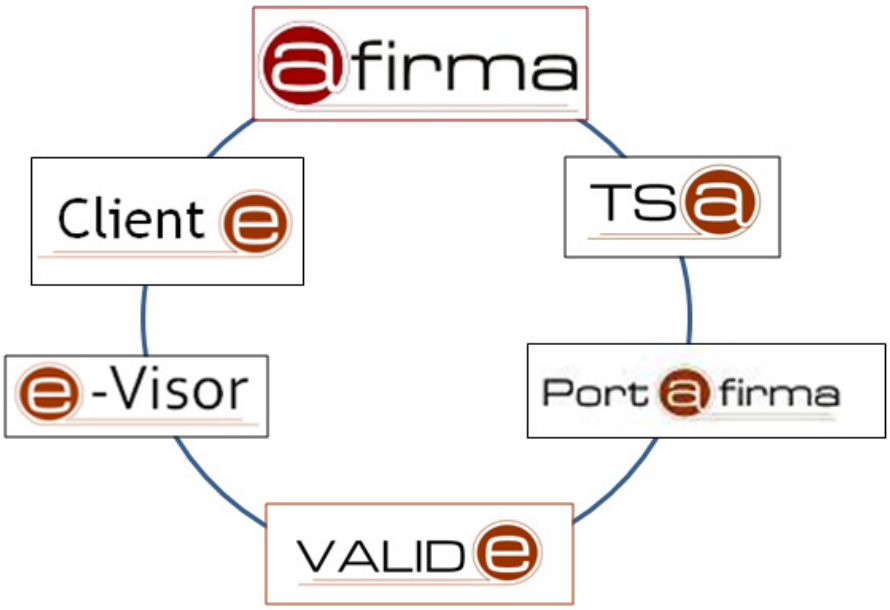
▫▫▫▫

Un mundo de servicios de firma electrónica: suite de aplicaciones y utilidades de firma electrónica @firma

- ***Autoridad de Validación @firma***
- ***Autoridad de sellado de tiempo TS@***
- ***CLIENTe @firma***
- ***Port@firmas***
- ***VALIDe***
- ***e-VISOR***



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 autentificación en las Administraciones Públicas**
- **Infraestructuras y servicios comunes de la Administración electrónica**

Miguel Álvarez Rodríguez
Laura Cabezas Manso,
Dirección General para el Impulso de la Administración Electrónica

Ministerio de la Presidencia

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.

La introducción de la firma-e y el DNI-e es ya una necesidad en la tramitación telemática de todas las Administraciones públicas, sin embargo, el desarrollo y extensión tecnológica que están teniendo está siendo desigual y pausada en el tiempo. Entre los inhibidores del uso generalizado de estas nuevas técnicas de identificación y firma, está la complejidad tecnológica que hay que introducir en los sistemas de información, los elevados costes e inversiones a realizar o la falta de recursos especializados disponibles en los diferentes organismos Públicos.

Conocedores de estos condicionantes y en el ejercicio de las potestades que tiene atribuidas, el Ministerio de la Presidencia ha implantado un proyecto denominado "Plataforma de validación y firma electrónica" compuesto por una serie de servicios y utilidades de firma electrónica. Este proyecto se centra en facilitar a las aplicaciones los complementos de seguridad necesarios para implementar la autenticación y firma electrónica avanzada basada en certificados digitales de una forma eficaz y efectiva, así como el acceso de los ciudadanos a la verificación de los documentos firmados. Se ofrecen de esta manera servicios que impulsan el uso de la certificación y firma electrónica en los sistemas de información de las diferentes Administraciones públicas que así lo requieran.

En concreto, la plataforma @firma 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). Para conseguir estos objetivos, una de las medidas adoptadas ha sido el impulso del uso de la firma y certificación electrónica. De entre ellas, una de las de mayor trascendencia ha sido la sustitución gradual del Documento Nacional de Identidad actual por el equivalente en formato electrónico, lo que se ha venido en denominar DNI-e.

2.Plataforma de Validación @firma

La plataforma de Validación y firma @firma ofrece un conjunto de servicios que facilita a las aplicaciones los complementos de seguridad necesarios para implementar la autenticación y firma electrónica avanzada basada en certificados digitales de una forma eficaz y efectiva. Se ofrecen así servicios que impulsan el uso de la certificación y firma electrónica en los sistemas de información de las diferentes Administraciones públicas.

