



Plataforma @firma

Componente validador - Manual de integración

Versión: v01r10

Fecha: 05/02/2018

Componente validador - Manual de integración

Queda prohibido cualquier tipo de explotación y, en particular, la reproducción, distribución, comunicación pública y/o transformación, total o parcial, por cualquier medio, de este documento sin el previo consentimiento expreso y por escrito de la Junta de Andalucía.

HOJA DE CONTROL

Título	Componente validador - Manual de integración		
Entregable	Documentación técnica Plataforma @firma		
Nombre del Fichero	20180205-Manual Integrador_v01r10		
Autor	DGPD		
Versión/Edición	v01r10	Fecha Versión	05/02/2018
Aprobado por		Fecha Aprobación	DD/MM/AAAA
		Nº Total Páginas	13

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Creación del documento	UTE	UTE	06/11/2013
v01r01	Modificada navegación	UTE	UTE	18/12/2013
v01r02	Actualización	UTE	UTE	23/01/2014
v01r03	Actualización	UTE	UTE	24/01/2014
v01r04	Actualización	UTE	UTE	20/02/2014
v01r05	Actualización	UTE	UTE	23/04/2014
v01r06	Actualización	UTE	UTE	30/09/2014
v01r07	Actualización	UTE	UTE	13/04/2015
v01r08	Actualización	UTE	UTE	13/08/2015
v01r09	Versión 2.0.7	UTE	UTE	29/03/2016
v01r10	Versión 2.0.10	UTE	UTE	05/02/2018

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias
Manuel Perera Domínguez	Jefe de Servicio	CHAP	1
José Ignacio Cortés Santos	Director de Proyecto	CHAP	1
Antonio Heredia Rizo	Jefe de Proyecto	UTE	1
Alejandro Román Márquez	Analista	UTE	1

ÍNDICE



**Consejería de Hacienda y Administración
Pública**

Dirección General de Política Digital

Plataforma @firma

**Componente validador - Manual
de integración**

1	Introducción.....	4
2	Novedades de la versión.....	5
3	Acceso al componente validador.....	6
4	Aplicación Web.....	8
5	Obtención de datos.....	12

1 Introducción

El componente validador (en adelante, afirma-validator) es un componente software cuya finalidad es la de informar al usuario del grado de compatibilidad de su equipo informático con el Cliente de Firma Electrónica de la Junta de Andalucía distribuido por la Consejería de Hacienda y Administración Pública.

Fundamentalmente, el componente realiza dos operaciones principales:

1. Obtiene cierta información del equipo del usuario a través de consultas estándares sobre variables definidas en su navegador web.
2. Contrasta la información obtenida en el primer punto con la matriz de compatibilidad del cliente para detectar posibles incompatibilidades y ofrecer soluciones a las mismas.
3. Realiza una prueba de firma preconfigurada similar a la que se realizaría desde la aplicación.
4. A partir de la prueba de firma determina la compatibilidad del equipo.

Se presenta mediante una página web que debe ser enlazada por las aplicaciones que hagan uso del Cliente de Firma Electrónica. Este manual describe los pasos a seguir para que las aplicaciones web interactúen con el componente validador y puedan obtener la información que éste facilita.

