en el equipo del firmante

La firma electrónica **siempre** se debe realizar en el ordenador del firmante (para certificados software) o en el token criptográfico (para certificados hardware).

Recepción de la firma por parte del receptor

Una vez firmado el documento, este se envía a la aplicación receptora, que debe verificar la integridad de la firma, y la validez del certificado del firmante.

El documento firmado puede ser enviado con o sin transformación de su formato, pero en ambos casos el documento firmado no se debe modificar, y por tanto la validez de la firma no se debe alterar.

Verificación de la firma por parte del receptor

El proceso de verificación de la firma consta de los siguientes pasos:

- Verificación de que el documento no ha sido modificado después de su firma.

- Verificación de que el certificado del firmante no se falso.

- Verificación de que el certificado del firmante se válido y no ha sido revocado por la autoridad de certificación que lo emitió.

- Verificación de que el certificado utilizado para firmar se un certificado emitido por una Autoridad de certificación en la que confiemos.

Almacenamiento de la firma electrónica por parte del receptor

En aquellos casos en que el documento firmado debe ser almacenado, se debe tener en cuenta los aspectos legales de la custodia de documentos firmados. En aquellos casos en que el documento firmado debe ser custodiado por un período largo de tiempo, hay mecanismos para garantizar a largo plazo que la firma del documento era válida en el momento de la recepción de éste.

Si tenemos un documento firmado electrónicamente, pero no utilizamos estos mecanismos que garanticen la firma electrónica a largo plazo, puede haber problemas en la validación de ésta, por ejemplo:

- Un documento firmado electrónicamente con un certificado personal deja de considerarse válido porque al día siguiente de su firma, se revoca el certificado del firmante, o porque pasado cierto tiempo el certificado del firmante ha caducado. En este caso, el receptor de la firma no puede considerarla como válida ya que no tiene garantías de la fecha en que se realizó la firma, y por tanto no puede saber si en el momento de la firma el certificado era válido o no.
- La autoridad de certificación emisora de un certificado personal con el que se han firmado varios documentos deja de prestar servicio. A partir de este momento no se es capaz de consultar el estado de revocación del certificado ni para el momento actual, ni para el momento en el que se realizó la firma.

Para evitar todos estos casos, el parlamento Europeo ha aprobado un proceso de custodia de documentos firmados electrónicamente a largo plazo, que puede realizarse con la aplicación IBkey-Valcert.

Publicación del documento firmado electrónicamente

En aquellos casos en que el documento debe ser verificado por terceras personas, conviene que se añada la dirección de verificación del documento en un proceso anterior a la firma de éste, y por lo tanto, debe ofrecerse un servicio de acceso o publicación de los documentos firmados electrónicamentee A la hora de publicarse estos documentos debe tenerse en cuenta la confidencialidad que deben cumplir y por tanto deben habilitarse mecanismos de autenticación en aquellos casos en que sea necesario.

Alternativamente se puede distribuir el fichero CADES-A, PADES-A o XADES-A con el documento firmado, ya que este garantiza de forma autónoma la validez de la firma, aunque cada cierto tiempo conviene volver a añadir un sello de tiempo al documento firmado para garantizar que sigue siendo válido (el día en que el algoritmo de firma del sello de tiempo que garantiza la validez de la firma deje de considerarse seguro).

Infraestructura necesaria para la firma electrónica

Infraestructura de certificados PKIX

Autoridades de certificación que cumplan con los estándares PKIX que emitan pares de claves (con certificado) x509, y publiquen los estados de revocación de los certificados emitidos. Esta infraestructura puede ser ofrecida por otros prestadores de servicios y no es el objetivo de este documento.

Aplicación de gestión de la configuración de firma electrónica

Facilita la gestión de la configuración de firma electrónica de forma centralizada.

Servicios de sellado de tiempo

Entidades que aseguren legalmente una fecha de firma de un documento mediante sellos de tiempo.

