



# **Manual de Usuario**

## **Comprobación de Requisitos de Firma**

**Edición: V1.0**

**Autor: Servicio de Innovación y Proyectos Informáticos**

**Fecha: Febrero 2011**

### Historia del Documento

<b>Versión: V1.0</b>	<i>Desarrollo nuevo</i>		
	<i>Elaborado por:</i>	<b>José Ramón Alvarez</b>	<i>Fecha: 17/02/2011</i>
	<i>Revisado por:</i>	<b>Diego García Carrera</b>	<i>Fecha: 17/02/2011</i>
	<i>Aprobado por:</i>	<b>Juan A. Barras Garcia</b>	<i>Fecha: 17/02/2011</i>

### Lista de distribución del documento

Nombre	Localización

# Índice

<b>1</b>	<b>INTRODUCCIÓN</b> .....	<b>4</b>
1.1	Conceptos previos.....	4
1.1.1	¿Que es la firma electrónica de documentos? .....	4
1.1.2	¿Que ventajas aporta la firma electrónica en la administración? .....	4
1.1.3	¿Qué necesito para poder firmar documentos digitales? .....	4
1.1.4	Que configuración necesita el PC: .....	5
<b>2</b>	<b>Objetivos del Servicio</b> .....	<b>6</b>
<b>3</b>	<b>Tecnología usada</b> .....	<b>7</b>
3.1	Cliente @Firma 5 .....	7
<b>4</b>	<b>Descripción de su funcionalidad</b> .....	<b>7</b>
4.1	Tabla de Requisitos.....	7
4.2	Acciones propuestas .....	8
4.3	Test de firma electrónica .....	9
<b>5</b>	<b>ANEXO 1 – INTEGRACION APPLET FIRMA 5 EN JCYL</b> .....	<b>10</b>
5.1	Cliente @Firma 5 v3.1.0.....	11
5.1.1	Lugar único de distribución.....	11
5.2	Más información sobre Firma Cliente.....	11
<b>6</b>	<b>ANEXO 2 – PROBLEMAS Y ERRORES DETECTADOS</b> .....	<b>12</b>
6.1	No aparece el DNle en el almacén de certificados de firefox.....	12

# 1 INTRODUCCIÓN

El presente documento describe la funcionalidad de la aplicación “RequisitosAE”, las funciones realizadas para controlar el applet de firma y la comprobación de los requisitos necesarios.

## 1.1 Conceptos previos

### 1.1.1 ¿Que es la firma electrónica de documentos?

- Añadir información a un documento que le proporcione validez legal y asegure a la misma integridad (no es posible manipularlo) y no repudio (se puede demostrar quien lo firmó).

### 1.1.2 ¿Que ventajas aporta la firma electrónica en la administración?

- Asegurar la autoría e integridad de un documento electrónico.
- Plenas garantías legales y con mayores controles y fiabilidad que la firma manuscrita.
- Requisito básico para usar servicios temáticos con la administración: solicitudes, ayudas, subvenciones, consulta de información privada etc.
- Utiliza las nuevas tecnologías para realizar actos administrativos de forma telemática con plenas garantías jurídicas.
- Posibilidad de efectuar trámites
  - 3 A cualquier hora y día del año: Servicio 24x7.
  - 3 Sin necesidad de desplazamientos.
  - 3 Con plenas garantías legales.
  - 3 Con mayor capacidad de seguimiento del ciudadano sobre sus propios trámites y estado de los mismos.

### 1.1.3 ¿Qué necesito para poder firmar documentos digitales?

- PC configurado con un software adecuado.
- Certificado Digital o DNI Electrónico:
  - 3 Un **Certificado Digital** es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.
  - 3 **DNI-Electrónico**: Es el clásico documento nacional de identidad (DNI) al que se han añadido un chip que contiene dos certificados digitales:
    - Certificado para Identificarse.
    - Certificado para Firmar.