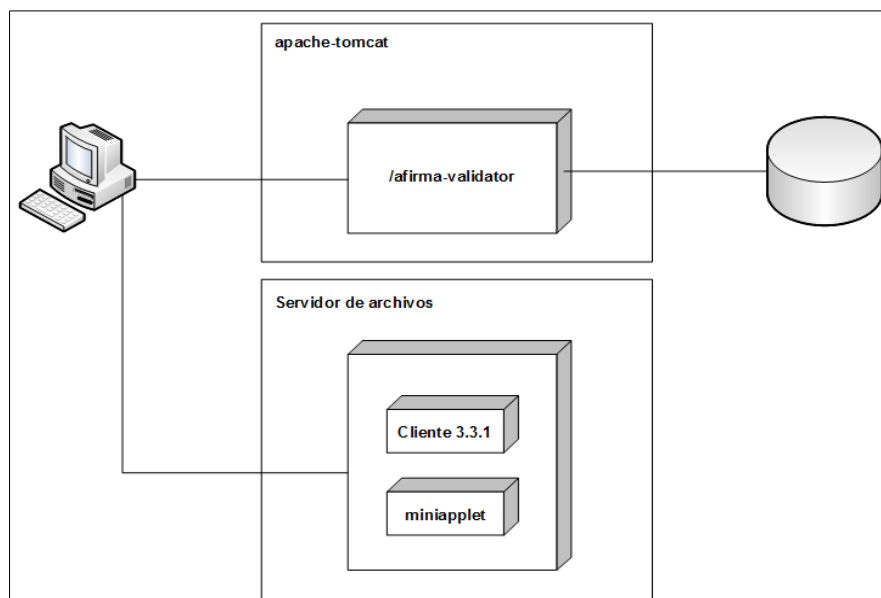


Ilustración 1: Arquitectura del componente validador

Actualmente existen **dos entornos disponibles del componente validador** independientes:

- Entorno de **Pruebas**:
 - <https://ws024.juntadeandalucia.es/afirma-validatorpru/>
- Entorno de **Explotación**:
 - <https://ws024.juntadeandalucia.es/afirma-validator/>



2 Novedades de la versión

Esta versión incluye las siguientes novedades funcionales:

1. Se ha incluido un nuevo parámetro opcional en la URL de la petición HTTPS: "**multiModeSign**". El parámetro indica si la firma a realizar es simple o multifirma. Los posibles valores son: S (si) o N (no). Toma el valor N por defecto.
2. Se ha modificado el fichero que se firma en el proceso de prueba, siendo ahora un fichero PDF en el caso de firma simple y dos ficheros pdf en el caso de multifirma.

3 Acceso al componente validador

El acceso al componente validador se realiza mediante una petición HTTPS a la aplicación web **afirma-validador**. Dicha URL debe incluir los siguiente parámetros obligatorios:

- **clientVersion:** Versión del cliente de firma a validar. Actualmente los componentes disponibles son:
 - applet_3.1.0 (Cliente de Firma 3.1.0)
 - applet_3.2.1 (Cliente de Firma 3.2.1)
 - applet_3.3.1_10 (Cliente de Firma 3.3.1u10)
 - applet_3.3.1_11 (Cliente de Firma 3.3.1u11)
 - applet_3.3.1_12 (Cliente de Firma 3.3.1u12)
 - applet_3.3.1_13 (Cliente de Firma 3.3.1u13)
 - applet_3.4 (Cliente de Firma 3.4)
 - miniapplet_1.1_4 (Miniapplet 1.1u4)
 - miniapplet_1.1_5 (Miniapplet 1.1u5)
 - miniapplet_1.2 (Miniapplet 1.2u1)
 - miniapplet_1.4 (Miniapplet 1.4.JAu02)
 - miniapplet_1.5 (MiniApplet 1.5.JAv01)
- **signatureFormat:** Formato de firma que realiza la aplicación cliente (CADES, XADES...). Los posibles valores son:
 - xades
 - cades
 - padés
- **signatureMode** (opcional): Modo de las firmas que realiza la aplicación cliente (IMPLICIT o EXPLICIT), toma el valor IMPLICIT por defecto.
- **signatureAlgorithm** (opcional): Algoritmo de firma que emplea la aplicación cliente, los posibles valores son: sha1, sha256, sha384 o sha512. Toma el valor "sha1" por defecto.
- **callbackUrl:** URL de vuelta de la aplicación cliente.
- **multiModeSign** (opcional): Indica si la firma a realizar es simple o multifirma. Los posibles valores son: S (si) o N (no). Toma el valor N por defecto.

La aplicación web cliente debe incluir en su página inicial la petición HTTPS para permitir al usuario acceder a la aplicación web del componente validador y con ello poder comprobar la configuración de su sistema.