Los servicios ofrecidos por la plataforma permiten la validación de los certificados digitales, la generación y validación de firmas electrónicas en múltiples formatos, auditoria de las transacciones y documentos firmados, sellado de tiempos o la compatibilidad con certificados digitales generados por múltiples prestadores de servicios de certificación.

Todas estas características convierten a @firma en una solución completa de autenticación y firma electrónica.

Los servicios ofrecidos a los organismos se pueden catalogar en los bloques que se describen a continuación, basándose la mayoría en web services compatibles con las tecnologías java y .NET. Todos los web services se encuentran disponibles tanto en

castellano como en inglés, facilitando así la integración e interoperabilidad con soluciones existentes en los organismos usuarios.

A) Servicios de validación.

Se corresponde con todos aquellos servicios orientados a obtener información de certificados y de la validación de certificados y firmas electrónicas. Entre los servicios de validación de certificados X.509 según la RFC 3280, se admite tanto el protocolo OCSP como la invocación de web services específicos.

Se permite realizar una validación completa de la firma electrónica proporcionada a la Plataforma. Como validación completa se entiende:

- Validación de la firma digital contenida en la firma electrónica frente a los datos proporcionados.

- Validación del certificado X.509 empleado y contenido en la firma electrónica. Se validará su integridad, periodo de validez y estado de revocación. Tanto el periodo de validez como el estado de revocación del certificado se comprueban frente a la fecha actual en caso que la firma electrónica no posea sello de tiempo o frente al mismo en caso contrario.

- Validación de la confianza del certificado. Se comprueba que el certificado y su emisor sean reconocidos y soportados por la plataforma. Este servicio puede ser empleado para validar tanto las firmas electrónicas generadas por la plataforma o el cliente de firma suministrado por el MPR como aquellas ajenas, siempre y cuando su formato sea soportado.

Los web services incluidos son:

- Validación de Certificados X.509v3 mediante http, ftp, ldap, OCSP
- Obtención de información de certificados en un XML normalizado.
- Validación de firma electrónica en múltiples formatos: XMLDsig, XadES, CADES...
- Validar Firma Bloques Completo o en documento
- Validar muktifirmas (tanto cosign como countersign)
- Validación Multinivel de Certificados Reconocidos por @firma
- OCSP responder

B) Servicios de realización de firma electrónica.

Engloba todos los servicios relativos a la realización de firmas electrónicas por parte de la Plataforma. Dichas firmas pueden ser de la propia Plataforma o solicitudes de firmas de servidor de los organismos, a partir de certificados hospedados en dispositivos seguros criptográficos de creación de firmas.

Este servicio permite a una aplicación cliente realizar, con el certificado de firma de servidor indicado, y siempre dentro del contexto de la plataforma @firma, una firma electrónica. Es decir, la generación de dicha firma se lleva a cabo en la plataforma, de ahí el nombre de firma electrónica de servidor.

Las firmas se pueden construir en varios formatos: PKCS#7, CMS (compatibilidad con todas sus versiones definidas por la IETF1), XMLSignature Básico, XMLSignature avanzado (XadES), CMS avanzado (CadES), PDF y ODF.

C) Validación de firma electrónica en múltiples formatos.

Proporciona la funcionalidad de verificar la firma de un fichero dado siendo capaz de reconocer los siguientes formatos de firma: PKCS7, CMS, XMLDSignature, XadES, CADES. Todos estos formatos son admitidos para firmas 'attached' o 'detached', enveloping, enveloped, explícitas o implícitas.

Como resultado de una verificación de firma se obtienen los datos de 'estado de la firma' (firma correcta o incorrecta), certificado/s (enumeración de el/los certificado/s con los que se firmó el fichero verificado), 'sello de tiempo' (en caso de tenerlo muestra la fecha y la hora en la que se firmó el fichero) y 'certificado de la TSA' (certificado utilizado por el servidor de sello de tiempo para generar el mismo).

