Segno: la versatilidad de un firmador digital para aplicaciones web

Damián Kruse; Ignacio Machado; Mariano Groizard; Martín Gutiérrez Gregoric
Honorable Tribunal de Cuentas de la Provincia de Buenos Aires, Argentina.
{dkruse, imachado, mgroizard, mgutierrez}@htc.gba.gov.ar
http://www.htc.gba.gov.ar

Innovación Tecnológica en las Organizaciones

Resumen

La implementación de la firma digital en el Honorable Tribunal de Cuentas de la Provincia de Buenos Aires, la cual se desarrolla en el contexto del Proyecto de Notificación Electrónica de acuerdo a la Ley Nacional N° 25.506 [1], favorece la gestión digital de los documentos, el cambio cultural y aumenta notablemente la eficiencia de los procesos involucrados.

Segno, surge de investigar los distintos firmadores digitales disponibles en el mercado, teniendo en cuenta las necesidades propias del organismo y la integración con los sistemas web ya implementados.

Dicha solución, es fácilmente adaptable a una infraestructura web existente, sus componentes tecnológicos poseen soporte para todos los navegadores y brinda transparencia al usuario al momento de firmar

Palabras clave: Firma digital, Notificación Electrónica, Segno, Honorable Tribunal de Cuentas

Introducción

La firma digital [2] es el mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje, y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

La firma digital se aplica en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos, por ejemplo documentos electrónicos, ya que proporciona una herramienta para detectar la falsificación y la manipulación del contenido.

Existen diferentes métodos de aplicar el proceso de firma digital; los mismos son determinados de acuerdo al tipo de documento electrónico a firmar (PDF, XML, DOC, etc).

Para generar una firma digital, se utiliza un software denominado “Firmador”, el cual se debe ajustar a la normativa vigente, en este caso la Ley de Firma Digital de la Provincia de Buenos Aires (N° 13.666)[3] y cumplir con los estándares establecidos para el método de firma a utilizar.

En el año 2015 el Honorable Tribunal de Cuentas de la Provincia de Buenos Aires (HTC) emite una resolución [4] que da inicio al proyecto de “Notificación Electrónica” (NE). La implementación de este proyecto se realiza en tres etapas.

La primer etapa del proyecto se implementó en Diciembre del año 2015 teniendo como objetivo la constitución del “Domicilio Electrónico” (DE) de los alcanzados. Es decir, la creación de un espacio virtual destinado a la

gestión de los aspectos vinculados con la NE, tales como, recibir las notificaciones. El proceso de constitución del DE consiste en completar por parte del alcanzado la Declaración Jurada Web (DJW), para ser presentada al HTC. El organismo procede a validar la DJW, y posteriormente dicha validación es notificada al alcanzado.

La segunda etapa, implementada a principios del año 2016, consiste en la gestión de la DJW por parte del alcanzado, desde su DE.

A mediados del año 2016 se realiza la implementación de la tercer etapa, la cual implica la publicación de notificaciones firmadas digitalmente en los domicilios electrónicos de los alcanzados. En este contexto se manifiesta la necesidad de adoptar un producto para firmar documentos PDF el cual cumpla ciertas características, entre las principales, poder ser adaptado de manera transparente a las aplicaciones ya existentes en el organismo.

Durante el desarrollo de este trabajo se exponen las tareas llevadas a cabo para la implementación de un firmador.

Descripción de la innovación

Segno está desarrollado utilizando JavaFX. Esta es una familia de productos y tecnologías para la creación de Rich Internet Applications (RIAs), permite crear aplicaciones con experiencias visuales que resultan atractivas.

Además utiliza la librería iText para la manipulación de archivos PDF y Bouncy Castle Crypto para administrar el uso de algoritmos criptográficos.

La comunicación entre la aplicación cliente y el servidor se realiza mediante servicios RESTful utilizando JSON como formato de datos de transferencia. Además, en dicha comunicación, se utilizan mecanismos de seguridad con el objetivo de autenticar cada requerimiento del cliente al servidor.

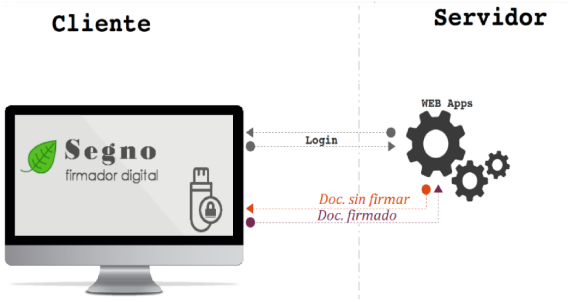

Fig. 1. *Mecanismo de interacción entre cliente y servidor*

Las ventajas de esta implementación son:

- ✓ Bajo mantenimiento del firmador.
- ✓ Utilización de un único firmador en diferentes aplicaciones del HTC.
- ✓ Actualización automática del firmador.

