

Comunicación

**Aplicación VALIDe:
Validación on-line de certificados y documentos
electrónicos para los ciudadanos.**



TEMAS RELACIONADOS:

Servicios para los usuarios:

- **Transparencia y participación ciudadana**

Implicaciones económicas y mercado único

- **Documento electrónico**

Eficiencia y sostenibilidad

- **Interoperabilidad entre Administraciones Públicas**

Iniciativas legales y tecnológicas.

- **Cumplimiento de la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos.**
- **Identidad digital, seguridad y reutilización**
- **Medios de identificación y autenticación en las Administraciones Públicas**
- **Infraestructuras y servicios comunes de la Administración electrónica**

Laura Cabezas Manso,

Dirección General para el Impulso de la Administración Electrónica
Ministerio de la Presidencia

1.INTRODUCCIÓN 4
2.DESCRIPCIÓN DEL SERVICIO 4
3.DESCRIPCIÓN FUNCIONAL 6
4.ARQUITECTURA TÉCNICA..... 9
5.REQUISITOS DE USO 10
6.RESULTADOS OBTENIDOS 11

1. Introducción

Las Administraciones Públicas ofrecen a los ciudadanos, 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 formatos de firma electrónica y los distintos certificados que pueden utilizarse para la identificación y la firma, implantar sistemas que soporten todas las funcionalidades puede resultar complejo y costoso.

El Ministerio de la Presidencia ofrece a los ciudadanos un servicio on-line para la validación de los documentos electrónicos firmados electrónicamente mediante certificados reconocidos, independientemente del formato de la firma. Se permite la validación de las firmas electrónicas de las Administraciones Públicas, y la visualización de los documentos firmados cuando estos están presentes en las firmas.

Aporta transparencia a la acción de la administración frente a los ciudadanos, proporcionando un punto único de verificación de todas las firmas electrónicas generadas por las Administraciones Públicas y facilita la confianza de los ciudadanos en los servicios públicos electrónicos.

Es una solución de referencia para cumplir con las medidas de Identificación y autenticación descritas en el Capítulo II de la Ley 11/2007 de Acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).

2. Descripción del servicio

El servicio VALIDe, de Validación de Firmas y Certificados Online, del Ministerio de la Presidencia funciona como un servicio no intrusivo o cerrado, que puede ser utilizado por todos los interesados de las distintas Administraciones Públicas, tanto estatal, como autonómica o local. Está disponible tanto a través de la red SARA como a través de Internet para su uso por los ciudadanos, a través de la URL:

<https://valide.redsara.es>

Los servicios son aplicables a todos los certificados electrónicos publicados por cualquier proveedor de servicio de certificación acreditado en España, incluidos los certificados de la tarjeta del DNIe del ciudadano, y los certificados de sede, sello y empleado público creados mediante la ley 11/2007 y especificados en el RD 1671/2009. El Ministerio de Industria, Turismo y Comercio, a través de la Dirección General para el Desarrollo de la Sociedad de la Información, es la autoridad competente para determinar cuáles son estos certificados acreditados en España. Se pueden consultar los certificados admitidos en la url:

<http://www.mityc.es/dgdsi/es-ES/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx>

Cuando se realizan trámites telemáticos, es necesario verificar la identidad de la otra parte con la que se realiza el trámite. Si esta identidad se acredita mediante un certificado electrónico, este servicio permite comprobar la validez de la firma y el estado del certificado con el que el ciudadano o administración está firmando el trámite. Para esta comprobación se utiliza la plataforma de validación del Ministerio de Presidencia @firma, delegando en ella la verificación de las credenciales del certificado o DNIe utilizado.

GOBIERNO DE ESPAÑA CTT VALIDe

Inicio
Validación de certificados y firmas
Acceso a usuarios registrados
FAQs

Validación de certificados y firmas

VALIDe

Validar Certificado
Si dispone de un certificado digital emitido por cualquier entidad de servicio de certificación reconocida, puede acceder en línea a su validez

Validar Certificado Sede
Podrá comprobar las URLs de sedes electrónicas, verificando la validez del certificado que contienen.

