



Plataforma @firma

Matriz de compatibilidad de applet 3.4

Versión:v01r00

Fecha: 25/05/2015

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.

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda y Administración Pública</p> <p>Dirección General de Política Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad de applet 3.4</p>
---	---	--

HOJA DE CONTROL

Título	Matriz de compatibilidad de applet 3.4		
Entregable	Matriz de compatibilidad del cliente de firma		
Nombre del Fichero	20150525-CF_Matriz-compatibilidad_3_4_v01r00		
Autor	DGPD		
Versión/Edición	v01r00	Fecha Versión	25/05/2015
Aprobado por		Fecha Aprobación	
		Nº Total Páginas	12

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Primera versión del documento	SCAE	DGPD	08/07/2014

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias
Manuel Perera Dominguez	Jefe de Servicio	CHAP	1
José Ignacio Cortés Santos	Director de Proyecto	CHAP	1

ÍNDICE

1. Objeto de este documento.....	4
2. Descripción de las pruebas realizadas.....	5
3. Descripción de los entornos de prueba.....	6
4. Matriz de compatibilidad.....	7
5. Resumen de Problemas, errores y dependencias detectadas.....	10
5.1 Habilitar soporte de Java en Google Chrome 42 y superior.....	10
5.2 Java 8 Update 25.....	10
5.3 Java 7 Update 45.....	10
5.4 Windows.....	11
5.5 Guadalinux.....	11
5.6 Ubuntu.....	11
5.7 Mac OS X.....	12

 <p>JUNTA DE ANDALUCIA</p>	<p>Consejería de Hacienda y Administración Pública</p> <p>Dirección General de Política Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad de applet 3.4</p>
---	---	--

1. Objeto de este documento

El presente documento tiene por objeto mostrar la matriz de compatibilidad del cliente de firma 3.4 conforme a las pruebas de aceptación realizadas.

 <p>JUNTA DE ANDALUCIA</p>	<p>Consejería de Hacienda y Administración Pública</p> <p>Dirección General de Política Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad de applet 3.4</p>
---	---	--

2. Descripción de las pruebas realizadas

El protocolo de pruebas del cliente de firma se ha basado en la simulación de procesos de firma en diferentes formatos mediante el uso de de la herramienta “afirma-validator”. Los formatos probados han sido los siguientes: CAdES-BES (implícito), XAdES-BES (internally detached) y PAdES-BES.

Todas las firmas constan de una firma de una cadena de texto aleatoria en formato implícito con un solo firmante. Posteriormente, en una segunda fase se han realizado firmas más complejas con varios firmantes (firmas y contrafirmas) utilizando la misma herramienta.

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda y Administración Pública</p> <p>Dirección General de Política Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad de applet 3.4</p>
---	---	--

3. Descripción de los entornos de prueba

Para la realización de las pruebas se han creado máquinas virtuales usando el software Oracle VirtualBox.

Los entornos considerados para verificar la compatibilidad de la firma de escritorio son los siguientes:

1. **Windows XP.** Se ha utilizado la arquitectura de 32 bits. Como navegadores se considerarán Internet Explorer 8, Google Chrome y Mozilla Firefox en sus últimas versiones. Máquina virtual Java 6 y 7 en sus últimas versiones.
2. **Windows 7.** Se ha utilizado la arquitectura de 32 bits. Como navegadores se considerarán Internet Explorer 8, 9 y 10, Google Chrome y Mozilla Firefox en sus últimas versiones. Máquina virtual Java 6 y 7 en sus últimas versiones.
3. **Windows 8.1.** Se ha utilizado la arquitectura de 64 bits, con la interfaz de “escritorio clásico”. Como navegadores se considerarán Internet Explorer 11, Google Chrome y Mozilla Firefox en sus últimas versiones. Máquina virtual Java 6 y 7 en sus últimas versiones.
4. **Guadalinex 8.** Como navegadores se considerarán Google Chrome y Mozilla Firefox en sus últimas versiones disponibles desde el repositorio. Máquina virtual Java 6 y 7 en sus últimas versiones disponibles desde el repositorio.
5. **Ubuntu.** Se han considerado las versiones LTS 12.04 y 14.04 en arquitectura de 64 bits. Como navegadores se considerarán Google Chrome, Chromium y Mozilla Firefox en sus últimas versiones disponibles desde el repositorio. Máquina virtual Java 6 y 7 en sus últimas versiones disponibles desde el repositorio.
6. **Mac OS X.** Se considerará la última versión disponible. Como navegadores se considerarán Safari, Google Chrome y Mozilla Firefox en sus últimas versiones disponibles. Máquina virtual Java 7 en su última versión.

Para el certificado se ha utilizado el almacén del navegador o, en su defecto, el almacén del propio sistema operativo. En algún caso concreto el cliente de firma no ha podido instanciar ningún almacén de claves, por lo que en estos casos se ha utilizado un almacén de claves PKCS#11 basado en ficheros para la ejecución de las pruebas.