#### **1.1.4 Que configuración necesita el PC:**

Se ha desarrollado un componente dentro de la AE que mantiene actualizada estos requisitos denominada Comprobación de requisitos de firma:

En resumen se necesita:

- Windows, Linux
- Navegador Web compatible (IE, Firefox, Chrome, Safari)
- Plug-in Java JRE
- Software de Firma : Applet instalado
- Certificado Digital

## 2 Objetivos del Servicio

Los objetivos de este servicio son:

- Informar de los requisitos mínimos que requiere el sistema cliente para el buen funcionamiento del applet de firma @firma 5
- Comprobar automáticamente que el equipo cliente dispone de esos requisitos mínimos
- Comprobar automáticamente la instalación del applet de firma @firma 5
- Instalar o actualizar automáticamente el applet de firma @firma 5
- Centralizar la distribución del applet de firma @firma 5
- Comprobar su buen funcionamiento en el equipo destino ofreciendo una simulación de firma

**Comprobación de Requisitos de Firma**



**Para poder utilizar los servicios del cliente firma @firma5, se requiere:**

- Disponer de un certificado digital válido o DNI Electrónico. Este certificado pudiera estar instalado en el navegador web o alojado en tarjeta criptográfica. Pulse [aquí](#) para ver la lista de certificados permitidos.
- En caso de usar tarjeta criptográfica o DNIE debe tener instalados correctamente los controladores de acceso tanto del lector como de la tarjeta y/o DNIE.
- Tener instalado en el PC el software de firma cliente. Applet.
- Cumplir los requisitos previos exigidos en el PC para poder ejecutar el cliente de firma.

**Mediante este servicio podrá consultar la configuración que necesita su equipo. También le informará de los pasos a seguir para subsanar las posibles carencias detectadas.**




COMPONENTE	VALORES SOPORTADOS	VALOR DETECTADO	RESULTADO
Sistema Operativo	Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Linux(Ubuntu)	Windows XP	✓
Navegador	Explorer 6 o superior, Firefox 2.0.0.20 o superior, Chrome 3.0 o superior, Safari 4.0 o superior	Explorer 7	✓
Plug-in Java	Se requiere Plug-in Java JRE de Sun 1.6.0_10 o superior Pulse en el siguiente enlace para instalar la última versión <a href="#">Plug-in Java</a>	1.6.0_24	✓
Lector de Documentos PDF	Para poder acceder a los formularios en formato PDF debe tener instalado en su equipo el programa Adobe Reader. Se requiere utilizar la versión 8.0 o superior. Puede descargar la última versión desde <a href="http://www.adobe.es">http://www.adobe.es</a>	8.0.0	✓
Cliente de Firma	Versión: 3.1.0	3.1.0 COMPLETA	✓

**Test Firma Electrónica**

[Simular Firma](#)

Figura 1 : Página del Servicio

## 3 Tecnología usada

### 3.1 Cliente @Firma 5

El Cliente de Firma es una herramienta de Firma Electrónica basada en applets Java integrados en páginas web mediante Javascript, que permiten una fácil implantación en aplicaciones Web ya existentes o que se vayan a desarrollar.

El Cliente hace uso de los certificados digitales X.509 y de sus claves privadas asociadas a los mismos que estén instalados en el repositorio (keystore) del navegador web así como de los que estén en dispositivos (SmartCards, USBKey) configurados en el mismo (el caso de los DNI-e)

## 4 Descripción de su funcionalidad

Este servicio se encarga de realizar todas las comprobaciones necesarias en el cliente para su correcto funcionamiento posterior en procesos de firma. Estas comprobaciones constan de una serie de requisitos, unos obligatorios y otros recomendados, que el cliente debe cumplir en su sistema.

Si la fase de comprobación de requisitos no se ha realizado satisfactoriamente se mostrará al usuario un apartado de **acciones propuestas**, el cual mostrará información para solucionar el problema.

