Nueva versión del cliente de firma electrónica. Cliente @Firma v 3.0

Ministerio de la Presidencia

DATOS GENERALES

Antecedentes del servicio

Existe una versión anterior del cliente @Firma de amplio uso en la administración, que requería una actualización tecnológica para poder ampliar su uso.

Objetivos específicos

El objetivo de los desarrollos consiste en agregar el soporte en el cliente @firma de los nuevos entornos de ejecución recientemente aparecidos en el mercado, de próxima aparición o que, estando establecidos desde hace tiempo, cuentan ya con una tasa de público reseñable y actualmente no están soportados por el cliente.
Estos desarrollos software van enfocados a mejorar el servicio que ofrece la Plataforma, ampliando sus funcionalidades de validación y firma, entre los que citamos:

- Agregar nuevos entornos de ejecución recientemente aparecidos en el mercado o que, estando establecidos desde hace tiempo, cuentan ya con una tasa de público reseñable y actualmente no están soportados por el cliente.
- Ampliación de las capacidades del cliente para el soporte de nuevos repositorios de certificados y tipos de firma
- Inclusión de un visualizador tanto para el documento original como la información de la firma asociada.
- Análisis del código para la liberación del cliente como software libre y estudio del modelo de licencia de Software Libre a adoptar.

Recursos empleados

Personal propio de la División de Proyectos de Administración Electrónica de la dirección General de Impulso para la Administración Electrónica del Ministerio de la Presidencia y asistencia técnica de la empresa Atos origin

Resultados

Se ha conseguido un nuevo cliente mucho más ligero, que ha cubierto la nueva funcionalidad requerida.

Lecciones aprendidas y conclusiones

El pretender un cliente universal que funcione con múltiples versinoes de navegadores, sistems operativos y formatos de firma hace que la complejidad del desarrollo sea muy grande.
Es necesario definir y acotar las posibles interpretaciones de los estándares de firma y criptografía para evitar inconsistencias en formatos de firma y conseguir interoperabilidad entre diferentes aplicaciones.

Referencias y enlaces

www.ctt.map.es

DATOS ESPECÍFICOS

Características que contribuyen a la confianza en el servicio

El cliente de firma permite la generación y validación de firmas electrónicas, en una aplicación con el aval de la administración y que aporta confianza en la utilización de documentos y ficheros electrónicos firmados.

Características que contribuyen a la seguridad del servicio

Se han incorporado los últimos algoritmos de seguridad y se ha desarrollado de acuerdo a los estándares internacionales de firma electrónica, entre los que cabe destacar la utilización de los siguientes Algoritmos de huella digital: MD2, SHA-256, SHA-384, SHA-512 (este último es el más seguro de los existente en la actualidad)
Igualmente se ha introducido la posibilidad de usar certificados electrónicos desde nuevos almacenes de certificados:

- Almacén de claves de Apple Mac OS X (Apple KeyRing).
- Almacenes de certificados en disco:
  - PKCS#12 / PFX (Personal File eXchange).
  - Java KeyStore (JKS, JCEKS).
  - Certificados X.509 en disco (CER/BER/PEM/etc.) para operaciones con clave pública.
  - Almacén propio (de @firma) para claves de firmado simétrico, con soporte multi-algoritmo.
- Almacenes remotos de firma (LDAP) para operaciones con clave pública.

Aspectos de accesibilidad del servicio

Se integra con cualquier aplicación de firma pues es un applet

Aspectos de usabilidad del servicio

Se han desarrollados interfaces simples para usuario básico y otros con toda la funcionalidad para usuarios avanzados con conocimientos específicos de firma y criptografía.

Características de participación ciudadana del servicio

Para que lo use cualquier ciudadano que a su vez use cualquiera de las aplicaciones de administración electrónica en donde sea necesaria su firma.

Datos del grado de satisfacción del servicio

Nuevo desarrollo que mejora el cliente anterior.

Enumere características de multiplataforma del servicio

Sistemas Operativos:
- Apple Mac OS X (32 y 64 bits) soportado con Mozilla / Firefox , Apple Safari y Google Chrome.

