Segno IO: Solución integral de firma digital en la Administración Pública.

Damián Kruse[1]; Ignacio Machado[1]; Mariano Groizard[1]; Germán Márquez[1], Martín Gutiérrez Gregoric[1], Juan M. Urruspuru[1]

Honorable Tribunal de Cuentas de la Provincia de Buenos Aires, Argentina.
{dkruse, imachado, mgroizard, gmarquez, mgutierrez, jurruspuru}@htc.gba.gov.ar
http://www.htc.gba.gov.ar

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 IO, surge como mejora de la investigación y desarrollo previo (Segno [2]), teniendo en cuenta las necesidades propias del organismo y la integración con los sistemas web ya implementados.

La solución presentada, conserva las ventajas de la versión anterior: una fácil adaptación a la infraestructura web existente, componentes tecnológicos con soporte para todos los navegadores, y mejora aspectos de la seguridad y la transparencia al usuario utilizando nuevas tecnologías.

Palabras claves: Firma Digital, Segno, Herramienta Informática, H.Tribunal de Cuentas, Provincia de Buenos Aires, Notificación Electrónica.

1 Introducción

La inclusión de la firma digital[3] en un organismo genera un gran cambio cultural y operativo derribando años de paradigmas. Dicho cambio en el Tribunal de Cuentas comenzó a principios de 2015 con el desarrollo de Segno. Dados los avances de la tecnología y la intención de mejorar diversos aspectos se desarrolló Segno IO, una versión mejorada, que toma las características más importantes de su predecesor haciendo hincapié en cuestiones de seguridad e interacción con el usuario.

Para ello se optó por utilizar Socket IO, una tecnología que proporciona un canal de comunicación basado en eventos, bidireccional y full-duplex sobre un único socket TCP. Esta librería tiene implementaciones en gran parte de los lenguajes actuales, por lo que puede ser utilizada en arquitecturas muy diversas.

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) [4] y cumplir con los estándares establecidos para el método de firma a utilizar.

A mediados del año 2016 se realiza el lanzamiento de Segno para comenzar a firmar digitalmente los documentos que se generan en el organismo. Luego de meses de investigación se comenzó a gestar la idea de una nueva versión del firmador mejorando los aspectos que se consideraron de vital importancia para el organismo, como la seguridad y la interacción con los usuarios.

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

2 Descripción de la innovación

Segno IO, al estar basado en Segno, continúa utilizando JavaFX, para la creación de Rich Internet Applications (RIAs), iText para la manipulación de archivos PDF y Bouncy Castle Crypto para administrar el uso de algoritmos criptográficos.
Como mejora de la versión anterior se incorporan las tecnologías Socket.io y JWT (JSON Web Tokens) lo que permite obtener las siguientes ventajas:

- ✓ Mejora en aspectos de seguridad en el proceso de comunicación mediante la utilización de la tecnología JSON Web Tokens (JWT).
- ✓ Mejora la experiencia del usuario en el proceso de firmado por la integración que se logra con las aplicaciones web existentes.
- ✓ La nueva arquitectura permite un fácil escalado ya que desacoplan la comunicación entre el firmador y las aplicaciones. Esto minimiza el intercambio de parámetros de conexión y facilita la integración de nuevas aplicaciones.

Socket.io es una tecnología basada en WebSockets, mediante la cual se permiten manejar eventos en tiempo real y comunicaciones bidireccionales. Al momento de escribir este documento, la API de WebSocket se encuentra en proceso de ser normalizada por el W3C, mientras que el protocolo WebSocket ya fue normalizado por la IETF como el RFC 6455 [5].

JWT es un estándar abierto (RFC-7519) [6] basado en JSON para la creación de tokens que sirven para enviar datos entre aplicaciones o servicios y garantizar que sean válidos y seguros, pudiendo cifrar y firmar las comunicaciones entre los componentes de la solución.

En concordancia con los aspectos de seguridad, toda transmisión de información entre los componentes se realiza sobre el protocolo HTTPS

2.1 Arquitectura de solución

En la Fig.1 se muestra la arquitectura de solución para Segno IO en la que se detallan sus componentes y el esquema de interacción entre los mismos.

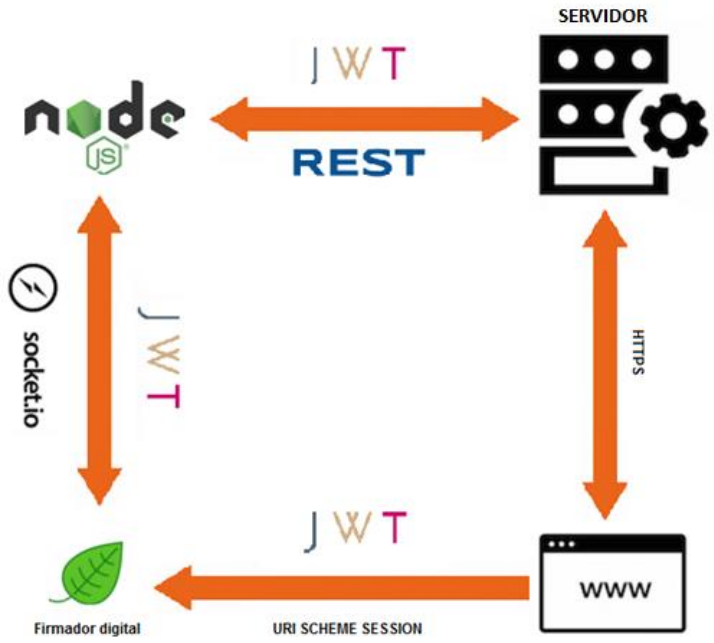

Fig. 1. *Arquitectura de solución*

La solución planteada cuenta con los siguientes componentes:

- **Aplicación Web**: Se encarga de proveer los documentos a firmar. Este componente mantiene claves para firmar los JWT utilizados para la comunicación con servidor NODE JS.
- **Servidor Node JS**: Encargado de administrar la comunicación entre las aplicaciones web y la aplicación Java. Mantiene una tabla <usuario, socket.id, clave_de_firmado>. Expone los servicios para que las aplicaciones web logren comunicarse con la aplicación Java y puedan firmar los documentos.
- **Firmador digital:** Encargada de firmar los documentos digitalmente. Reside en el equipo del usuario firmante y debe ser configurada como predeterminada para abrir el uri scheme generado por la aplicación web.