▼ Comprobación de Requisitos de Firma



**Para poder utilizar los servicios del cliente firma @firma5, se requiere:**

- » Disponer de un certificado digital válido o DNI Electrónico. Este certificado pudiera estar instalado en el navegador web o alojado en tarjeta criptográfica. Pulse [aquí](#) para ver la lista de certificados permitidos.
- » En caso de usar tarjeta criptográfica o DNIe debe tener instalados correctamente los controladores de acceso tanto del lector como de la tarjeta y/o DNIe.
- » Tener instalado en el PC el software de firma cliente. Applet.
- » Cumplir los requisitos previos exigidos en el PC para poder ejecutar el cliente de firma.

**Mediante este servicio podrá consultar la configuración que necesita su equipo. También le informará de los pasos a seguir para subsanar las posibles carencias detectadas.**

COMPONENTE	VALORES SOPORTADOS	VALOR DETECTADO	RESULTADO
Sistema Operativo	Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Linux(Ubuntu)	Windows XP	✓
Navegador	Explorer 6 o superior, Firefox 2.0.0.20 o superior, Chrome 3.0 o superior, Safari 4.0 o superior	Safari 3.0.0	✗
Plug-in Java	Se requiere Plug-in Java JRE de Sun 1.6.0_10 o superior Pulse en el siguiente enlace para instalar la última versión <a href="#">Plug-in Java</a>	1.6.0_24	✓
Lector de Documentos PDF	Para poder acceder a los formularios en formato PDF debe tener instalado en su equipo el programa Adobe Reader. Se requiere utilizar la versión 8.0 o superior. Puede descargar la última versión desde <a href="http://www.adobe.es">http://www.adobe.es</a>	8.0.0	✓
Cliente de Firma	Versión: 3.1.0	3.1.0 COMPLETA	✓

**! Acciones Propuestas**

Navegador no soportado. Utilice uno de los navegadores compatibles

Figura 2 : Sección de Acciones Propuestas

Si la comprobación de requisitos se ha realizado satisfactoriamente se mostrará al usuario un apartado para que realice una simulación de firma electrónica.

### 4.1 Tabla de Requisitos

Son 6 los requisitos comprobados:

Requisito	Importancia	Descripción
Sistema Operativo	Obligatorio	
Navegador	Obligatorio	
Plugin Java	Obligatorio	Comprueba que el plug-in java instalado es el correcto. Es necesario tener activados los controles activos. Estos controles pueden ser activados de dos maneras en el explorador: <ol style="list-style-type: none"> <li>Herramientas/opciones Internet/seguridad/nivel predeterminado/medio ó bajo</li> <li>Herramientas/opciones Internet/seguridad/nivel personalizado y activar los complementos ActiveX.</li> </ol>
Plugin Adobe reader	Recomendado	Lector de documentos PDF
Ciente de firma	Obligatorio	Comprueba si existe una la instalación del applet de firma y nos muestra la versión del mismo.

COMPONENTE	VALORES SOPORTADOS	VALOR DETECTADO	RESULTADO
Sistema Operativo	Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Linux(Ubuntu)	Windows XP	✓
Navegador	Explorer 6 o superior, Firefox 2.0.0.20 o superior, Chrome 3.0 o superior, Safari 4.0 o superior	Explorer 7	✓
Plug-in Java	Se requiere Plug-in Java JRE de Sun 1.6.0_10 o superior. Pulse en el siguiente enlace para instalar la última versión <a href="#">Plug-in Java</a>	1.6.0_24	✓
Lector de Documentos PDF	Para poder acceder a los formularios en formato PDF debe tener instalado en su equipo el programa Adobe Reader. Se requiere utilizar la versión 8.0 o superior. Puede descargar la última versión desde <a href="http://www.adobe.es">http://www.adobe.es</a>	8.0.0	✓
Ciente de Firma	Versión: 3.1.0	3.1.0 COMPLETA	✓

**Figura 3 : Comprobación automática de los requisitos**

Las especificaciones de todos los requisitos (valores soportados, versiones...) se puede parametrizar en un fichero de propiedades

## 4.2 Acciones propuestas

Como se ha dicho anteriormente se mostrará al usuario un aparatado de acciones propuestas en el caso de que su sistema no cumpla con alguno de los requisitos especificados.

Las especificaciones de todos las acciones propuestas se realizan en el fichero de propiedades.