El código HTML de la petición HTTP debe tener una apariencia similar a:

```
<html>  
<body>  
...  
</body>  
</html>
```



```
<a href="http://[HOST_AFIRMA_VALIDATOR]/validator.action?  
clientVersion=[COMPONENTE_FIRMA]&signatureFormat=[FORMATO_FIRMA]&signatureMode=[M  
ODO_FIRMA]&signatureAlgorithm=[ALGORITMO]&callbackUrl="[URL_APP_CLIENTE]&multiMode  
Sign=[FIRMA_MULTIPLE]">Compruebe si su equipo es compatible con la firma  
electronica</a>  
  
...  
</body>  
</html>
```

Se permite el envío de los parámetros mediante GET y POST.

4 Aplicación Web

Se muestra a continuación la pantalla inicial del componente validador:



Automáticamente se inicia la detección de la máquina virtual java instalada en el equipo y la posterior comprobación del resto de componentes del entorno del usuario: sistema operativo y navegador web.

A continuación se muestra la pantalla de resumen de resultados una vez obtenidos y contrastados los datos del entorno del usuario:

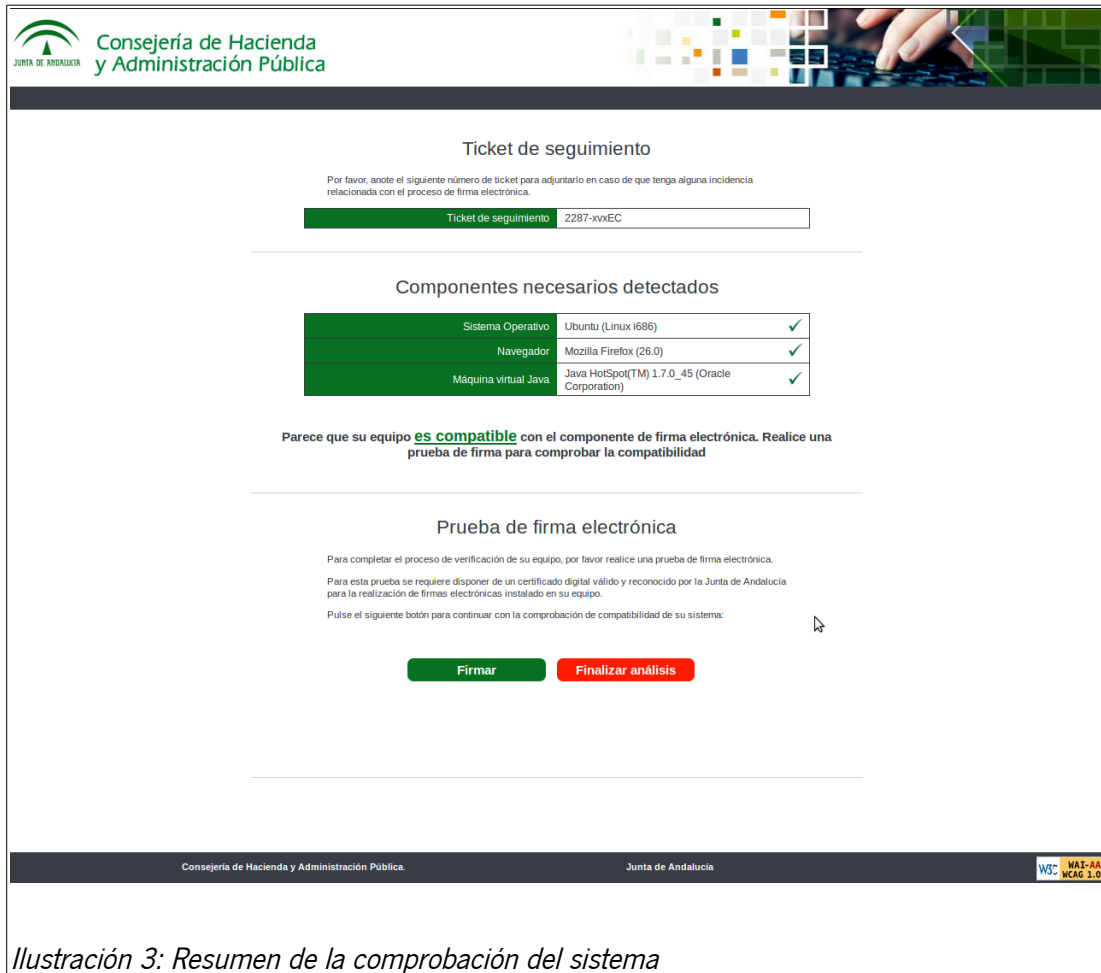





Ilustración 3: Resumen de la comprobación del sistema

En esta pantalla se incluye la siguiente información:

- **Ticket de seguimiento:** Se aporta al usuario un ticket de seguimiento para poder referirse a la comprobación del sistema local ante eventuales incidencias al respecto.
- **Componentes necesarios detectados.** En este apartado se exponen los componentes detectados respecto al Sistema Operativo, Navegador y Máquina Virtual Java. Además, se indica si los componentes son compatibles con el cliente de firma solicitado en los siguientes términos:

Símbolo	Resultado
	El componente es válido y compatible con la versión del cliente y la firma requerida.
	No se ha podido determinar si el componente es compatible con la versión del cliente y la firma requerida.
	El componente no es compatible con la versión del cliente y la firma requerida.

Prueba de firma electrónica

Para completar el proceso de verificación de su equipo, por favor realice una prueba de firma electrónica.

Para esta prueba se requiere disponer de un certificado digital válido y reconocido por la Junta de Andalucía para la realización de firmas electrónicas instalado en su equipo.