Servicios de custodia de documentos firmados

Repositorios de documentos firmados electrónicamente según los estándares aceptados en la UE (CADES-A, PADES-A,XADES-A) que realicen los mecanismos necesarios para asegurar la validez de documentos firmados electrónicamente, a lo largo del tiempo.

Aplicaciones de firma electrónica

Aplicaciones que utilicen la firma electrónica de documentos y envíen el documento a un repositorio público o privado de documentos firmados.

Necesidades del firmante

Par de claves X509.

Token de firma electrónica (tarjetas criptográficas PKCS11) y sus drivers.

Lector de tarjetas criptográficas y sus drivers.

Necesidades de la custodia del documento firmado

Cumplir con los estándares aceptados legalmente (CADES-A, PADES-A, XADES-A).

Necesidades del receptor de la firma

En aquellos casos en que el documento pueda imprimirse, que el documento disponga de un apunte en el que aparezca una URL de verificación del documento del repositorio que mantiene la custodia del documento.

Alternativamente, que el documento custodiado cumpla con los estándares aceptados legalmente (CADES-A, PADES-A, XADES-A).

Herramientas de firma electrónica

¿Qué son?

Las herramientas de firma electrónica son un conjunto de servicios ya sea en forma de aplicación, servicio, o librerías de desarrollo, que facilitan el uso de la firma electrónica, el control en el uso de la firma electrónica, y gestionan parte del ciclo de vida de los documentos firmados electrónicamente.

¿Quién debe usarlas?

Cualquier aplicación que quiera utilizar firma electrónica debe utilizar las herramientas aquí expuestas y de la manera que se indica. En caso que haya funcionalidades no implementadas o dudas en su uso conviene contactar con el servicio de seguridad a través de un correo electrónico a suport@caib.es o, a seguretat@dgtic.caib.es.

¿Qué componentes forman parte?

Las herramientas de firma electrónica que se facilitan para el desarrollo de otras aplicaciones y servicios son:

1. Api de firma electrónica
2. Servicio de validación de certificados
3. Servicio de custodia documental
4. Portafirmas de altos cargos

API de firma electrónica

Desde la CAIB se han desarrollado unas librerías Java que facilitan la creación de aplicaciones que utilicen dispositivos de almacenamiento de certificados personales para firma electrónica (Tarjetas electrónicas, dispositivos de firma electrónica, Sistema de criptografia de Windows, o keystores JKS), y ofrece la posibilidad de realizar diferentes funciones con estos dispositivos, así como también facilita la verificación de documentos firmados electrónicamente.

El objetivo de la API de firma es que las diversas aplicaciones cumplan de forma unificada los mismos requerimientos técnicos y funcionales a la hora de firmar y verificar documentos.

¿Qué pasos se hay que seguir para utilizar la API de firma electrónica?

1. Cuando se quiere utilizar la API de firma electrónica en una nueva aplicación, se tiene que solicitar el alta de un identificador asociado a la aplicación y para cada tipo de documento (o content-type). Con este identificador, se configurará qué tipo de firma se requiere para los documentos que pertenezcan a la aplicación, y que pueden ser la combinación de :
    - Certificado reconocido para firma electrónica / No reconocido (sólo autenticación)
    - Firma con sello de tiempo / sin sello de tiempo (*)
    - Firma RAW (No convierte a mime el contenido, y genera smimes PKCS7 enveloped) / No RAW (formato estándar, genera smimes PKCS7 dettached)

(*) El uso de la firma con sello de tiempo no se debería utilizar en los clientes, ya que no se puede garantizar la disponibilidad de los servicios de sellado de tiempo de proveedores externos. Por lo tanto, se debe optar por el servicio de Custodia Documental o añadir el sello de tiempo a la hora de recibir y validar el documento firmado, ya que el mecanismo de custodia puede hacer-se off-line y no garantizar la hora en la que se recibió el documento, si no la hora en la que se custodió.