Las posibles acciones propuestas son las siguientes:

**!** Acciones Propuestas

Sistema operativo no soportado. Debe utilizar un Sistema Operativo soportado

**!** Acciones Propuestas

Navegador no soportado. Utilice uno de los navegadores compatibles

**!** Acciones Propuestas

Debe actualizar su plugin java. Instale la última versión desde el siguiente enlace [Plug-in Java](#)

En el enlace especificado se puede descargar la última versión del plugin de java.

**!** Acciones Propuestas

Se recomienda actualizar su plugin de Acrobat Reader. Puede descargar la última versión desde <http://www.adobe.es>

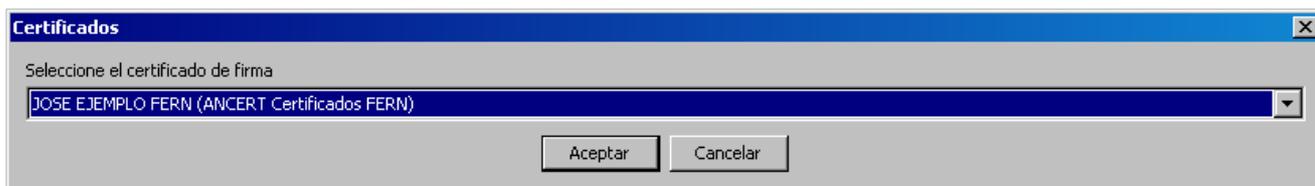
En el enlace especificado se puede descargar la última versión del plugin de Acrobat Reader.

### 4.3 Test de firma electrónica

Si la comprobación del sistema operativo, navegador, plugin-java, y componente firma sean correctos, se podrá realizar una simulación de firma para comprobar su funcionamiento.



Para realizar la simulación se debe de tener un certificado ó DNle. El componente le ofrecerá la lista de certificados disponibles.



Si todo ha sido correcto nos indicara lo siguiente:

✓ La simulación de firma se ha realizado correctamente.  
Su navegador puede operar con la administración electrónica.

---

**DATOS DEL CERTIFICADO**

- Emitido por : Agencia Notarial de Certificación S.L. Unipersonal - CIF B83395988
- Firmante : EJEMPLO FERN, JOSE
- NIF :11111111H
- Fecha Caducidad : 03 de febrero del 2013

## 5 ANEXO 1 – INTEGRACION APPLLET FIRMA 5 EN JCYL

La plataforma de Administración Electrónica de la Junta de Castilla y León está sufriendo una remodelación completa para basarla en la nueva versión de @firma 5.

En esa nueva remodelación se han tomado una serie de decisiones determinantes que condicionan todo el sistema y que afectan a la forma de uso del **applet de Firma**, entre las que se destacan:

- Pasar de usar PKCS#7 como algoritmo de firmado por **formato XADES**.
- No usar la custodia incluida en @firma 5 pasando a almacenar los documentos firmados en un **DOE** (un servicio mas de toda la Plataforma de Administración Electrónica JCYL) con sus propios requisitos relacionados al formato de documento a almacenar.
- Considerar como documento firmado un formato XADES al que se le han añadido información XML denominada METADATOS. El formato básico de ese documento firmado sería:

```
<?xml version="1.0" encoding="UTF-8"?>
<AFIRMA>
<CONTENT >[Información firmada. Generalmente HASH o Resumen del documento] </CONTENT>
<ds:Signature> [Token de Firma XADES]</ ds:Signature>
<METADATOS>[Tags metadatos formato XML. Ver Proyecto DOE]</METADATOS>
```

<DOCUMENTO>[Contenido del documento original den Base64] </DOCUMENTO>  
</AFIRMA>

El **Cliente de Firma electrónica de @firma 5** es uno de los elementos clave de esta plataforma. Es el encargado de generar estas firmas usando la clave privada de un certificado de usuario.

## 5.1 Cliente @Firma 5 v3.1.0

El Cliente de Firma es una herramienta de Firma Electrónica basada en applets java integrados en páginas web mediante Javascript, que permiten una fácil implantación en aplicaciones Web ya existentes o que se vayan a desarrollar.