D) Certificados reconocidos por la Plataforma

La plataforma @firma admite certificados digitales reconocidos conforme el estándar ITU-T X.509 v3, emitidos por múltiples Prestadores de Servicios de Certificación. Todos los prestadores se encuentran inscritos en el registro de la Secretaria de Estado de Telecomunicaciones y para la Sociedad de Información del Ministerio de Industria, Turismo y Comercio de autoridades conforme a lo establecido en el artículo 30 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Se pueden consultar los certificados admitidos en la url: http://www.mityc.es/dgdsi/es-ES/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx

Actualmente la plataforma @firma valida más de 100 tipos de certificados de 13 Prestadores de Servicios de Certificación y uno extranjero. Ya se validan además los nuevos mecanismos de firma de las AAPP según la Ley 11/2007: Certificado de sede, sello y empleado público.

Puede encontrar amplia información en el documento Declaración de Prácticas de Certificación de @firma, a través del servicio de soporte de @firma o en la página web: http://www.dnielectronico.es/seccion_aapp/rel_autoridades.html

3.Autoridad de sellado de tiempo TS@

La Autoridad de Sellados de Tiempo (TSA) es una solución tecnológica que se centra en proporcionar servicios de sellado de tiempo, emisión de sellos de tiempo, validación de sellos de tiempo y resellado. El servicio de sellado de tiempo permite emitir sellos de tiempo de los documentos electrónicos que los Organismos suministren al servicio. Un sello de tiempo es una firma electrónica realizada por una Autoridad de Sellado de Tiempo (TSA) que permite demostrar que los datos suministrados han existido y no han sido alterados desde un instante específico en el tiempo (proveniente de una fuente fiable de tiempo).

El Ministerio de la Presidencia dispone de una TSA, la cual está sincronizada (por NTP y mediante Stratum2 con conexión GPS) con el Real Observatorio de la Armada. El Real Observatorio de la Armada tiene como misión principal el mantenimiento de la unidad básica de Tiempo en España así como el mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC (ROA), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (R. D. 23 octubre 1992, núm. 1308/1992). Los servicios de la TSA están disponibles para todo Organismo o Entidad Pública perteneciente a las diferentes Administraciones Públicas sea cual sea su ámbito: Administración General del Estado, Comunidades Autónomas, Diputaciones Provinciales o Entes Locales.

Desde el Ministerio de la Presidencia se ofrece la ayuda y el soporte necesario para que los Organismos integren estos servicios de certificación de valor añadido en los sistemas de información de Administración Electrónica que admitan autenticación y firma electrónica basada en certificados digitales. Para ello se ha desarrollado un cliente a integrar dentro de las aplicaciones de aquellos Organismos que deseen dotar de una referencia válida de tiempo. TS@ es una plataforma de sellado de tiempo, con las funcionalidades de sellado, validación y resellado de sellos de tiempo. Los servicios disponibles en la TSA son:

- **1 Solicitar sello de tiempo.** Por medio de este servicio se proporciona la funcionalidad de generar un sello de tiempo para una acción de firma de datos o de documento.
- **2 Validar sello**. A través de este servicio se proporciona la posibilidad de verificar la validez de un sello de tiempo contenido en una firma digital.
- **3 Solicitar resellado de tiempo.** La utilidad más importante del servicio de resellado de tiempo consiste en preservar la longevidad de la validez de los sellos generados sobre los documentos o transacciones, en caso de que se pueda poner en cuestión la validez de un sello emitido. Por medio de este servicio se proporciona la funcionalidad de generar un nuevo sello de tiempo para una acción de firma de datos o de documento.

Actualmente la TSA publica los servicios de sello de tiempo de las formas siguientes:

-Notación abstracta ASN.1, de esta forma se cumple con las especificaciones de la IETF RFC3161, utilizando sintaxis de peticiones y respuestas en notación abstracta ASN.1 codificado en DER.
-Web Service diseñados para facilitar la integración con las aplicaciones, utilizando la especificación de mensajes XML-SOAP.

Los protocolos de sellado de tiempo, en los cuales se basa la plataforma, se encuentran especificados en las siguientes normas:

•RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocols ", estándar definido por la Internet Engineering Task Force (IETF) para el protocolo Time Stamp.

•IETF RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs).

