Viafirma platform

Descripción Ampliada del Producto

ÍNDICE

1. INTRODUCCIÓN

1.1. ¿Qué es viafirma platform?

Viafirma platform es una plataforma de firma electrónica que simplifica el desarrollo de aplicaciones que requieran usar certificados digitales x509.v3 de infraestructuras de clave pública (PKI), de cara a introducir procesos de firma electrónica que tengan la misma validez legal que la firma manuscrita.

Viafirma platform encapsula la complejidad relativa a esta materia y se despliega como un servicio más de una infraestructura global, siguiendo el paradigma de arquitecturas SOA (Service Oriented Architecture). Cualquier aplicación puede así incluir funciones de autenticación y firma electrónica utilizando los servicios que el sistema ofrece, abstrayendo a las aplicaciones de los problemas y complejidades técnicas relacionadas con el uso de certificados digitales, como son la criptografía de clave pública, validaciones de certificados con CRL y OCSP, lectura avanzada de certificados, envolturas de múltiples formatos de firma o verificación de documentos firmados entre otras características soportadas.

1.2. Introducción a características tecnológicas

El sistema **viafirma platform** está construido bajo una arquitectura Java EE, y se pueden destacar algunos aspectos relevantes como los citados a continuación:

- Construcción basada en Apache Maven y compilado y desplegado de forma automática con la herramienta de integración continua Jenkins.
- Uso de Java Cryptographic Extension (JCE), Bouncy Castle, EhCache, JAX WS o Apache XML Security entre otras.

1.3. Arquitectura de viafirma platform

Pueden destacarse algunas características referentes de arquitectura de esta plataforma:

- Arquitectura plugable. Todas las funcionalidades que puedan ser personalizables disponen de interfaces que admiten la inyección de plugins personalizados, de cara a poder adaptar el comportamiento a cada cliente. Ejemplos de este tipo de servicios serían:

- Interpretación de atributos de certificados digitales, permitiendo configuración personalizada para el tratamiento de certificados con particularidades específicas incluidas en cada Política de Certificados.
- Custodia de documentos firmados delegados en conectores plugables, como base de datos, filesystem, caché o conectores basados en el protocolo CMIS, permitiendo interactuar con gestores documentales compatibles con este protocolo, como Alfresco, Sharepoint, etc.
- Múltiples formatos de firma.
- Registro de auditoría de operaciones en modalidades online para registros síncronos, y registros diferidos para procedimientos de auditoría asíncronos.
- Soporte a distintos almacenes de certificados de forma concurrente: cacert, JKS, HSM, PKCS11.
- Políticas de stampers que permiten personalizar el aspecto de los justificantes de firma, con elementos de seguimiento CSV (Código Seguro de Verificación) como Barcode, QR-Code o permalinks personalizables.

2. CARACTERÍSTICAS A DESTACAR

2.1. Integración

Los servicios de integración se ofrecen a través de varios protocolos, como SOAP con ws-* (securizando con WS-Security), REST o RMI.

Para varias arquitecturas se han creado clientes específicos que permiten al integrador abstraerse de la lógica de firma en cliente, interactuando con componentes locales como applet, JNLP, aplicación escritorio o apps móviles.

Estos clientes específicos se ofrecen en los lenguajes Java, .NET y PHP, y para integraciones M2M (mobile2mobile) se ofrecen SDK nativas para iOS y Android.

2.2. Componentes para Firma en Cliente

Viafirma platform dispone de un cliente de firma electrónica para entornos web que permite la autenticación y firma electrónica en prácticamente cualquier combinación de sistema operativo y navegador y asegura a la vez su integración con un mínimo coste de implantación y con soporte de los formatos más avanzados de firma electrónica.

Para ello, viafirma platform ofrece de forma automática o preconfigurada distintos componentes de firma en cliente:

- **Applet**: para entornos con Java y navegadores con soporte a NPAPI.
- **JNLP**: para entornos con Java y navegadores sin soporte a NPAPI.
- **Viafirma desktop**: para entornos Windows 7, 8 y 10, con o sin Java y navegadores con o sin soporte NPAPI.
- **Viafirma UWP**: para entornos Windows 10, con o sin Java y navegadores con o sin soporte NPAPI.

