13

SDK (SOFTWARE DEVELOPMENT KIT) DE FIRMA ELECTRÓNICA

Oscar García Reyes
Business Sales Consultant. Área de Seguridad
Grupo SIA

Carlos Guerra Belver
Consultor Técnico. Área de Infraestructuras de Seguridad
Grupo SIA

1. INTRODUCCIÓN

La Identidad Digital es una herramienta fundamental para extender las aplicaciones en Administración electrónica a los ciudadanos.

En la actualidad ya existen diversas iniciativas para ofrecer identidad digital, como tarjetas de identificación u otros certificados. Con el fin de reducir complejidad y costes, es importante que la identidad electrónica sea independiente de las demás aplicaciones. Por otro lado, el manejo de dichas aplicaciones podría llegar a ser muy complejo sin la implementación de servicios de infraestructuras que sean capaces de proveer con perfiles, políticas de control de accesos y regulaciones legales.

Los servicios de infraestructuras están dedicados a proveer validación de certificados, matrículas, firmas digitales, gestión de derechos digitales, o SSO. Combinados con servicios web, estos permitirán una mayor fluidez en los procesos de cara a tramitar las solicitudes de los ciudadanos.

El paso definitivo será la expansión de aplicaciones de firma digital a sistemas avanzados de archivo dedicados a localizar y recuperar documentos firmados en el pasado, para que los ciudadanos se sientan más cercanos al concepto de la "administración sin papel".

Es muy importante que las firmas electrónicas que son archivadas localmente puedan ser verificadas años después. Iniciativas como EESSI (European Electronic Signature Standardization Initiative) o IETF (Internet Engineering Task Force) han trabajado para conseguir que las firmas electrónicas puedan ser utilizadas como evidencias mucho tiempo después de ser creadas.

En el caso de EESSI, nada más publicarse la Directiva Europea 1999/93/CE por la que se establece el marco comunitario para la firma electrónica, un grupo de expertos redactó un informe (http://www.ict.etsi.org/eessi/Documents/Final-Report.pdf) en el que se define los Servicios de Archivo Confiables (Trusted Archival Services –TAS) con el fin de aumentar las garantías de los documentos firmados digitalmente.

En el ámbito PKIX, IETF publicó un primer borrador (http://www.ietf.org/proceedings/03nov/I-D/draft-ietf-pkix-tap-00.txt) en el que se definen las Autoridades Confiables de Archivo (Trusted Archive Authority – TAA) como un servicio que garantiza el "no repudio" en periodos largos mediante el mantenimiento de una infraestructura segura de almacenamiento.

El desarrollo de la firma electrónica, así como del despliegue de autoridades de certificación está alcanzando la madurez en España y resto de países. En este entorno se hace relativamente común encontrar requerimientos para fortalecer diversos procesos encontrados en las aplicaciones para garantizar las funcionalidades de integridad y no-repudio proporcionadas por esta tecnología.

Dichos requerimientos no suponen descartar las aplicaciones actuales, sino más bien complementarlas con funcionalidad adicional. Esto significa que las aplicaciones evolucionan, a menudo mediante la liberación de nuevas versiones, para adaptarse a esta nueva necesidad, pero manteniendo toda la lógica de la aplicación y de negocio ya incorporada en el producto.

El Grupo SIA, en su extensa actividad desarrollada en el área de seguridad, ha realizado una intensiva valoración de los distintos productos existentes para la implementación de firma. En esta labor se han identificado una serie de elementos que exigen, o bien unos tiempos de capacitación de los desarrolladores muy altos por la complejidad de sus funciones, o bien ligarse a tecnologías específicas.

Dentro de este marco, SIA desarrolló unas librerías para la incorporación por parte de las organizaciones de dichas funcionalidades de forma sencilla en las aplicaciones. Debido a la diferente casuística encontrada, así como a los cambios legales (prohibición de distribución de la máquina virtual de Java de Microsoft), se ha hecho imprescindible el desarrollo de nuevos componentes que van más allá de la actualización de la versión anterior, ya que incorpora importantes diferencias cualitativas y cuantitativas. **Esta nueva librería es lo que denominamos SDK de Firma Electrónica y el presente documento describe sus características así como la evolución futura de esta solución.**

2. OBJETIVOS Y ALCANCE

2.1 OBJETIVOS

El principal objetivo del producto es disponer de un componente que permita incorporar funcionalidad de firma electrónica al mayor número de aplicaciones posibles teniendo en cuenta sus diferentes características en lo que se refiere a los lenguajes de desarrollo, diversidad de entornos clientes y servidores.