Funcionalidades:

- ✓ Firma de documentos PDF y protección de los mismos contra modificaciones y copiado de información.
- ✓ Integración con dispositivos PKCS#11.
- ✓ Soporte para múltiples firmas
- ✓ Incorporación de datos del firmante, obtenidos de su Certificado en la estampa visible de la firma.
- ✓ Imagen de firma personalizada.
- ✓ Soporte para la inclusión de Sello de Tiempo incrustado
- ✓ Visor de documentos por firmar y firmados

Validaciones:

- ✓ Certificado firmante contra CRL (Certificate Revocation List)
- ✓ Caducidad del certificado firmante.

- ✓ CUIT/CUIL del certificado y el usuario logueado en el sistema.

Proceso de implementación de la innovación

De las primeras posibles soluciones se descarta las de tipo standalone, estas no permiten la integración con el resto de las aplicaciones web utilizadas en el organismo. El usuario debe instalar el software en forma local, descargar un documento pdf a firmar y luego subirlo él mismo a la aplicación web. Esto genera un proceso muy engorroso para los usuarios y no permite cumplir con el objetivo principal: integración transparente del proceso de firmado con el resto de las aplicaciones web del organismo.

Otro escenario evaluado fue con la interacción de un HSM. En este caso la clave privada del usuario se guarda en una partición del HSM, la cual es accedida mediante un pin que conoce el mismo usuario. La aplicación web interactúa directamente con el HSM mediante una conexión segura. El inconveniente de este escenario es que se le quita al usuario la posibilidad de tener un token en su poder donde se guarde su clave privada.

Al investigar las distintas soluciones se observa que la mayoría de los firmadores basados en tecnologías web se encuentran desarrollados con tecnología applet de java, la cual será descontinuada en el futuro cercano. La misma se descarta por las siguientes razones:

- Requiere un plugin de Java a instalarse en el navegador y Oracle ya anunció que abandonará este desarrollo a partir de la versión 9 de Java.
- Sun no ha creado una implementación del plug-in para los procesadores de 64 bits.
- Un applet podría exigir una versión específica del JRE.
- Puede tener vulnerabilidades que permiten ejecutar código malintencionado.

Resultados

El 8 de Agosto de 2016 se firma digitalmente el primer documento emitido por el HTC. Al día de la fecha el HTC ha iniciado la prueba piloto de Notificación Electrónica y se han firmado 142 cédulas de notificación y 53 informes de traslado. Actualmente se han realizado 111 notificaciones electrónicas.

Los tiempos se han acelerado notablemente logrando 30 horas promedio, y 4 días como máximo, para realizar una notificación comparado con las de papel que llegaban a tardar 40 días.

Conclusiones o discusión abierta

La firma digital es uno de los pilares fundamentales para consolidar iniciativas de modernización, transparencia y gobierno electrónico. Su utilización en documentos digitales, la equipara a los documentos papel, dotando de integridad y no repudio a los documentos firmados digitalmente.

Si bien la leyes nacional de Firma Digital tiene más de quince años de vigencia - la de la provincia de Buenos Aires poco menos de diez - podría asegurarse que su despliegue, lejos está de ser masivo, justificado en el gran cambio de paradigma que este representa. El

desafío para los próximos años, será fomentar la utilización de la firma digital en usuarios particulares y organismos privados.

Segno es una pequeña e innovadora contribución para firmar documentos digitalmente. Puede integrarse con cualquier aplicación web siguiendo un protocolo de comunicación siendo totalmente transparente para el usuario.

Resuelve los problemas mencionados que se encontraron en los firmadores disponibles en el mercado y deja la posibilidad de seguir mejorando su funcionamiento.

Actualmente seguimos investigando y desarrollando mejoras en la solución por medio de tecnologías alternativas (Socket.IO), las cuales proveen una comunicación aún más directa entre la aplicación web y el cliente residente que finalmente interactúe con el hardware del usuario.

Además, se estudian nuevas funcionalidades como la de otorgarle la posibilidad al usuario firmante de elegir el lugar en donde se visualizará la firma dentro del documento.

Referencias

[1] Ley Nacional de Firma Digital 25.506
http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[2] http://firmadigital.gba.gov.ar/

[3] Ley Provincial de Firma Digital 13.666
http://www.gob.gba.gov.ar/legislacion/legislacion/l-13666.html

[4] Resolución HTC N° 7 / 2015.
http://www.htc.gba.gov.ar/resolucion-007-2015