Validar Firma
Consulte la validez de un documento firmado electrónicamente con múltiples formatos y tipos de certificados, como facturas electrónicas, contratos, etc.

Realizar firma
Firma electrónicamente un documento con tu DNI electrónico o cualquier otro certificado reconocido con las máximas garantías de integridad y autenticidad.

Acceso a usuarios registrados
Si dispone de usuario, puede acceder introduciendo su nombre y contraseña

FAQs
Consulte nuestras FAQs si tiene alguna duda

VERSION 1.2 Accesibilidad | Guía de navegación Contactar

W3C HTML 4.01 W3C WAI-AA WCAG 1.0

Los servicios ofrecidos a los organismos se pueden catalogar en cinco bloques:

1- Validar Certificado

Permite validar el estado de un certificado digital emitido por cualquier entidad de servicio de certificación reconocida, tanto en autenticidad, vigencia y estado de no revocación. El objetivo de este servicio es permitir a un usuario comprobar que el certificado utilizado es un certificado válido y que no ha sido revocado y que por tanto sigue teniendo plena validez para identificar a su propietario.

- 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 de la información correspondiente a los campos del certificado.
- Validación de certificados extraídos de sedes electrónicas.

2- Validar Sede Electrónica

Se permite comprobar la validez de una sede electrónica a través del estado del certificado digital de sede electrónica emitido por cualquier entidad de servicio de certificación reconocida, tanto en autenticidad, vigencia y estado de no revocación.

- Validación de sedes electrónicas a través de su URL.
- Verificación que la URL introducida coincide con aquella informada en el certificado de sede.

3- Validar Firma

Permite consultar la validez de un documento firmado electrónicamente con múltiples formatos y tipos de certificados, como facturas electrónicas, contratos, resguardos firmados electrónicamente de una aplicación electrónica como un registro electrónico, etc.

Se comprueba la firma electrónica, devolviendo al usuario la identidad del firmante. En caso de existir múltiples firmantes, se verifican todos ellos y se representa la jerarquía y orden de firma. El firmante puede ser tanto un ciudadano como un funcionario o una administración a través de actuación automatizada mediante sello electrónico.

En caso que la firma incluya el documento firmado, también se permite al ciudadano el acceso a éste.

4- Realizar Firma

Permite firmar electrónicamente un documento con cualquier certificado reconocido del que se posea la clave privada, con las máximas garantías de integridad y autenticidad.

- Por defecto se realiza firma en formato XAdES implícito, con firma envolvente, mediante un algoritmo RSA con SHA1.
- Para usuarios registrados además permite el uso de diferentes formatos de firma electrónica como PKCS#7, CMS, XML signature, XAdES y CAdES.
- Para acceder a esta funcionalidad es necesario la instalación de un applet que proporciona un cliente de firma que permite la firmar electrónica. Para ello se emplean los certificados digitales de usuario que se hallan instalados en el navegador o disponibles en tarjeta inteligente, como la del DNI electrónico. Los navegadores y sistemas operativos soportados para la realización de firmas se indican en www.ctt.map.es/web/clientefirma

5- Demostrador de servicios de @firma

Para los usuarios registrados de las Administraciones Públicas proporciona además un demostrador del funcionamiento de los web-services de @firma. De esta forma facilita a las Administraciones la integración de los servicios de validación y firma de la Plataforma @firma en sus servicios electrónicos. Permite evaluar todos los servicios y realizar las pruebas funcionales necesarias.

1. Descripción Funcional

Los ciudadanos tras realizar un trámite electrónico pueden disponer de un recibo electrónico firmado ó un documento firmado.