2. Se debe estudiar con el servicio de seguridad la manera en que se explotará la aplicación para validar la configuración que tenemos de explotación, y si los servicios que se piden se pueden ofrecer.
3. Se tiene que notificar que autoridades de certificación se quiere admitir, y qué certificados emitidos por estas autoridades de certificación se quiere utilizar. Si actualmente la CAIB no admitiese alguna de estas autoridades de certificación, se tendría que hacer un trámite que implica una auditoria para a ver qué certificados se debe admitir como reconocidos y no reconocidos.
4. El uso de diferentes tipos de certificados puede implicar mecanismos de explotación diferentes en los entornos de producción y de preproducción, y por tanto es necesario consultar al servicio de seguridad sobre el uso de estos tipos de certificados.
5. Se tiene que notificar qué dispositivos de firma electrónica se utilizarán. Actualmente se utilizan Tarjetas Oberthur, tarjetas MMAR, el servicio de criptografía de Windows, los tokens USB de Tradise, el DNI electrónico, tarjetas incryptoki2, tarjetas Starcos,

keystores JKS para a firma de servidor, y un servidor de firma para sellos de Órgano (Direcciones Generales y otros).

6. En el caso que la API no ofrezca los servicios necesarios, deberá notificarse al servicio de seguridad las funcionalidades necesarias para ver si es necesario desarrollarlas en la API de firma o no.

¿Dónde puedo obtener recursos de la API de firma?

La web de la API de firma está en http://www.caib.es/signaturacaib donde se pueden encontrar la JavaDoc de la API, los instaladores para los clientes y para los servidores, y applets típicos de ejemplo.

Adicionalmente, para aquellas aplicaciones que requieran que el usuario envíe documentos firmados, hay disponible una aplicación de escritorio que implementa las funcionalidades de la api de firma. La web está en http://www.caib.es/signaturacaib/ibkey/index.htm

Otro detalle importante es identificar en qué versión de Jboss CAIB (módulo seycon de jboss) se desplegará la aplicación. Esto es debido a que en algunas versiones de Jboss, la pantalla de identificación utiliza un applet que fuerza el uso de la versión 1.5 de Java, y otras la 1.6 Esta configuración es importante a la hora de diseñar las páginas que utilizan un applet de firma electrónica , ya que tienen que utilizar la misma versión de Java que la de la pantalla de identificación, o habría problemas en la ejecución del applet.

Servicio de validación de certificados

La plataforma de la CAIB dispone de un servicio de validación de certificados para las autoridades de certificación admitidas. Este servicio es importante a la hora de validar una firma electrónica ya que una validación consta de:

- Verificar que el documento no se ha modificado desde que se firmó.
- Verificar que el certificado con el que se firmó no está revocado.

¿Qué pasos hay que seguir para utilizar el servicio de validación de certificados?

La API de firma, en las instalaciones de servidor, está integrada con el servicio de validación de certificados cuando se llama al método **Signaturev.verify()**

Se puede obtener más información de la configuración de los servidores en:

http://www.caib.es/signaturacaib/docum/manual_instal_servidores.jsp

¿Dónde puedo obtener los recursos necesarios para utilizar el servicio de validación de certificados?

Se puede obtener más información en:

http://www.caib.es/signaturacaib/docum/manual_instal_servidores.jsp

Servicio de custodia documental

El servicio de custodia documental cumple los estándares CADES (RFC 5126) /PADES/XADES aprobados por la UE como formatos válidos para la custodia de documentos firmados electrónicamente. Estos estándares permiten garantizar la validez de la firma electrónica y del estado de revocación del certificado con el que se firmó el documento durante un período largo de tiempo (long term signature), y de forma auto-contenida. Así, si desde el momento de la custodia hasta el momento en que se tuviera de verificar, la Autoridad de certificación hubiese desaparecido, se podría validar igualmente esta información.

