@Firma - Plataforma de Validación de Firma Electrónica

Nombre:

Plataforma de Validación de Firma Electrónica

Acrónimo:

@Firma

Publicador:

Ministerio de Hacienda y Administraciones Públicas

Descripción:

Plataforma de validación y firma electrónica multi-PKI, que se pone a disposición de las Administraciones Públicas, proporcionando servicios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva.

Descripción detallada:

Las Administraciones Públicas ofrecen servicios públicos electrónicos en los que se necesita firma electrónica y métodos avanzados de identificación o autenticación basados en certificados digitales. Debido a los múltiples certificados que pueden utilizarse y la multitud de estándares, implantar sistemas que soporten todas las funcionalidades puede resultar complejo y costoso.

Por ello, el Ministerio de Hacienda y Administraciones Públicas ofrece la plataforma de **servicios de validación y firma electrónica multi-PKI** @firma, como un servicio de validación de certificados y firmas electrónicas, desacoplado de las aplicaciones. Es una solución de referencia para cumplir con las medidas de Identificación y autentificación descritas en el Capítulo II de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP).

El objetivo es comprobar que el certificado utilizado por el ciudadano es un certificado válido y que no ha sido revocado y que por tanto sigue teniendo plena validez para identificar a su propietario. Los servicios de la plataforma son aplicables a todos los certificados electrónicos cualificados publicados por cualquier proveedor de servicio de certificación supervisado por el Ministerio de Industria Turismo y Comercio en España, incluidos los certificados del DNIe.

La plataforma de validación del Ministerio de Hacienda y Administraciones Públicas funciona como un servicio no intrusivo, que puede ser utilizado por todos los servicios telemáticos ofrecidos por las distintas Administraciones Públicas, tanto **estatal, como autonómica o local.** Para facilitar la integración con el servicio se proporcionan unas librerías de integración **'Integr@',** que también permiten firma en servidor.

Además de ofrecerse como servicio, está disponible como software para instalar por las administraciones públicas (**modelo federado**), con múltiples utilidades de valor añadido, entre las que se encuentran la generación y validación de firmas electrónicas en múltiples formatos.

Los servicios ofrecidos a los organismos se pueden catalogar en:.

1- Servicios de validación:

- web services de **validación de firmas** digitales en múltiples formatos
- web services de **validación de certificados** electrónicos de diferentes perfiles y prestadores.
- **OCSP** multiprestador
- Validación longeva de firmas.

2- Servicios de firma electrónica:

- A través del servicio DSSAfirmaVerify se posibilita la actualización o **upgrade** de firmas electrónicas desde un formato

básico a un formato más avanzado. Es posible especificar el formato al que se desea extender la firma. Los distintos valores pueden ser: BES, EPES, T, C, X, X-1, X-2, X-L. X-L-1, X-L-2 y A. Soporta los algoritmos de hash SHA1 y SHA2 y los algoritmos de firma RSA y curvas elípticas.
- Únicamente para el modelo federado (instalación propia del organismo de la plataforma @firma', se ofrece una funcionalidad de firma en servidor.

3- Para la firma de trámites automatizados, se proporciona una API (**Integr@**) que proporciona funciones de creación de firmas en diferentes formatos, así como facilita la integración con los Web Services avanzados de @firma. Dicha API puede descargarse desde el área de descargas de esta misma página.

4-Para la firma de los ciudadanos en local, independiente de la plataforma de validación pero como parte de la 'Suite @firma' se proporciona un componente que se integra con los navegadores de los usuarios, para facilitar la incorporación de la firma en los tramites informatizados. Permite realizar firmas desde entornos de sobremesa y desde dispositivos móviles. Puede consultar más información de este componente en la página especifica del cliente de @firma.

5- Servicios de sellado de tiempo. Puede consultar más información de este servicio en la página especifica de la TS@

6- Otros componentes de la Suite. Puede consultar el resto de servicios y productos de la 'Suite @firma' en la página de la Suite

7- Soporte a la Operación: a través de servicios de soporte a la integración, apoyo a la evolución hacia nuevos estándares de firma electrónica.

Requisitos:

Para integrarse en @firma es necesario seguir unos pasos sencillos:

1. Estar conectado a la red SARA.
2. Ponerse en contacto con el servicio de soporte a través del formulario habilitado al efecto y facilitar sus datos de contacto.
3. El equipo de soporte le informará de los prerrequisitos y le facilitará el formulario para el control de acceso que el organismo debe cumplimentar. Junto con la documentación de bienvenida, se facilitará el Manual de Programación de WS de @firma junto con las instrucciones técnicas necesarias para conectar las aplicaciones de los servicios de administración electrónica a la Plataforma @firma. Dicha información también está disponible en el área de descargas, para usuarios de las administraciones públicas registrados en el PAE.
4. El organismo debe conectar las aplicaciones de servicios de administración electrónica para acceder a la Plataforma a través de servicios web.
5. Para acceder a la totalidad de la documentación es necesario ser un usuario registrado, para ello, acceder a la página del PAE y darse de alta cómo usuario en el menú de la derecha: "Acceso a Usuarios" -> "Registrarse"