2.2.1. Applet de firma y autenticación

Compatible para aquellos navegadores que aún no han bloqueado el uso de NPAPI, y que sigue permitiendo al usuario poder interactuar con sus certificados instalados en su sistema operativo, navegador o dispositivos externo, como smartcards o tokens USB. El applet también es compatible para la firma digitalizada o biométrica.

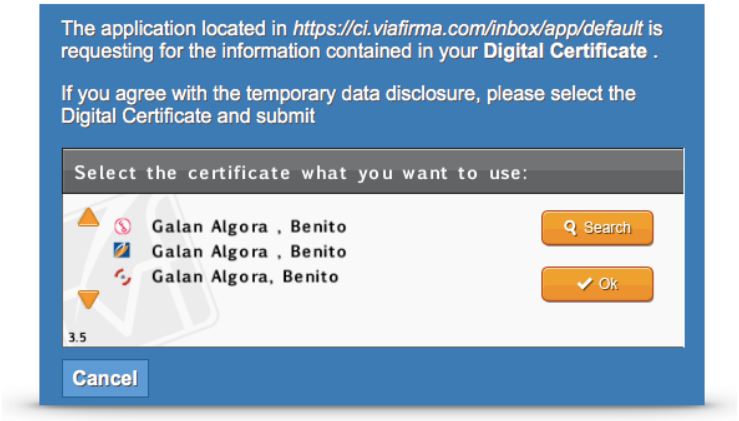

imagen 1 applet de viafirma para firma, autenticación y firmas digitalizadas (biométricas)

2.2.2. Componente JNLP

Como medida recomendada por Oracle/Sun, y en aquellos entornos en los que el usuario sólo puede hacer uso de navegadores con bloqueo de NPAPI y, por tanto, no pudiendo hacer uso de applets, viafirma platform hace push de un componente ligero, instalable bajo un proceso Java Web Start, y que permite al usuario poder interactuar con sus certificados instalados en su sistema operativo, navegador o dispositivos externo, como smartcards o tokens USB.

Este componente JNLP también es compatible para la firma digitalizada o biométrica.

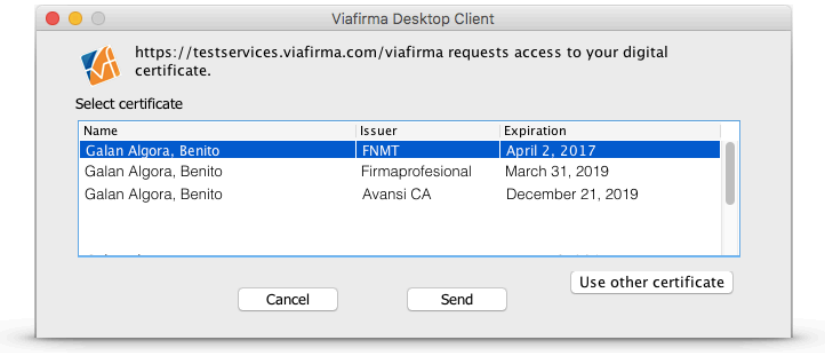

imagen 2 viafirma componente JNLP

2.2.3. Viafirma Desktop

Este componente, a modo de aplicación escritorio, es ofrecido para clientes que NO tengan JAVA, o bien aquellos que aun teniendo JAVA instalado e incluso navegadores que aún soportan el uso de applets, prefieren el uso de la aplicación escritorio por usabilidad.

Viafirma desktop es compatible en entornos Windows 7, 8 y 10. Para entornos Windows 10 el usuario además podrá optar por el cliente nativo de viafirma diseñado exclusivamente para Windows UWP, es decir, una misma aplicación que podrá usar en sus dispositivos favoritos con Windows 10: escritorio, portátiles, smartphone y tablets.