•ETSI TS 102 023 Policy requirements for time-stamping authorities.

•XML Timestamping Profile of the 2 OASIS Digital Signature Services (DSS) ver. 1.0

4.Cliente de @firma

El Cliente de Firma es una herramienta de firma electrónica que funciona en forma de Applet de Java integrado en una página Web mediante JavaScript. Permite realizar firmas CadES, XAdES, PDF Y ODF. Hace uso de los certificados digitales X.509 y de las claves privadas asociadas a los mismos que estén instalados en el repositorio (keystore) del navegador web o el sistema operativo así como de los que estén en dispositivos (SmartCards, USBKey) configurados en el mismo (el caso de los DNI-e). Se ejecuta en cliente, en el ordenador del usuario, no en el servidor Web. Esto es así para evitar que la

clave privada asociada a un certificado tenga que "salir" del contenedor del usuario (tarjeta, dispositivo USB o navegador) ubicado en su PC.

Contiene las interfaces y componentes web necesarios para la realización de los siguientes procesos (además de otros auxiliares como cálculos de hash, lectura de ficheros, etc…):

- Firma de ficheros binarios.
- Multifirma masiva de ficheros binarios.
- Cofirma (CoSignature) : Multifirma al mismo nivel.
- Contrafirma (CounterSignature) : Multifirma en cascada.

Como complemento al cliente de firma, se encuentra un cliente de cifrado que nos permite realizar las funciones de encriptación y desencriptación de datos atendiendo a diferentes algoritmos y configuraciones. Además permite la generación de sobres digitales.

Los tipos de firma generados en el caso de las firmas CAdES y XAdES son las siguientes:

CADES

Tipo de firma			Explicación	La hace el cliente
Attached		Implícita	La firma contiene el hash de los datos y un campo con los propios datos.	SI
Detached		Explícita	La firma contiene el hash de los datos.	SI

XADES

Tipo de firma			Explicación	La hace el cliente
Attached	enveloping	implicita	la firma contiene los datos. Los datos son el base 64 de un documento, o un xml	SI
		explicita	Igual a la implícita pero se firma el hash.	SI
	enveloped. Solo para datos XML	implicita	los datos (XML) contienen la firma	SI
		explicita	N/A. Los hash no pueden contener ninguna firma	NO
Detached	internally	implicita	Se crea una superestructura XML que contiene tanto la firma, como los datos. La firma contiene una referencia al nodo XML con los datos.	SI
		explicita	Igual que la implícita pero se firma el hash.	SI
	externally	implicita	La firma referencia a los datos mediante una URL cuando están en remoto (HTTP) y no dispone de ninguna referencia a los datos cuando están en local.	NO
		explicita	No tiene sentido referenciar un hash remoto.	NO

5.Port@firmas

Es una **suite integrada de herramientas** para dotar a los usuarios de una organización de la capacidad de realizar **procesos de aprobación sobre documentos** por medio de firma electrónica. De esta manera, Por@firma permite **definir flujos de aprobación de documentos** y los pone a disposición de los destinatarios que los aprobarán, mediante su firma electrónica, o rechazarán. También permite **independizar los procesos de aprobación** de documentos de las lógicas de negocio de la organización, facilitando la integración de la tecnología de firma electrónica y aportando total fiabilidad y seguridad a los procesos organizativos.

El objetivo de este sistema es proporcionar a las Administraciones Públicas un software listo para instalar, que permita integrar fácilmente los servicios de workflow de las diferentes unidades con funcionalidad de firma electrónica. Mediante esta aplicación se pretende que las distintas unidades pueden integrar con sus sistemas de workflow, los flujos de firma de documentos, facilitando de esta manera la reducción de uso del papel y la agilización de los procedimientos.

Al estar integrado con la Plataforma de validación de firma @firma, también 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. Los servicios son aplicables a todos los certificados electrónicos cualificados publicados por cualquier proveedor de servicio de certificación acreditado en España, incluidos los certificados de la tarjeta del DNIe del ciudadano.

Cuando se realizan trámites telemáticos es las administraciones públicas, es necesario la firma de documentos de diferente tipo. Port@firmas permite la firma de documentos, independientemente de su formato, mediante estándares avanzados de firma como XAdES

6.VALIDe

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.