2.2 Interacción entre los componentes

A continuación se detallan los procedimientos involucrados en Segno IO en los cuales se percibe las mejoras introducidas en el firmador:

- **Inicio***:* ¿cómo se establece la conexión entre los componentes que intervienen?

    1. El usuario ingresa a la aplicación web y genera una nueva sesión en la misma.
    2. Desde la aplicación web, cuando selecciona la opción de listar documentos a firmar, se descarga por medio de un uri scheme[7] (session) un token generado de manera aleatoria y firmado utilizando JWT. La aplicación predeterminada para el uri scheme es el Firmador digital.

3. El Firmador digital reenvía, mediante Socket IO, el token firmado recibido por parámetro al servidor de Socket.io
4. El servidor de Socket.io recibe el JWT (token) firmado y mediante REST le consulta a la aplicación web a quien corresponde dicho token. La aplicación web recupera el token, y verifica su integridad con la clave que corresponde a dicho usuario.
5. El servidor de Socket.io recibe la información, y le informa al firmador digital la clave de firmado que va a utilizar para firmar aquellos requerimientos que intercambia con la aplicación web.

- **Firmado**: ¿cómo se realiza la firma digital? una vez establecida la comunicación se procede a firmar digitalmente de la siguiente manera:

6. El usuario selecciona el documento a firmar y ejecuta la opción de firmar.
7. La Aplicación Web se comunica con el servidor de Socket.io enviando el usuario solicitante y el documento a firmar en formato Base64.
8. El servidor Socket.io recibe el requerimiento, verifica en qué socket está el usuario que solicita firmar el documento y lo envía a firmar mediante un mensaje.
9. El Firmador Digital recibe la instrucción de firmar y devuelve el documento firmado al servidor Socket.io el cual, posteriormente genera un nuevo llamado utilizando REST a la aplicación que solicitó la firma del documento.

2.3 Otras características de la solución

El firmador digital Segno IO presenta las siguientes características que hacen a la firma digital:

- ✓ 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 token
- ✓ Imagen de firma personalizada.
- ✓ Soporte para la inclusión de Sello de Tiempo incrustado (Time Stamping)
- ✓ Visor de documentos por firmar y firmados
- ✓ Posibilidad de elección por parte del usuario del lugar de la firma dentro del documento.

En cuanto a validaciones a realizar al momento de firmar se realizan los siguientes chequeos:

- ✓ Certificado firmante contra OCSP y CRL (Certificate Revocation List)
- ✓ Caducidad del certificado firmante.
- ✓ CUIT/CUIL del certificado y el usuario logueado en el sistema.

3 Resultados

Segno IO continuó con los logros obtenidos por su versión anterior, se han firmado 126 fallos, 1.390 cédulas de notificación, 181 informes de traslado y 267 comunicaciones simples.
Los tiempos se han acelerado notablemente logrando 28 horas promedio, y 4 días como máximo, para realizar una notificación comparado con las de papel que llegaban a tardar 40 días.

Las tecnologías aplicadas en Segno IO han permitido incorporar firma digital en nuevas aplicaciones en el HTC de manera ágil. También, el uso de librerías estandarizadas repercutió en facilidad de mantenimiento en el código fuente del firmador.

4 Próximas actividades

Las mejoras introducidas en Segno IO fueron significantes, aun así, las ventajas pueden optimizarse con las siguientes actividades:

- Uso de la tecnología Socket.io en toda la arquitectura
  Con el objetivo de lograr comunicación asincrónica en toda la arquitectura se buscará reemplazar el esquema de REST por el de Socket.io entre la aplicación web y el componente de Node.JS.
- Uso de claves asimétricas entre los componentes
  Se buscará el uso de claves asimétricas para evitar la transferencia de claves simétricas entre los componentes de la arquitectura, a los efectos de robustecer en materia de seguridad la arquitectura.
- Cifrado de los JWT (JWE)
  Además del firmado de los JWT se propone como mejora el cifrado de los tokens.

5 Conclusión

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

6 Referencias

[1] Ley Nacional de Firma Digital 25.506
http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.html
[2] Damián Kruse, Ignacio Machado, Mariano Groizard y Martín Gutiérrez. (2016). Segno: La versatilidad de un firmador digital para aplicaciones web. En Malbernat L. R.; Finochietto J.R.; Bacigalup G.F. (Comps.), II Jornadas Argentinas de Tecnología, Innovación y Creatividad - II JATIC 2016, Mar del Plata, Argentina.
http://jatic2016.ucaecemdp.edu.ar/trabajos/WCIEE405CI-Kruse-MachadoJATIC2016.pdf
[3] http://firmadigital.gba.gov.ar/
[4] Ley Provincial de Firma Digital 13.666
http://www.gob.gba.gov.ar/legislacion/legislacion/l-13666.html
[5] RFC 6455 https://tools.ietf.org/html/rfc6455
[6] RFC 7519 https://tools.ietf.org/html/rfc7519
[7] Uri Scheme: https://tools.ietf.org/html/rfc3986