Éste recibo puede estar compuesto de un documento en cualquier formato (pdf, doc, xml, etc) y una firma electrónica, la cual puede estar también en cualquier formato soportado por @firma (CAdES, XAdES, Xmlsignature, Pkcs#7, etc). Habitualmente en el recibo electrónico / documento firmado además se adjunta el certificado del firmante, pero en otras ocasiones el usuario puede necesitar también validar un certificado de forma separada a la firma electrónica en la que estaba incluido. Para dar solución a esta problemática se realiza esta aplicación Web VALIDE, que será accedida mediante un navegador.

Para usar la aplicación el usuario se conecta al portal de manera transparente y por defecto, con un perfil invitado. También podrá acceder con roles diferentes accediendo al menú "Acceso de Usuarios Registrados". Los modos de acceso son:

- Sin credenciales, que asociará al usuario el perfil invitado. Es el utilizado por defecto.
- Con credenciales (almacenados en el directorio LDAP del CTT), según los cuales el usuario puede asociarse al perfil "usuario registrado" o bien al perfil "administrador".

Para lo cual se dispondrá de una tabla local en la que se encontrarán los identificadores de los administradores del sistema.

Se dispone de unas funcionalidades u otras según el perfil del usuario.

Una vez el usuario accede y haya sido asignado a un perfil de uso, se le muestran las acciones de que dispone, que pueden ser:

- Validar certificado digital en fichero
- Validar certificado sede en una url
- Validar firma digital en fichero
- Realizar una firma digital
- Demostrador de WS de @firma
- Administración
- Faqs
- Finalizar Sesión

Toda la aplicación será accesible en base a la normativa Doble-A del W3C-WAI facilitando el acceso al mayor número de personas posible que deseen utilizarlo. En la aplicación existe un "CAPTCHA" para evitar los "robots".

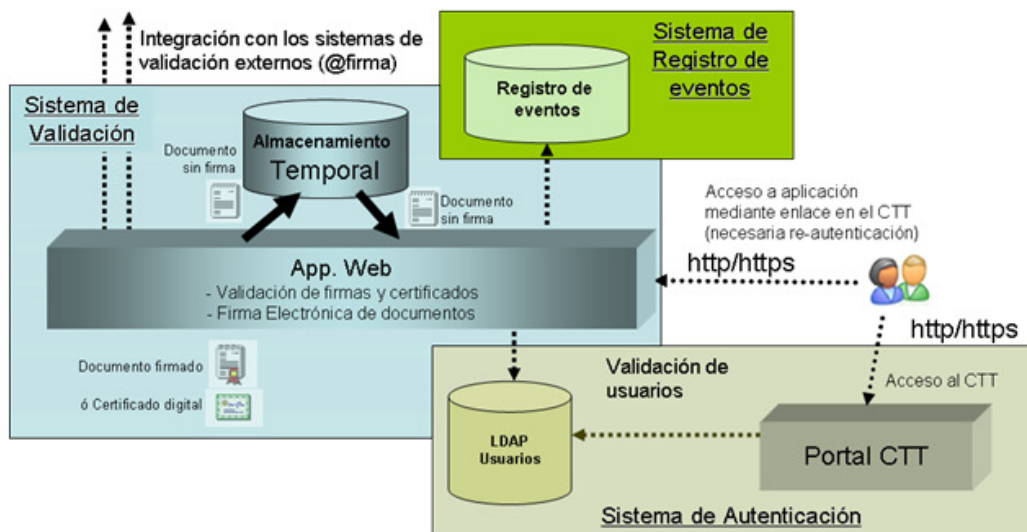


Imagen "Captcha" con cadena: "7gdpf" con los botones "Recargar Captcha"

Una vez comprobado que el captcha es correcto, el documento será validado haciendo uso de los servicios del sistema de validación externo que haya sido configurado (@firma).

Debido a que los servicios de @firma requieren de una autenticación, en cada petición SOAP se enviarán las credenciales de la aplicación. Todas las transacciones generadas serán además anotadas en el registro de eventos, se registrará: Fecha y hora, Dirección IP del usuario, Organismo al que pertenece (si procede), ID Usuario (si procede), Acción realizada (en este caso "Validación de firma-e").