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.

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.

- •Validación de certificados X.509, de todas las Autoridades de Certificación reconocidas en el país por el Ministerio de Industria.
- •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.

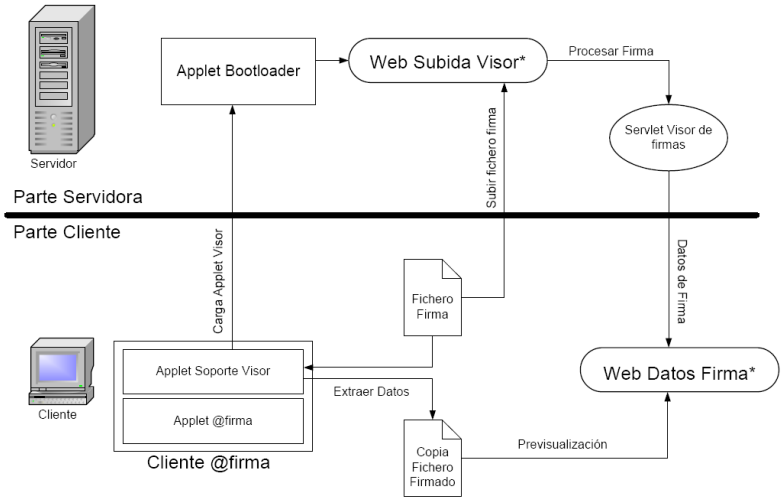
- •Por defecto se realiza firma en formato XADES implícito, con firma envolvente, mediante un algoritmo RSA con SHA1.
- •Para usuarios registrados además permite el uso de diferentes formatos de firma electrónica como PKCS#7, CMS, XML signature, XAdES y CAdES.
- •Para acceder a esta funcionalidad se utiliza el ClientE de @firma.

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.

7.e-VISOR

Como complemento a valide, actualmente está en construcción un visualizador normalizado de documentos firmados generados por una AAPP al que accedería el ciudadano. Se compone de una parte cliente donde el ciudadano cargaría el fichero con el documento electrónico a visualizar, y una parte servidora, basada principalmente en servlets donde se generaría la parte a visualizar con toda la información pertinente y los datos de las firmas, a través de un proceso de generación automático.



El proceso para el visionado de los datos de firma será el siguiente:

1. El usuario accederá a la página "Web Subida Visor".
2. La Web cargará el applet Bootloader, situado en la parte servidora, y este permitirá la carga del applet de soporte del visor (instalado como parte del cliente de firma).
3. El usuario seleccionará el fichero de firma a través del formulario de la página y pulsará elbotón "Aceptar".
4. El applet de soporte del visor analizará la firma y extraerá una copia de los datos
5. almacenándolos en un fichero temporal. Si se conoce el formato de los datos a través del mimetype de la firma, se indicará la extensión correspondiente en el fichero generado.
6. El fichero será enviado al servidor junto la ruta del fichero temporal generado con los datos extraídos de la firma.
7. El servlet visor generará una página Web que contendrá la información de la firma.
    - Si se espera que el formato esté soportado por el navegador, se realizará una previsualización del mismo.
    - Si no se espera que el formato este soportado por el navegador, se mostrará un enlace para su descarga.
8. El navegador Web mostrará al usuario la página generada con la información de firma.

8.Requisitos de uso

✓Autoridad de Validación @firma

Para acceder a los servicios es necesario disponer de accesibilidad a la Plataforma desde los sistemas de información del Organismo en cuestión a través de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que ofrece servicios de intranet entre las Administraciones Públicas. Las solicitudes de servicio realizadas mediante servicios web (Web Services -WS) deben realizarse por los puertos 8080 ó 443. Las peticiones al servicio *ValidarCertificado* mediante OCSP se deben dirigir al puerto 80. Los web services de @firma son totalmente interoperables y compatibles con las tecnologías java y .NET, y siguen los perfiles de OASIS WS Security, WS Interoperability y DSS OASIS para las firmas electrónicas.