El producto se plantea como un SDK (Software Development Kit) y por tanto requiere de trabajo por parte de los desarrolladores de cada aplicación para incorporar la funcionalidad a cada una de ellas, si bien el tiempo requerido para realizar esta actividad se optimiza en todo lo posible, no solo por lo que se refiere a la simplicidad de las API, sino también en lo relacionado con el material entregado dentro del SDK.

La solución se centra en certificados X509v3 aceptados por la mayoría de navegadores, y emitidos por la mayor parte de las autoridades de certificación.

El producto no incorpora funcionalidad para el almacenamiento y gestión de los documentos firmados, quedando esta funcionalidad a discreción de la aplicación desarrollada.

Desde un punto de vista normativo destacar que el producto de firma electrónica cumple con las interpretaciones técnicas de la Directiva Europea 1999/93/CE por la que se establece un marco comunitario para la firma electrónica.

3. DESCRIPCIÓN DE LA SOLUCIÓN PROPUESTA

3.1 Descripción Funcional

La solución permite realizar operaciones de firma y verificación. La operación de firma puede ser hacerse tanto en cliente (navegador) como en servidor, mientras que la verificación de firmas se realiza únicamente en el servidor. Esto es debido al peso importante de los componentes necesarios para la verificación de firma así como los requerimientos especiales de conectividad que no pueden garantizarse en todos los clientes.

Se pueden utilizar certificados de distintas autoridades de certificación, tanto por los clientes como por los servidores. No obstante, la aceptación de nuevas autoridades de certificación debe ser configurada específicamente de forma que se controle el círculo de confianza de la aplicación.

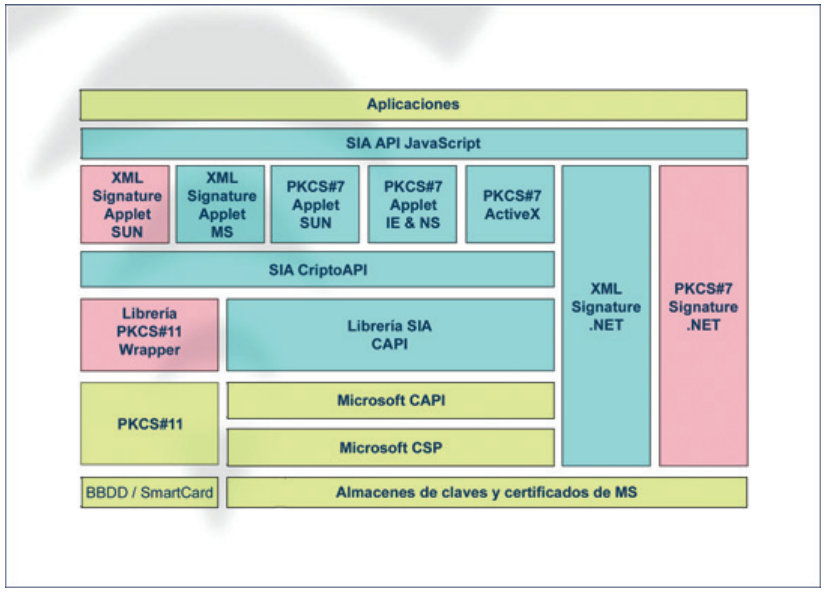
La verificación realiza tanto la comprobación técnica de la corrección del documento, como la verificación de la validez del certificado (periodo de validez correcto) y por último, se comprueba que dicho certificado no ha sido revocado por la autoridad de certificación correspondiente. Para la verificación de las CRL se realizan conexiones con los diversos servicios LDAP configurados para el certificado concreto con el que se firmó el documento, autenticándose si así lo requiere el servicio.

La firma electrónica se genera siempre de acuerdo a estándares. Por un lado es posible generar un PKCS #7 (Clear-Signed) en el que se genera una matriz de datos correspondiente a la firma pero separado del documento. Por otro lado se tiene la capacidad de firmar documentos XML de acuerdo a la especificación (XML Signature RFC 3275) en su modo **"Enveloped XML Signature"** en el que el documento y la firma quedan ligados en un único XML y de acuerdo a la especificación técnica voluntaria ETSI (TS 101 903 v1.2.2) en relación a la implementación de Firmas Electrónicas Avanzadas XML (XAdES)

Si bien, ambas soluciones permiten el concepto de firma paralelo o serie, así como la verificación de estas en serie o paralelo, su implementación no se ha llevado a cabo en todos los módulos, aunque todos lo soportan (sería la aplicación la que debería gestionar los dos tipos de firmas).