A continuación se muestra el esquema de la solución con la integración entre todos los sistemas y aplicaciones. Posteriormente se detallarán los componentes sus funcionalidades.



- **Validación de certificado.**
Esta funcionalidad está disponible para todos los usuarios. El usuario puede validar certificados instalados en el navegador o contenidos en ficheros locales del usuario. A los usuarios registrados se les devolverá información adicional de la validación.

El usuario seleccionará el fichero que contiene el certificado a validar y completará el valor del captcha. El certificado será enviado al servidor llamando a @firma para la realización de esta tarea. Se mostrará al usuario la pantalla con el resultado de la validación con los detalles del certificado. Internamente se hará uso de la funcionalidad de @firma de validación de certificados mediante Web Service (y no mediante OCSP), ya que devuelve los parámetros del certificado.

- **Validación de sede.**
Esta funcionalidad está disponible para todos los usuarios. El usuario puede validar una sede electrónica a través de su URL. Se realizarán las mismas operaciones que en el caso anterior, pero se verificará además que la URL introducida coincide con la sede contenida en el certificado.
- **Validación de firma / Visualización del contenido.**
Esta funcionalidad está disponible para todos los usuarios. El usuario puede validar la firma recibida de la administración, y en el caso de que el documento esté contenido en la firma, podrá extraerlo. A los usuarios registrados se les devolverá información adicional de la validación.

El usuario seleccionará el fichero que contiene la firma a validar y completará el valor del captcha. El fichero será enviado al servidor llamando a @firma para la realización de esta tarea. Se mostrará al usuario la pantalla con el resultado de la validación con los detalles de la firma y del certificado. Haciendo uso de la información contenida en el propio fichero firmado, si existe, se le indicará la aplicación con la que podrá abrir el contenido. Además de la posibilidad de la descarga del contenido firmado, se le mostrará la información relativa a la firma. En el caso de que se trate de una firma realizada por varios firmantes se muestra la información de todos ellos (Nombre y apellidos, DNI...). Ya que algunos formatos de firma soportan la inclusión de un sello de tiempo, si se encontrara, se mostrará la información del mismo.

- Realización de firma.
Esta funcionalidad está disponible para todos los usuarios. El ciudadano puede realizar firmas de sus documentos a través de las utilidades que proporciona el cliente de firma de @firma. Esta funcionalidad está disponible para todos los usuarios. Los usuarios anónimos realizan todas las firmas en formato XAdES implícito. Para los usuarios registrados se darán más opciones. Es necesario que el usuario disponga de un certificado digital instalado en el navegador o en tarjeta inteligente, con los driver correspondientes.

El cliente de @firma es el encargado de la realización de firma conforme a los criterios requeridos por el usuario (tipo de firma, formato, etc.). El resultado de la firma será un fichero que se almacenará en el sistema del usuario. Se comprueba inicialmente si el componente está instalado, ofreciendo al usuario la instalación en caso de no ser detectado. Además en caso de detectarse una nueva versión se le informará al usuario de su existencia y se le ofrecerá la posibilidad de su actualización.