✓Autoridad de sellado de tiempo TS@

Para acceder a los servicios es necesario disponer de accesibilidad a la Plataforma desde los sistemas de información del Organismo en cuestión a través de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que ofrece servicios de intranet entre las Administraciones Públicas. Estos sistemas que soportan los servicios de administración electrónica disponibles para los ciudadanos y empresas, accederán a la Plataforma a través de servicios web, peticiones HTTPS o mediante peticiones TCP.

✓CLIENTe @firma

El cliente de firma está disponible para todas las Administraciones públicas que lo soliciten. Los requisitos de funcionamiento son:

- •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
- •Disponer de un certificado digital junto con su 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.

Los navegadores y sistemas operativos soportados son los siguientes:

Windows 64 Bits (XP, Vista, 7, Server 2003, Server 2008)					
MS Internet Explorer	Mozilla Firefox		Google Chrome	Apple Safari	Opera
6 y superiores	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	NO SOPORTADO

Mac OS X x86 (10.5 y superiores)					
MS Internet Explorer	Mozilla Firefox (KeyStore de Mac OS X)		Google Chrome	Apple Safari	Opera
5.5	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
NO SOPORTADO	JSE 1.6.0_07 y superiores	JSE 1.6.0_07 y superiores	JSE 1.6.0_07 y superiores	JSE 1.6.0_07 y superiores	NO SOPORTADO

Linux 2.6 x86 (32 Bits)					
MS Internet Explorer	Mozilla Firefox		Google Chrome	Apple Safari	Opera
	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
	JSE 5u22 y superiores (32 Bits)	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	NO SOPORTADO

Sun Solaris / OpenSolaris (10 y superiores, x86, x64 y SPARC)					
MS Internet Explorer	Mozilla Firefox		Google Chrome	Apple Safari	Opera
5,5	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
NO SOPORTADO	JSE 5u22 y superiores (32 Bits)	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	NO SOPORTADO

✓Port@firmas

Para instalar el portafirmas es necesario instalar el siguiente SW base:

- •Base de datos ORACLE 9i o 10g
- •Servidor de aplicaciones web Apache Tomcat con JRE 1.4.2 recomendable a partir de la versión 1.4.2_07 o JRE 1.5
- •Cuenta de correo necesaria para la notificación de cambios de estados de las peticiones a través de correo electrónico
- •Hacer la integración con la plataforma @firma para hacer uso de sus servicios de validaciónP

Para utilizar los servicios de validación de firmas y certificados o realización de firmas es necesario estar conectado a la Extranet Administrativa SARA.

Los navegadores soportado por Port@firmas:

- •Firefox 1.5 ó superior.
- •Microsoft Internet Explorer 6 ó superior.

✓VALIDe

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)

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).

✓e-VISOR

- Sistemas operativos soportados:
  - Sun Solaris (SPARC, x86)
  - Linux
  - Windows
  - Mac OS X (Intel, 64 bits)
- Entorno de ejecución de Java
  - JRE 1.6u18 32 bits y superiores (Linux, Solaris, Windows), Java for Mac OS X Update 5 [JRE 1.6.0_07] (Mac OS X).
- Navegadores Web
  - Microsoft Internet Explorer 7, 8 (Windows)
  - Mozilla Firefox 3.0 y superiores, incluyendo 3.5 (Solaris, Linux, Windows, Mac OS X)
  - Apple Safari 4 (Windows, Mac OS X)
  - Google Chrome 3 y superiores (Windows)

9.Resultados Obtenidos

Las ventajas que proporciona esta suite de productos y servicios de firma electrónica son las siguientes:

- Acercamiento de la firma electrónica a ciudadanos y administraciones. Mediante este conjunto de servicios se proporcionan herramientas e instrumentos para comprobar la validez de una firma y de un certificado digital, y para la realización de firmas electrónicas en múltiples formatos interoperables, lo que permitirá a los usuarios y AAPP familiarizarse con los servicios de administración electrónica seguros.

- Un punto de interoperabilidad de firmas y certificados electrónicos. De hecho, actualmente la plataforma @firma valida más de 100 tipos de certificados de 13 Prestadores de Servicios de Certificación. Ya se validan además los nuevos mecanismos de firma de las AAPP según la Ley 11/2007: Certificado de sede, sello y empleado público.

- 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.

- Servicios de sellado de tiempo para las AAPP, sincronizados con la hora oficial del Estado.