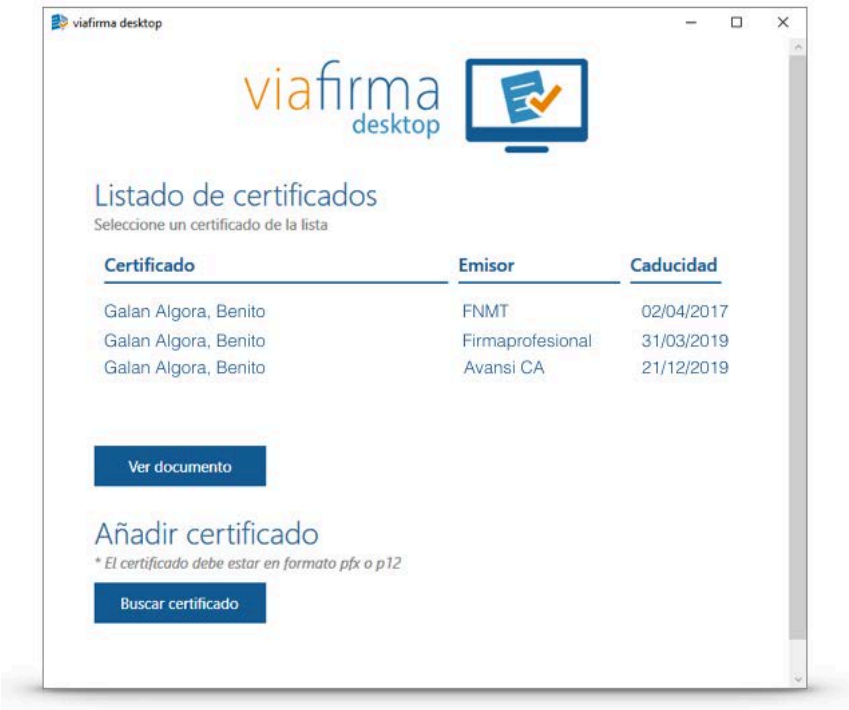

imagen 3 viafirma desktop para windows 7, 8 y 10

2.2.4. Viafirma Desktop para Windows 10

Aplicación nativa basada en el paradigma de Microsoft para “aplicaciones universales”, pudiendo usar una misma aplicación en entornos escritorios y móviles, incluyendo smartphones y tablets con Windows 10.

imagen 4 viafirma para Windows UWP (windows 10)

2.2.5. Viafirma mobile

Como un cliente más para firma en cliente, y con lógica totalmente extraída de la responsabilidad del integrador, viafirma platform detecta de forma automática si el usuario está navegando con un dispositivo móvil y su sistema operativo, ofreciendo a éste la apertura por protocolo de la app viafirma mobile.

La app viafirma mobile permite el uso de certificados digitales en formato software (.p12 y .pfx), importados cómodamente desde repositorios externos como Dropbox, iCloud o Drive, y también en smartcards en aquellos casos donde se haga uso de lectores compatibles.

Estas apps están disponible de forma gratuita en los respectivos markets, Google Play, App Store y Windows Store.

2.2.5.1. Viafirma mobile para iOS

Disponible en App Store desde 2010, siendo la primera app iOS del mercado con soporte a firma electrónica basada en el uso de certificados.

Con las versiones actuales la evolución de la app ha facilitado más aún su uso, permitiendo la importación e instalación de certificados desde ubicaciones externas, y en los dispositivos con TouchID permitiendo incluso protegerlos con la huella del usuario.

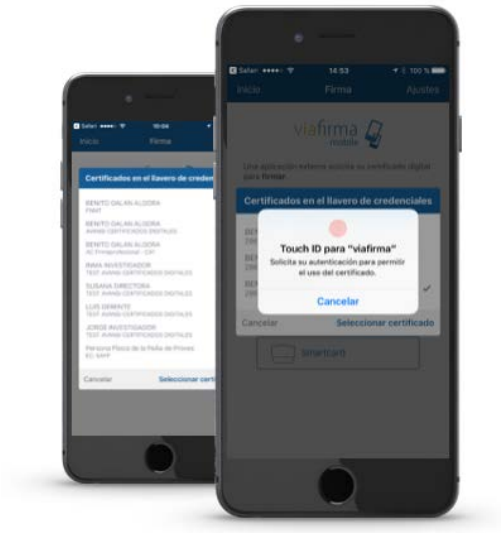

imagen 5 viafirma mobile para iOS

2.2.5.2. Viafirma mobile para Android

Disponible en App Store desde 2010, siendo la primera app Android del mercado con soporte a firma electrónica basada en el uso de certificados.