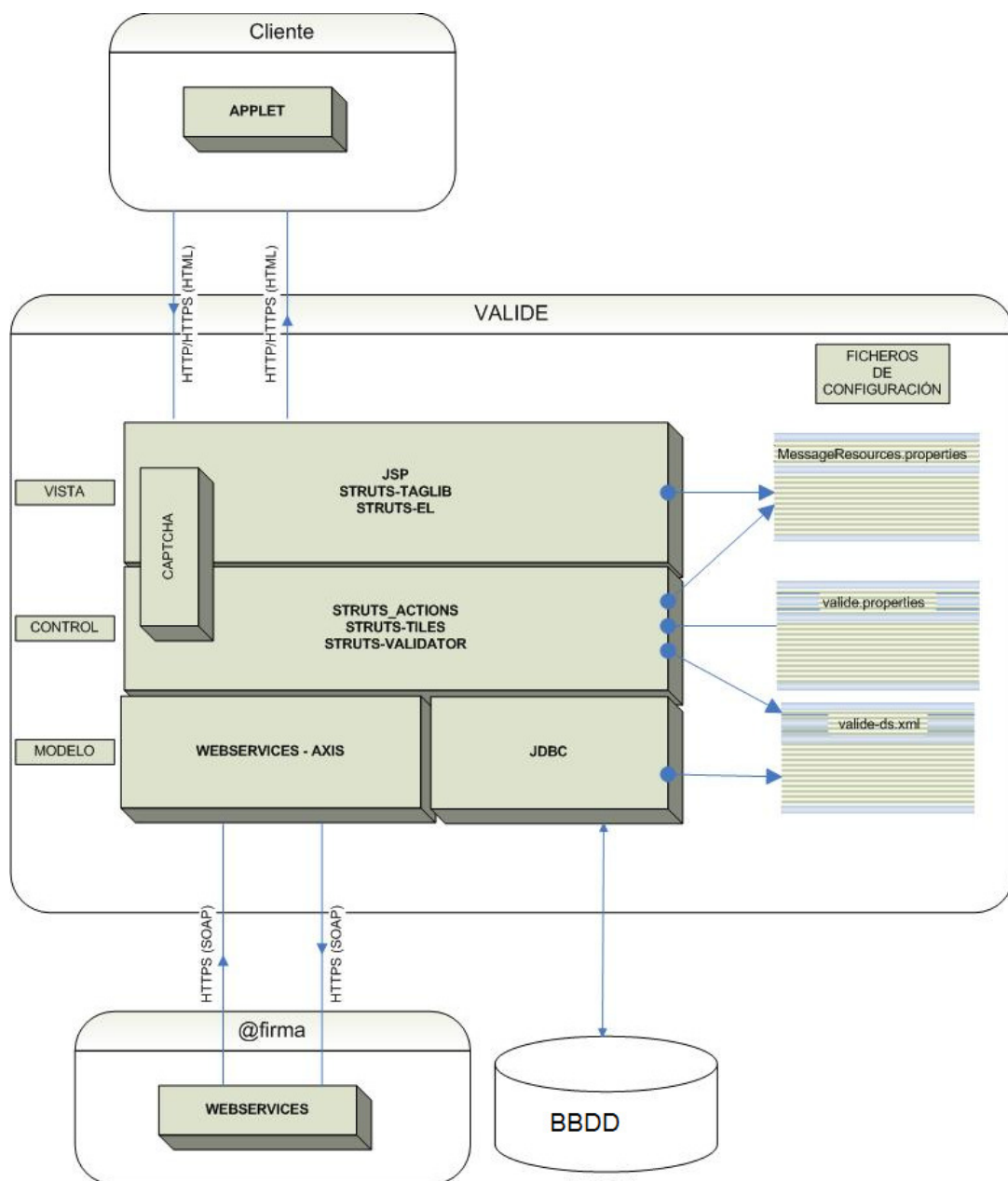
1. Arquitectura Técnica

El servidor en el que se encuentre la aplicación debe reunir las siguientes características:
JBoss 4.2.1GA

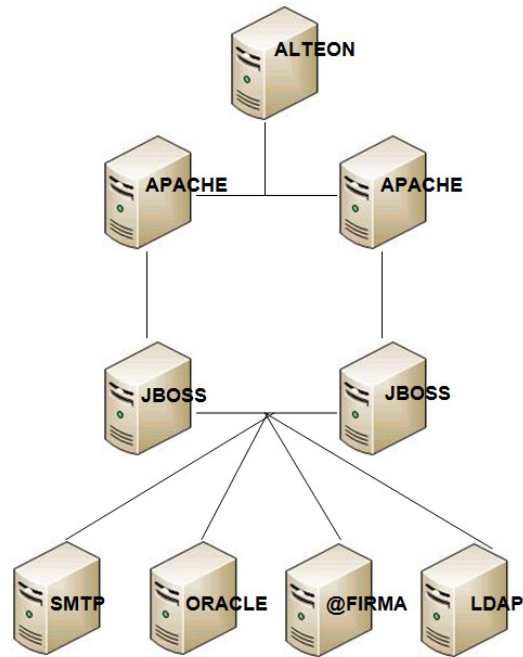
- Versión de Java: J2SDK 1.5.0_15
- Base de datos: ORACLE. En la misma máquina o en otra a la que la aplicación pueda tener acceso.