Pulse el siguiente botón para continuar con la comprobación de compatibilidad de su sistema:

Firmar

Finalizar análisis

El resultado de la firma es correcto

Ilustración 4: Resultado de prueba de firma

- **Posibles soluciones a los problemas.** Si la aplicación ha detectado que no tiene todos los componentes necesarios dados los datos del entorno del usuario, se muestra el recuadro “Solución de Problemas”, que incluye información de versiones de componentes (Sistemas Operativos, Navegadores o Máquinas Virtuales Java) que sí son compatibles con el cliente de firma y el tipo de firma requerido. A continuación se muestra a modo de ejemplo una captura de este apartado:

Su equipo **no es compatible** con el componente de firma electrónica. No se detectó Java en su equipo.

Solución de problemas

Navegador Mozilla Firefox (26.0)

Para poder utilizar la firma electrónica debe utilizar alguno de los navegadores soportados para su sistema operativo:

- google chrome (19 - 29)
- mozilla firefox (13.0 - 22.0)
- opera (12.02 - 12.12)

Máquina virtual Java No detectado

Se requiere el uso de Java para habilitar la firma electrónica en su equipo. Deberá instalar alguna de estas versiones:

- java hotspot(tm) 1.6.0_33 - 1.6.0_45 (sun microsystems inc.) [descargar](#)
- java hotspot(tm) 1.7.0_07 - 1.7.0_25 (oracle corporation) [descargar](#)
- openjdk 1.6.0_20 - 1.6.0_24 (sun microsystems inc.) [descargar](#)

Ilustración 5: Solución de problemas

- **Prueba de firma electrónica.** Una vez detectado el entorno del usuario se requiere la realización de una “Prueba de firma electrónica” con el cliente de firma y el tipo de firma indicados en los parámetros de la URL. Indicándose finalmente si el proceso de firma se ha realizado correctamente, lo cual indicaría que el sistema del usuario está preparado para realizar firmas.

Prueba de firma electrónica

Para completar el proceso de verificación de su equipo, por favor realice una prueba de firma electrónica.

Para esta prueba se requiere disponer de un certificado digital válido y reconocido por la Junta de Andalucía para la realización de firmas electrónicas instalado en su equipo.