Con las versiones actuales la evolución de la app ha facilitado más aún su uso, permitiendo la importación e instalación de certificados desde ubicaciones externas e integrándolo con el llavero de credenciales de Android.

imagen 6 viafirma mobile para Android

2.2.5.3. Viafirma mobile para Windows UWP

Adaptándose al nuevo paradigma de Microsoft para “aplicaciones universales”, pudiéndose usar en todos los dispositivos con Windows 10 a partir de una única aplicación, viafirma mobile también está disponible para UWP (Universal Windows Platform).

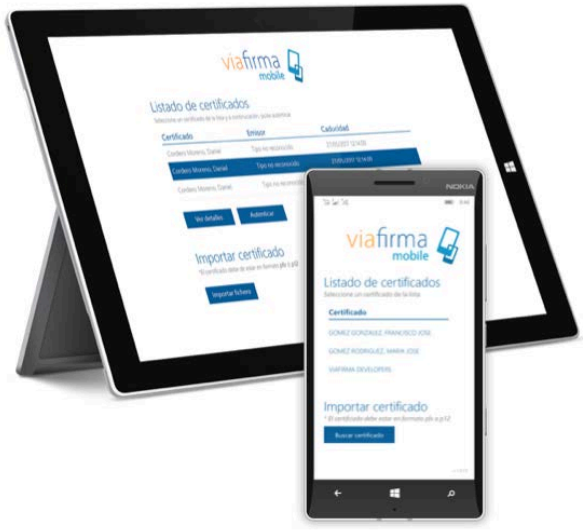

imagen 7 viafirma mobile para Windows UWP

2.3. Firma digitalizada (biométrica)

Entre los formatos de firma disponibles en los servicios de viafirma platform se encuentran formatos para firma digitalizada o biométrica.

En estos casos, la firma consiste en la captura de una serie de evidencias grafológicas obtenidas a partir de dispositivos específicos ya soportados por viafirma, como smartphones, tablets y tabletas digitalizadoras como las de Wacom Topaz.

imagen 8 viafirma mobile con firma digitalizada/biométrica

imagen 9 viafirma con firma digitalizada/biométrica en Wacom

2.4. Sellos de Tiempo

Viafirma platform soporta la integración con cualquier TSA (Timestamping Authority) que cumpla el estándar RFC 3161, necesario en formatos de firma (cualquiera de firma longeva) que recojan dentro de las evidencias de firma sellos de tiempo.

Este soporte de sellados de tiempo puede ser utilizado con cualquier tipo de formato que admita la inclusión de los timestamping, modalidad de firma, operación en cliente, servidor, etc.

Están soportados distintos mecanismos de autenticación del servicio de TSA, como autenticación básica, autenticación "Encapsulation (CMS)" o autenticación basada en TLS (RFC2246).

2.5. Validación de Certificados

Además de los mecanismos de validación intrínsecos a cada operación de autenticación o firma con certificado digital, los integradores tienen a su disposición servicios específicos para la validación de certificados, obteniendo de forma sencilla el estado del certificado que se desea consultar, o el certificado asociado a un proceso de firma.

Entre las posibles configuraciones asociadas a la validación de certificados, viafirma platform permite alternar entre varias opciones:

- Priorizar CRLs vs. OCSP y viceversa: dado un certificado que informe en sus propiedades y políticas ambos mecanismos de validación, viafirma platform permite establecer un orden a medida del integrador, pudiendo utilizar un mecanismo u otro en el orden deseado.

- Caché de CRLs: en aquellos escenarios donde se desee optimizar los procesos de firma, normalmente en procesos de firma desatendida de muy alta concurrencia, la configuración de viafirma platform permite la activación del cacheo de CRLs; esto significa que si la última CRL consultada no caduca hasta dentro de 4 horas, durante ese tiempo la información se consulta en caché, sin necesidad de obtener la CRL.