Ventajas:

Los beneficios que la plataforma facilita a los organismos son:

- El reconocimiento de múltiples certificados.
- Independencia del prestadores de servicios de certificación ya que soporta de varios protocolos de validación de certificados (OCSP, HTTP, LDAP).
- El uso de Políticas de Seguridad para garantizar la confidencialidad, autenticidad e integridad de todas las transacciones realizadas.
- Mayor eficiencia y menor coste en la utilización de la firma electrónica en los servicios telemáticos prestados.
- Hace transparente para las aplicaciones el uso de diferentes formatos de firma electrónica como PKCS#7, CMS, XML signature, XAdES, CAdES, PAdES
- La interoperabilidad con los servicios proporcionados por las Administraciones Públicas. Se hace extensible la interoperabilidad al ámbito Europeo y al de sus organismos e instituciones al ser contempladas las especificaciones de compatibilidad con la Unión Europea.
- Reducción de costes: el servicio permite optimizar el coste de los servicios de validación de certificados por cada aplicación.
- Innovación: la plataforma de la validación multi-PKI se ha convertido en el primer servicio centralizado principal que proporciona servicios electrónicos horizontales a todas las Administraciones Públicas del país gratuitamente.

Normativa relacionada:

Capítulo II de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP).

Red de Origen:

SARA

Organismos destinatarios:

Todas las AA.PP.

Requisitos de acceso:

Para integrarse en @firma es necesario seguir unos pasos sencillos: Estar conectado a la red SARA Ponerse en contacto con el servicio de soporte y facilitar sus datos de contacto. El equipo de soporte le informará de los prerrequisitos y le facilitará el formulario para el control de acceso que el organismo debe cumplimentar. Junto con la documentación de bienvenida, se facilitará el Manual de Programación de WS de @firma junto con las instrucciones técnicas necesarias para conectar las aplicaciones de los servicios de administración electrónica a la Plataforma @firma. El organismo debe conectar las aplicaciones de servicios de administración electrónica para acceder a la Plataforma a través de servicios web implementados en tecnología Microsoft® o Java. Las Comunidades Autónomas firmarán un convenio con el Ministerio de la Presidencia, al cual deberán adherirse las Entidades Locales que deseen acceder a la Plataforma. Por último, para acceder a la totalidad de la documentación es necesario ser un usuario registrado, para ello, acceder a la página del CTT (http://www.ctt.mpr.es) y darse de alta cómo usuario en el menú de la derecha: Acceso a Usuarios -> Registrarse

Información Tecnica:

Los servicios que ofrece son:

Validación de certificados X.509 según la RFC 3280, de las Autoridades de Certificación incluidas en la plataforma. Entre las funcionalidades de validación se pueden destacar:

Reconocimiento y validación del DNI electrónico emitido por la Dirección General de la Policía, y de múltiples prestadores.
Validación de certificados X.509 según la RFC 3280, de todas las Autoridades de Certificación reconocidas en el país por el Ministerio de Industria
Validación Multinivel de certificados (en el caso de estructura de certificación de más de dos niveles).
Obtención mediante un parseo en XML, de la información correspondiente a los campos del certificado, según la Política de Confianza definida para el tipo de certificado de que se trate.
Caché de validación configurable en tiempo, para evitar tener que acceder al PSC ante validaciones de un mismo certificado en un corto período de tiempo.

Validación de Firma:

Hace transparente para las aplicaciones el uso de diferentes formatos de firma electrónica como PKCS#7, CMS, XML signature, PDF, ODF, XAdES, CAdES, PAdES, y diferentes algoritmos criptográficos...
Validación de firma vía servicios web (WS) de un elemento firmado, indicando si la firma es correcta y la validez, fechado de tiempo, etc. También se realiza la interpretación de los campos de los certificados a un XML homogéneo.

Generación de Firma:

A través del servicio DSSAfirmaVerify se permite la actualización o upgrade de firmas electrónicas a un formato más avanzado, para ello es posible especificar el formato al que se desea extender la firma. Los distintos valores pueden ser: BES, EPES, T, C, X, X-1, X-2, X-L. X-L-1, X-L-2 y A.
En estos momentos los algoritmos de hash soportados son SHA1 y SHA2 (el resto se hallan obsoletos).
En estos momentos los algoritmos de firma digital soportados son RSA y curvas elípticas.

Gestión y administración

La plataforma realiza la gestión y administración de los Prestadores de Servicios de Certificación adheridos. Todas las operaciones realizadas en la plataforma son registradas para la auditoria y trazabilidad del sistema.

Demostrador de @firma : Acceso directo a los servicios de @firma (herramienta VALIDe).

URL información:

http://administracionelectronica.gob.es/es/ctt/afirma

Mail:

https://ssweb.seap.minhap.es/ayuda/consulta/CAID