Pulse el siguiente botón para continuar con la comprobación de compatibilidad de su sistema:

Firmar

Finalizar análisis

El resultado de la firma es correcto

Su equipo **es compatible** con el componente de firma electrónica. Finalice el análisis para volver a la aplicación.

Ilustración 6: Resultado de prueba de firma

5 Obtención de datos

Finalizado el análisis del entorno mediante la aplicación `afirma-validator`, el usuario puede retornar a la aplicación web cliente mediante el botón **“Finalizar análisis”**, ubicado en el recuadro de “Prueba de firma electrónica”.

Si el usuario opta por finalizar el análisis, el Componente Validador realizará la siguiente petición HTTP:

```
[callbackURL]?r=[resumenDatosXMLBase64URLEncoded]
```

Los datos contenidos en el parámetro “r” corresponden a un fichero XML codificado en Base64. Opcionalmente, la aplicación cliente puede procesar los datos incluidos en el parámetro devuelto, decodificando el contenido y obtener el resumen del resultado de la validación. Se muestra un ejemplo de los datos decodificados y la descripción de cada uno de los datos:

```
<?xml version="1.0" encoding="UTF-8"?>
<afirmaValidator>
  <reportVersion>1.1</reportVersion> <!-- Versión del informe -->
  <ticket>10933-JDBND</ticket> <!-- Ticket de seguimiento -->
  <reportTime>2015-04-15 17:24:19.165</reportTime> <!-- Fecha del test -->
  <osName>Windows</osName> <!-- Nombre Sistema Operativo -->
  <osVersion>7</osVersion> <!-- Versión Sistema Operativo -->
  <osArch>Win32</osArch> <!-- Arquitectura Sistema Operativo -->
  <browserName>Google Chrome</browserName> <!-- Nombre Navegador -->
  <browserVersion>30.0.1599.69</browserVersion> <!-- Versión Navegador -->
  <jreName>Java HotSpot(TM)</jreName> <!-- Nombre JRE -->
  <jreVersion>1.7.0_40</jreVersion> <!-- Versión JRE -->
  <jreVendor>Oracle Corporation</jreVendor> <!-- Proveedor JRE -->
  <clientVersion>miniapplet_1.1_3</clientVersion> <!-- Versión Applet -->
  <signatureFormat>xades</signatureFormat> <!-- Formato de firma -->
  <signatureMode>implicit</signatureMode> <!-- Modo de firma -->
  <signatureAlgorithm>SHA256withRSA</signatureAlgorithm> <!-- Algoritmo de
  firma -->
  <osResult>ND</osResult> <!-- Resultado comprobación Sistema Operativo -->
  <browserResult>ND</browserResult> <!-- Result. comprobación Navegador -->
  <jreResult>SC</jreResult> <!-- Resultado comprobación JRE -->
  <signTestResult>OK</signTestResult> <!-- Resultado test de firma -->
  <signTestValidationResult>OK</signTestValidationResult> <!-- Resultado
  validación de firma -->
  <callbackUrl>
    https://ws031.juntadeandalucia.es/notificaciones/snja/inicio.jsp
  </callbackUrl> <!-- URL de retorno -->
  <multiModeSign>N</multiModeSign> <!-- Firma múltiple -->
</afirmaValidator>
```

Los **elementos del fichero XML que informan del resultado** de la validación del entorno pueden tomar los siguientes valores:

- **osResult**, **browserResult**, **jreResult**: **"ND"** (No Definido en la matriz), **"SC"** (Compatible), **"NC"** (No Compatible).
- **signTestResult**: **"NR"** (Test No Realizado), **"OK"** (Válido), **"ERROR"** (Error).

A modo de ejemplo, se muestra un fragmento de código a ejecutar en la ruta de retorno para recuperar y decodificar el resultado de la validación:



```
String param = (String)request.getParameter("r");  
if(param != null){  
    String xml = new String(Base64.decode(param));  
    System.out.println(xml);  
}
```