La firma paralelo se corresponde con procedimientos en los que es necesario que varios usuarios firmen un documento, pero no existe un orden necesario en las firmas. Se corresponde con flujos como por ejemplo la aprobación de un documento por el departamento jurídico, técnico y financiero donde es necesario que todos ellos validen el documento para su aprobación.

La firma en serie refleja flujos en los que, no sólo son importantes las firmas sino que además es necesario que el documento se firmara en un orden concreto. Por ejemplo una aprobación de vacaciones irá aprobada primero por el responsable directo, el siguiente directivo firma porque está de acuerdo con el documento y además porque éste ya está firmado por el responsable directo y finalmente recursos humanos aprueba las vacaciones basándose principalmente en la firma del director.



3.2 Arquitectura propuesta

La arquitectura de los distintos componentes se resume en el gráfico presentado a continuación. En él se puede ver coloreado los componentes que aporta SIA, así como los elementos que deben disponerse de base para el funcionamiento.

Los componentes de servidor permiten:

Verificación XML Signature Java SUN: Verificación de firma XML desde una máquina Java SUN instalada en el servidor de aplicaciones (o compatible). No soporta la firma serie y paralelo.

Verificación XML Signature Java MS: Verificación de firma XML desde una máquina virtual Java de Microsoft instalada en el servidor Web. No soporta firmas en serie o paralelo.

Verificación XML Signature .NET: Verificación de firma XML desde una aplicación desarrollada en .NET. Soporta firmas en serie y en paralelo.

Verificación PKCS#7 Java SUN: Verificación de firma PKCS#7 desde una máquina Java SUN instalada en el servidor de aplicaciones (o compatible). No implementa las firmas serie y paralelo, pero si soporta su uso.

Mientras que los componentes cliente cumplen el siguiente propósito:

SIA API JavaScript: API única que permite el desarrollo de aplicaciones independiente de la tecnología utilizada en el cliente. Da la estabilidad necesaria a la aplicación desacoplando la dependencia de las distintas tecnologías del cliente o referidas a la firma. SIA además adquiere el compromiso de mantener todas las funciones de la API aquí expuestas en futuras versiones de la librería por lo que la aplicación podrá ampliar la funcionalidad futura a nuevas versiones sin impacto en el desarrollo. No se descarta la ampliación del número de funciones para incorporar funcionalidades en el futuro.

XML Signature Applet MS: Este componente permite la firma XML desde clientes que dispongan de la máquina virtual Java de Microsoft. No soporta firmas en serie ni en paralelo.

PKCS#7 Applet SUN: Permite la firma PKCS#7 desde clientes que dispongan de la máquina Java de SUN. Este componente, en caso de no disponer de el, puede ser descargado gratuitamente si bien tiene un peso considerable (entorno a 14 Mb). Por otro lado permite su utilización desde navegadotes distintos a Internet Explorer. No implementa las firmas en serie y en paralelo, pero si soporta su uso.

PKCS#7 Applet IE & NS: Este componente permite la firma PKCS#7 desde clientes que dispongan de la máquina virtual Java de Microsoft en el caso de Internet Explorer (IE) o la máquina virtual de Netscape (NS) en el caso de navegadores Netscape 4.7x. No implementa firma serie o paralelo, pero si está soportado su uso.

PKCS#7 ActiveX: Permite la firma PKCS#7 mediante un componente ActiveX. Su uso se restringe al navegador Internet Explorer. Al igual que el Applet IE & NS, no implementa firma serie o paralelo, pero su uso está soportado.

XML Signature .NET: Permite la firma XML en el cliente para desarrollos realizados en entorno .NET. Soporta firma en serie y en paralelo.

SIA CriptoAPI: Conjunto de primitivas criptográficas común e independiente de la tecnología de acceso al certificado.

Librería SIA CAPI: Permite el acceso a las librerías de Microsoft mediante primitivas estándares y encapsulando la importante complejidad de dicha tecnología.

4. PRODUCTOS INCLUIDOS EN SDK

El SDK incluye los siguientes componentes:

- Librerías de cliente y servidor.
- Documentación de las API de cada uno de los componentes incluyendo parámetros y códigos de retorno
- Ejemplos: Incorpora código fuente comentados para su uso por los desarrolladores a modo de guía.