El Cliente hace uso de los certificados digitales X.509 y de sus claves privadas asociadas a los mismos que estén instalados en el repositorio (keystore) del navegador web así como de los que estén en dispositivos (SmartCards, USBKey) configurados en el mismo (el caso de los DNI-e)

### 5.1.1 Lugar único de distribución

Se ha optado por ubicar en **un lugar único una distribución** del cliente de firma que han de usar todas las aplicaciones:

**<https://<Servidor>/RequisitosAE/binarios/3>**

Ese lugar único de distribución se le ha añadido una serie de opciones de comprobación de requisitos mínimos y botones para que el propio usuario pudiera instalarse el applet a voluntad del ciudadano.

## 5.2 Más información sobre Firma Cliente

Puede consultar mas información accediendo al **Centro de Transferencia de Tecnología (CTT)** mediante internet a la web: <http://www.ctt.map.es>

Proyecto Cliente @firma : <http://www.ctt.map.es/web/clienteafirma>

Preguntas frecuentes:

<http://www.ctt.map.es/web/cache/offonce/proyectos/clienteafirma/pid/992;jsessionid=3792E0DD5D556993A43248578D7D0AC9>

## 6 ANEXO 2 – PROBLEMAS Y ERRORES DETECTADOS

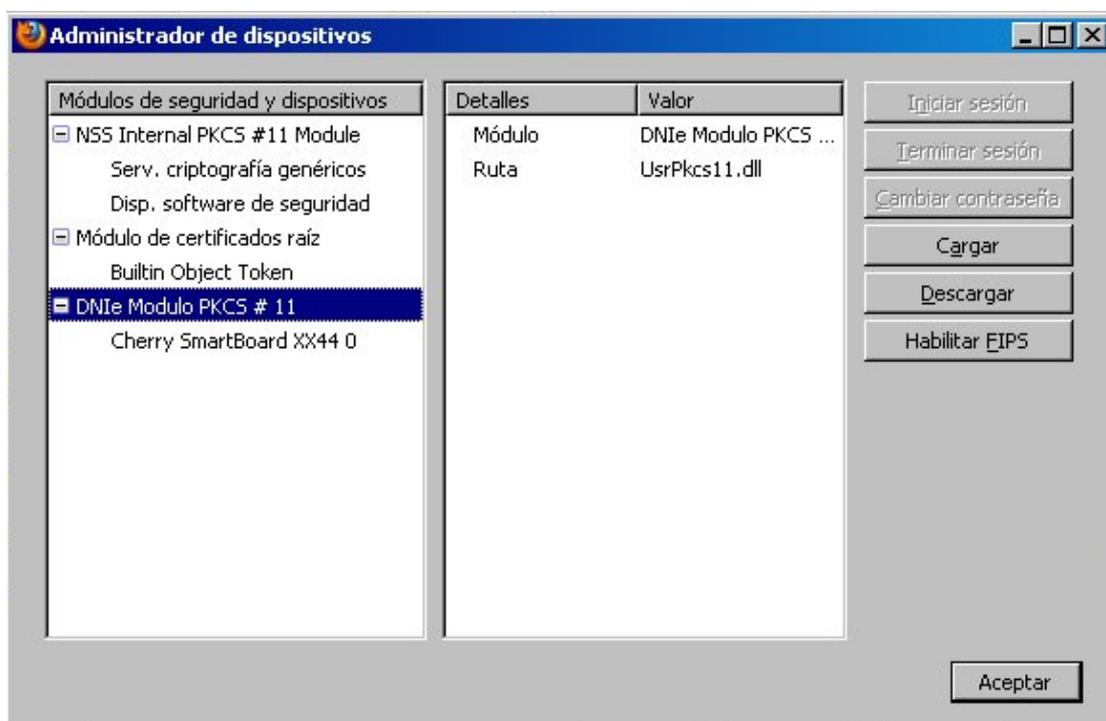
### 6.1 No aparece el DNle en el almacén de certificados de firefox

En ocasiones, principalmente en usuarios que no tienen permisos de administrador en sus equipos, firefox no carga el DNI electrónico.