La aplicación será desarrollada en el lenguaje Java. Las tecnologías con las que se implementará la aplicación serán:

- Struts 1.3.8: Struts-Actions, Struts-Validator, Struts-Tiles, Struts-Tags.
- Axis 1.4.
- JSP (JSTL 2.0).
- JDBC.
- Jcaptcha 1.0-RC6.



La arquitectura se muestra en el diagrama siguiente:



1. Requisitos de uso

Para utilizar los servicios de validación de certificados y sedes, o la validación de firmas electrónicas es necesario:

- Conexión a Internet.
- Acceder desde un navegador y sistema soportado por VALIDE:
 - a) Navegador:
 - Firefox 1.5 ó superior.
 - Microsoft Internet Explorer 6 ó superior.
 - b) Sistemas operativos:
 - Microsoft Windows 2000 / XP / Vista
 - Sistemas LINUX (Red Hat, Guadalinex, Ubuntu, etc)

Para realizar firmas digitales de documentos, se ha de cumplir lo siguiente:

- Tener instalada en su equipo la máquina virtual de Java (JRE) con versión 1.5.22 o posterior, y que su navegador utilice dicha JRE como motor de Java. Se recomienda el uso de maquinas virtuales java 1.6
- Para realizar una firma digital necesitará además un certificado digital del que se disponga la clave privada (con extensión pfx o p12), instalado en el navegador. También se permite realizar firmas electrónicas a través de certificados en tarjeta inteligente (DNI-e) con los driver instalados.
- Disponer de permisos en su equipo para poder instalar el componente de firma electrónica o applet.

Consultar en la página del cliente de @firma los navegadores y sistemas operativos soportados para la realización de firmas.

www.ctt.map.es/web/clienteafirma

Si se desea acceder a la funcionalidad avanzada para las Administraciones Públicas es necesario estar conectado a la red SARA y registrarse como usuario del Centro de Transferencia de Tecnología (CTT).

1. Resultados Obtenidos

Las ventajas que proporciona este servicio son las siguientes:

- Los ciudadanos podrán disponer de un punto único de acceso para la validación de firmas electrónicas basadas en certificados electrónicos independientemente de la administración que generó el documento electrónico.
- Los ciudadanos podrán disponer de un punto único de acceso para la validación de sedes electrónicas, distinta de la propia sede, para cualquier prestador de servicios de certificación que emita el certificado de la sede.
- Los ciudadanos podrán disponer de un punto único de acceso para la validación de certificados digitales, para todos los prestadores de servicios de certificación reconocidos en España.
- Acercamiento de la firma electrónica a ciudadanos y administraciones. Mediante este servicio se proporciona un interfaz sencillo para comprobar la validez de una firma y de un certificado digital, y para la realización de firmas electrónicas, lo que permitirá a los usuarios familiarizarse con los servicios de firma electrónica.
- Los ciudadanos podrán estar en posesión de los documentos firmados por las administraciones, no solo de un justificante, lo que les aporta mayores garantías. Estos documentos firmados suelen tener formatos no visibles a través de herramientas convencionales. Mediante el servicio de validación de firmas podrán ver el contenido de los documentos electrónicos firmados.
- Extensión de la confianza en los servicios públicos digitales. Los ciudadanos y las Administraciones Públicas podrán comprobar on-line la validez de las firmas y de los certificados digitales.
- Se facilita la integración con la plataforma de validación de certificados y firma electrónica del MPR, @firma, mediante un demostrador del funcionamiento de los web-services.