5. ROAD MAP

La arquitectura presente tiene previsto evolucionar para alcanzar un mayor número de entornos en el cliente. El siguiente gráfico presente la futura arquitectura de acuerdo a la previsión:

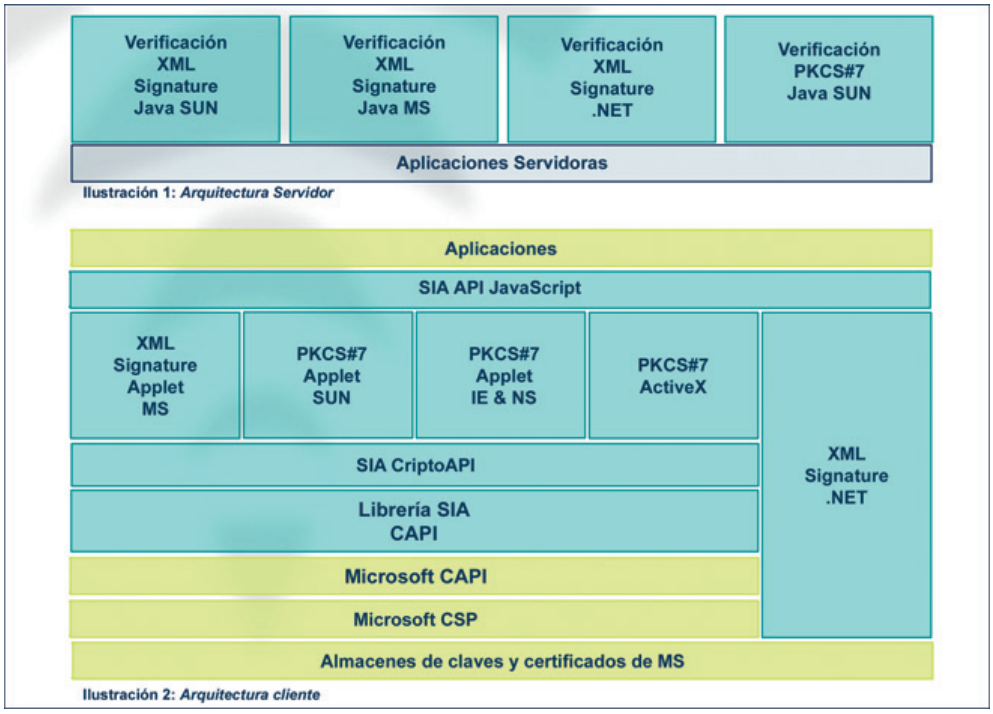


Ilustración 1: *Arquitectura Servidor*

Ilustración 2: *Arquitectura cliente*

En ella se observa la incorporación de los siguientes componentes:

PKCS#11 Wrapper: Permite la utilización, no solo de CSP como mecanismo de acceso a los certificados sino también de PKCS#11 (estándar más extendido, tanto para smartcards, como en entornos cliente no-Microsoft).

XML Signature Applet SUN: Permite la generación de firmas XML desde la máquina virtual de Sun.

PKCS#7 Signature .NET: Para aplicaciones desarrolladas en .NET, este componente permite que el cliente genere firma PKCS#7.

6. CONCLUSIONES Y VENTAJAS

La solución presentada permite adquirir un componente que facilite enormemente el desarrollo de las aplicaciones relacionadas con firma. SIA ha combinado su experiencia durante los últimos 6 años en el desarrollo e integración de soluciones relacionadas con infraestructuras de clave pública para refinar las librerías presentadas en este SDK.Las principales ventajas que presenta son:

- API estables garantizan el funcionamiento futuro de las aplicaciones.
- Multi-CA: Permite la utilización de distintas autoridades de certificación.
- Fácilmente integrables: Por su diversidad de entornos y tecnologías de desarrollo contempladas.
- Extensibles: Permiten incorporar nuevas tecnologías y entornos sin impacto en las aplicaciones.
- Soporte telefónico: Proporciona una resolución rápida de cuestiones o dudas. SIA por otra parte proporciona los siguientes valores añadidos/garantías de éxito:
- Más de 500 proyectos ejecutados de seguridad ejecutados en los últimos tres años.
- Más de 120 profesionales con dedicación íntegra a la seguridad.
- Participación en la mayoría de los principales proyectos de certificación en España.

El producto denominado "SDK de firma electrónica" garantiza el cumplimiento de los requisitos aparecidos en la Directiva Europea 1999/93/CE por la que se establece un marco comunitario para la firma electrónica. Para ello se ha tenido en cuenta las especificaciones técnicas voluntarias aprobadas por el Comité Europeo de Normalización (CEN) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI) dependientes de EESSI (Iniciativa Europea de Normalización de la Firma Electrónica).

De esta forma, el producto de firma electrónica garantiza la compatibilidad de los sistemas y la interoperabilidad tecnológica, objetivos necesarios para conseguir que la normativa reguladora del uso de la certificación digital en el ámbito administrativo sea común para el conjunto de las Administraciones.