- CRLs publicadas sobre LDAP; posibilidad de configurar el acceso a un LDAP a modo de repositorio local de CRLs en aquellos escenarios peculiares donde no permiten la salida a internet para este tipo de validaciones.

2.6. Validación de Formatos de Firma

Los formatos de firma estándares además podrán ser validados por viafirma platform, ofreciendo para ello una serie de servicios destinados a integradores e informará del cumplimiento del formato de firma, así como su integridad documental.

2.7. Formatos de Firma Soportados

La plataforma soporta prácticamente cualquier estándar vigente en la actualidad incluyendo los últimos estándares de firmas longevas. Se enumeran a continuación los principales formatos soportados:

- Firmas PDF: PAdES-BES, -EPES, -LTV
- Firmas XML: XAdES-BES, -EPES, -T, -XL y –A.
- Firmas Binarios: CAdES-BES, -EPES y –T.
- Otros formatos permitidos: CMS/PKCS#7, XMLDsig, Factura-e (XAdES-EPES con política específica de Factura-e).

Además, para los formatos que lo soporten, se permiten envolturas del tipo Attached, Detached, Enveloping y Enveloped.

2.8. Procedimientos y modalidades de firma

Entre los procedimientos de firma disponibles destacamos:

- **Firma atendida** (firma en cliente):
    - Firma en escritorio: con applet, JNLP o viafirma desktop.
    - Firma móvil: con iOS, Android y Windows UWP.
    - Firma digitalizada/biométrica: desde dispositivos móviles, Wacom y Topaz.
- **Firma desatendida** (firma en servidor):

- Sobre almacenes software: cacert y JKS
- Sobre HSM: Thales y Safenet/Gemalto, incluyendo arquitecturas de explotación de claves sobre repositorios cifrados.

- **Firma en Bucle**: interacción sobre una lista de documentos que deben ser firmados con una única "acción" de firma, permitida tanto para entornos de firma desatendida (firma en servidor) como para procesos de firma en cliente, incluyendo dispositivos móviles.
- **Firma en Lote**: procedimiento habitual en procedimientos administrativos en los que varios documentos deben ser firmados "conjuntamente", obteniendo como resultando un único fichero firmado, en formato XAdES.
- **Multifirma**: un mismo documento firmado por varios firmantes, haciendo uso de los distintos mecanismos habilitados a tal efecto por los distintos formatos de firma, tanto en procedimientos de firma desatendida (firma en servidor) como en firma en cliente, incluyendo firma desde dispositivos móviles.

2.9. Políticas de stampers y justificantes de Firma

Viafirma platform dispone de interesantes funcionalidades relacionadas con la generación de stampers de firma y recibos de firma en general.

- **Identificador único** y permanente que es la referencia única de la firma en la plataforma, útil para la creación de CSV (Código Seguro de Verificación) y permalinks de descargas.
- **Permalink**: URL personalizable destinada a la ubicación única de un recurso firmado, utilizada normalmente en justificantes de firma que deban estar accesibles por el público o interesado.
- **Códigos de barra**: con soporte a UCC128 y PDF417.
- **Códigos bidimensionales**: con soporte a la generación de QR-Codes, con información dinámica como permalinks.
- **Imágenes**: permite incluir imágenes personalizadas a modo de "sello" que ayudan a la socialización del documento firmado y que incluso permiten ser impresos.
- **Justificantes de firma**: confección de un documento PDF con el resumen de las propiedades de firma utilizando todos los elementos gráficos enumerados anteriormente, pensado sobre todo para formatos de firma que no ofrecen información semántica, como formatos XML o CMS.

Además se permite personalizar el uso de los componentes de forma combinada para adaptarse a las necesidades de cada caso:

- Rotación del stamper 90 y 270 grados.
- Transparencia de las imágenes insertadas.
- Impresión de atributos asociados a la firma, como nombre de firmantes, fecha, etc.
- Impresión selectivas en páginas del documento: primera, última, todas o específica.