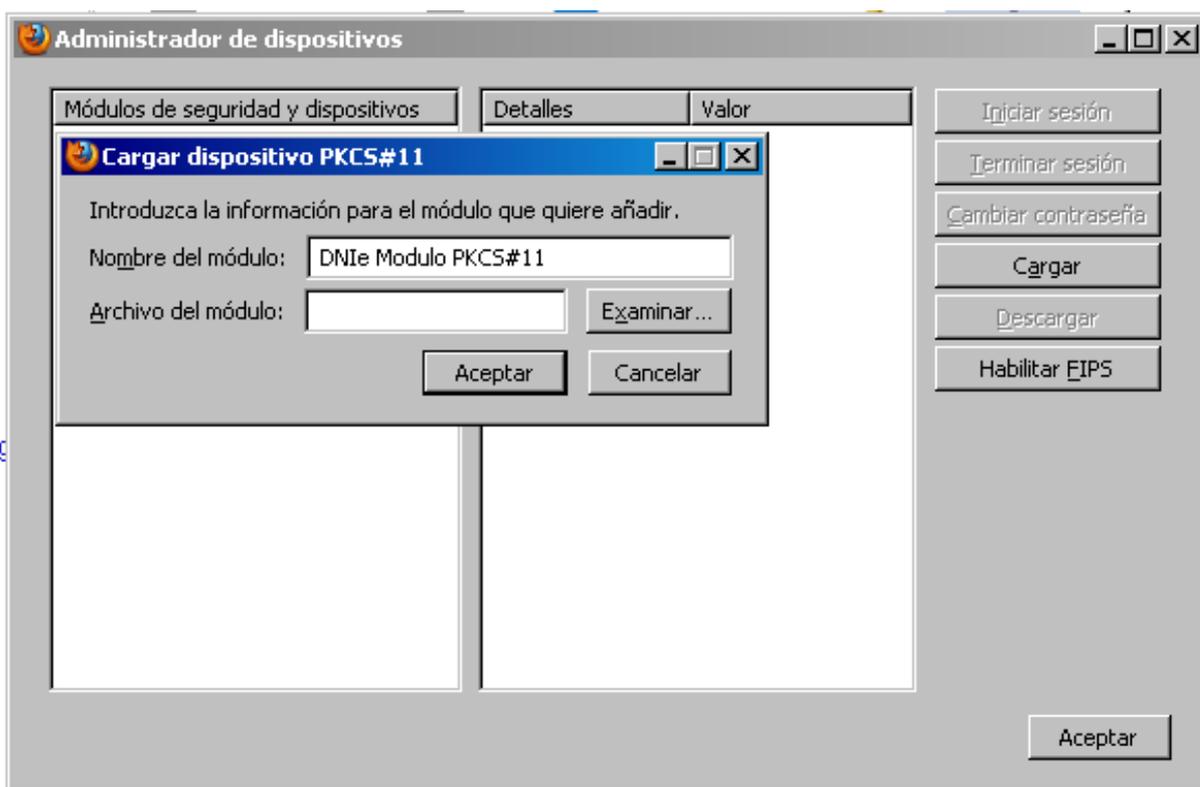
#### Solución:

Si los drivers del DNI electrónicos (módulo criptográfico) han sido instalados correctamente en el equipo, podemos comprobar que firefox lo registra en la siguiente pantalla:

Herramientas -> Opciones -> Avanzado -> Cifrado -> Dispositivos de Seguridad



En el caso de que no aparezca, deberemos cargarlos mediante la opción “Cargar” del panel derecho.



En “nombre de módulo” introducimos: “DNIe Modulo PKCS#11” y como “Archivo del módulo” pulsando en el botón “Examinar” buscamos en nuestro sistema de archivos el fichero “UsrPkcs11.dll” que se encuentra en la carpeta “C:\WINDOWS\system32”.