El servicio de custodia está integrado con el validador de certificados (Ibkey-Valcert), y sólo admite las autoridades de certificación que estén dadas de alta en el validador.

¿Qué pasos hay que seguir para utilizar el servicio de custodia?

Es conveniente acordar una reunión previa con el servicio de seguridad para conocer las funcionalidades del servicio de custodia y las buenas prácticas para su uso.

Para dar de alta una aplicación para que pueda acceder al servicio de custodia, hay que solicitar al servicio de seguridad un formulario y devolverlo firmado por parte del ingeniero responsable del desarrollo.

Para dar de alta un tipo de documento para la aplicación, hay que solicitar al servicio de seguridad un formulario y devolverlo firmado por parte de alguno de los responsables LOPD del documento.

Una vez aceptada la petición, se asignará un código de usuario y un password.

Opcionalmente, se puede enviar el cliente de acceso al servicio de custodia ya configurado, con el que se podrá establecer comunicaciones con el servicio de custodia.

Para pasar la aplicación a producción será necesario haber firmado y enviado los formularios de la aplicación, por parte del ingeniero al cargo del desarrollo, y los formularios de los tipos de documentos a custodiar por parte de algún responsable LOPD de la aplicación. Éste es un paso imprescindible, y no se realizará ninguna acción en producción hasta que esta documentación se haya entregado y aprobado.

¿Dónde puedo obtener recursos para el servicio de custodia?

El servicio de seguridad las facilitará.

Portafirmas de altos cargos

Todos los documentos que firmen los altos cargos, se deben firmar mediante el envío del documento al portafirmas de altos cargos.

¿Qué pasos hay que seguir para utilizar el portafirmas de altos cargos?

Es conveniente acordar una reunión previa con el servicio de seguridad para conocer las funcionalidades del servicio, y las buenas prácticas para su uso. Una vez realizada, se os asignará un código de usuario y una contraseña.

Los tipos de documentos asociados a la aplicación cliente se pueden solicitar mediante el envío de un correo electrónico a seguretat@dgtic.caib.es por parte del responsable de desarrollo de la aplicación. Para cada tipo de documento que se quiera firmar se debe enviar la siguiente información:

- Nombre
- Descripción
- Tipos de rechazos posibles para el documento. Por defecto hay un tipo "otros" que permite introducir una descripción.
- Tipos de dispositivos criptográficos que se quiere utilizar (DNI-E, tarja Oberthur, tarja MMAR,...)
- Autoridades de certificación que emitan los certificados que se quiere utilizar.

En la fase de pruebas será necesario planificar con el servicio de seguridad un conjunto de pruebas para verificar que la integración se realiza correctamente. La integración con el portafirmas tiene unos requisitos técnicos especiales para que su uso no afecte al rendimiento del sistema de notificación de eventos generados en el portafirmas.

¿Dónde puedo obtener los recursos necesarios para el portafirmas?

Para obtener los certificados personales de los usuarios finales se tiene que seguir la información de :

http://www.caib.es/sacmicrofront/contenido.do?mkey=M08110610180317195848&lang=CA&cont=34771

Los certificados de pruebas se pueden obtener de http://www.caib.es/signaturacaib/

El portafirmas está formado por diversos componentes:

- Web del portafirmas.
- Servicios web del portafirmas.

Se dispone de dos entornos: Producción y preproducción:

Las URLs de los servicios son:

- Web producción: https://intranet.caib.es/portafirmas/inicio.do
- WebService de producción: https://intranet.caib.es/portafirmasws/web/services/CWS

- Web preproducción: https://proves.caib.es/portafirmas/inicio.do
- WebService de preproducción: https://proves.caib.es/portafirmasws/web/services/CWS

El Portafirmas está integrado con el validador de certificados (Ibkey-Valcert), y sólo admite las autoridades de certificación que estén dadas de alta en el validador.