Navegadores Web:
- Mozilla / Firefox 3.0, 3.1, 3.5 y 3.6, Google Chrome, 3.0 y 4.0 Apple Safari 4.0 en Windows y Mac OS X.

Formatos de firma:
- ODF para documentos OpenOffice.org 3 y superiores

Algoritmos de huella digital:
- MD2, SHA-256, SHA-384, SHA-512 (este último es el más seguro de los existente en la actualidad)

Entorno de ejecución de Java JRE 1.6 (Java 6)

Se ha introducido la posibilidad de usar certificados electrónicos desde nuevos almacenes de certificados:
- Almacén de claves de Apple Mac OS X (Apple KeyRing).
- Almacenes de certificados en disco:
  - PKCS#12 / PFX (Personal File eXchange).
  - Java KeyStore (JKS, JCEKS).
  - Certificados X.509 en disco (CER/BER/PEM/etc.) para operaciones con clave pública.
  - Almacén propio (de @firma) para claves de firmado simétrico, con soporte multi-algoritmo.
- Almacenes remotos de firma (LDAP) para operaciones con clave pública.

Enumere características de multilingüismo del servicio

Al ser una herramienta orientada a integradores, esta funcionalidad depende principalmente de la aplicación con la que se integre y del sistema operativo sobre el que se ejecute.

Cite aspectos de reingeniería del servicio

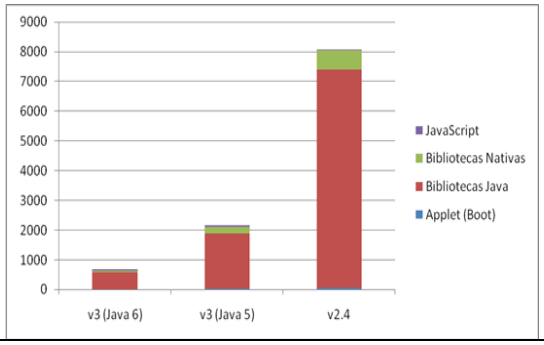
Se ha realizado una reingeniería completa de la versión anterior del cliente, que permite que se ejecute en:
- Nuevos entornos de ejecución
- Nuevos almacenes de certificados soportados
- Funcionalidad de firma masiva inteligente

La versión 3 del cliente sólo hace uso de productos externos de código abierto, evitando posibles problemas de redistribución y evolución

Enumere características de eficiencia (rendimiento, consumo) del servicio

Con la reingeniería y optimización del código se han conseguido reducciones espectaculares de tamaño de la aplicación respecto a la versión 2.4:

	v3 (Java 6)	v3 (Java 5)	v2.4
Applet (Boot)	15	35	68
Bibliotecas Java	563	1843	7320
Bibliotecas Nativas	50	234	651
JavaScript	47	47	35
	675	**2159**	**8074**



Enumere características de neutralidad tecnológica del servicio

La reconstrucción que se ha llevado a cabo del cliente lo independiza de cualquier software de pago y hace posible su futura liberación como software libre.

Enumere características de arquitecturas abiertas del servicio

El cliente ha sido transformado para basarse únicamente en distintos módulos de la JRE de Java y productos de software libre:

- BouncyCastle: Generación y manipulación de firmas binarias.
- iText: Firma y manipulación de ficheros PDF.
- JXAdES: Firma avanzada en formatos XML.

El uso preferente de las funcionalidades que provee la plataforma Java (descartando productos de terceros cuando es posible) garantiza la compatibilidad del cliente en versiones futuras de Java y en cualquier plataforma

Enumere características de reutilización del servicio

Esta herramienta se distribuye desde el Ministerio de Presidencia a todas las Administraciones Públicas españolas de forma gratuita, lo que hace que pueda reutilizarse e integrarse en otros entornos de la Administración.

Junto al cliente, se distribuye la documentación necesaria para desarrolladores e integradores. La documentación para desarrolladores describe los métodos que dan acceso a toda la funcionalidad del cliente de firma y del componente instalador.