4. Matriz de compatibilidad

A continuación se muestran las matrices de compatibilidad en función de la máquina virtual Java utilizada.

S.O.	JRE 1.6 (1.6.0_45)						
	Firefox	I. Explorer				Chrome (1)	Safari
	38	8	9	10	11	43	7
Windows XP	OK	OK	N/D	N/D	N/D	OK	NOK
Windows 7	OK	OK	OK	OK	N/D	OK	NOK
Windows 8.1	OK	N/D	N/D	N/D	OK	OK	NOK
Guadalinex 8	OK	N/D	N/D	N/D	N/D	NOK (2)	N/D
Ubuntu 12.04	OK	N/D	N/D	N/D	N/D	NOK (3)	N/D
Ubuntu 14.04	OK	N/D	N/D	N/D	N/D	NOK (3)	N/D
Mac OS X Mavericks (4)	N/D	N/D	N/D	N/D	N/D	N/D	N/D

(1) A partir de la versión 42 del navegador Google Chrome, se ha deshabilitado por defecto la ejecución de applets java. Es necesario activar el soporte de java para poder ejecutar el cliente de firma.

(2) No es posible la descarga del navegador Chrome. Al tratar de instalar el paquete se detecta la versión del sistema operativo antiguo (Ubuntu 11.10) y no permite su instalación.

(3) A partir de la versión 35 del navegador Chrome para Linux ha retirado el soporte al plugin de Java, por lo que no resulta posible la ejecución de applets en esta versión del navegador. Más información en el siguiente enlace: <https://code.google.com/p/chromium/issues/detail?id=375909>

(4) No existe Java 6 oficial para la última versión de Mac OS X.

Leyenda:

OK: Configuración que ha funcionado satisfactoriamente.

NOK: Configuración que no ha funcionado correctamente.

N/D: Configuración no disponible.

S.O.	JRE 1.7 (1.7.0_67)						
	Firefox	I. Explorer				Chrome (1)	Safari
	38	8	9	10	11	43	7
Windows XP	OK	OK	N/D	N/D	N/D	OK	NOK
Windows 7	OK	OK	OK	NOK (2)	N/D	OK	NOK
Windows 8.1	OK	N/D	N/D	N/D	OK	OK	NOK
Guadalinux 8	NOK (3)	N/D	N/D	N/D	N/D	NOK (4)	NOK
Ubuntu 12.04	OK	N/D	N/D	N/D	N/D	NOK (5)	NOK
Ubuntu 14.04	OK	N/D	N/D	N/D	N/D	NOK (5)	NOK
Mac OS X Mavericks	NOK (6)	N/D	N/D	N/D	N/D	NOK (7)	OK

(1) A partir de la versión 42 del navegador Google Chrome, se ha deshabilitado por defecto la ejecución de applets java. Es necesario activar el soporte de java para poder ejecutar el cliente de firma.

(2) Con Internet Explorer 10 sólo se ha conseguido completar firmas en formato CAdES. Las firmas en formato XAdES y PadES generan el error "error al firmar: Result error".

(3) El applet no carga correctamente. Al realizar una operación de firma se produce el error "error al firmar: null".

(4) No es posible la descarga del navegador Chrome. Al tratar de instalar el paquete se detecta la versión del sistema operativo antiguo (Ubuntu 11.10) y no permite su instalación.

(5) La versión 35 del navegador Chrome para Linux ha retirado el soporte al plugin de Java, por lo que no resulta posible la ejecución de applets en esta versión del navegador. Más información en el siguiente enlace: <https://code.google.com/p/chromium/issues/detail?id=375909>

(6) El applet no llega a ejecutarse en el navegador Firefox.

(7) La versión de Chrome para Mac OS X es de 32 bits, siendo por tanto incompatible con las versiones de Java de 64 bits.

Leyenda:

OK: Configuración que ha funcionado satisfactoriamente.

NOK: Configuración que no ha funcionado correctamente.

N/D: Configuración no disponible.

S.O.	JRE 1.8 (1.8.0_45)						
	Firefox	I. Explorer				Chrome (1)	Safari
	38	8	9	10	11	43	7
Windows XP	OK	OK	N/D	N/D	N/D	OK	NOK
Windows 7	OK	OK	OK	OK	N/D	OK	NOK
Windows 8.1	OK	N/D	N/D	N/D	OK	OK	NOK
Guadalinux 8	NOK (5)	N/D	N/D	N/D	N/D	NOK (2)	NOK
Ubuntu 12.04	NOK (5)	N/D	N/D	N/D	N/D	NOK (3)	NOK
Ubuntu 14.04	NOK (5)	N/D	N/D	N/D	N/D	NOK (3)	NOK
Mac OS X Mavericks	NOK (3)	N/D	N/D	N/D	N/D	NOK (4)	OK

(1) A partir de la versión 42 del navegador Google Chrome, se ha deshabilitado por defecto la ejecución de applets java. Es necesario activar el soporte de java para poder ejecutar el cliente de firma.

(2) La versión 35 del navegador Chrome para Linux ha retirado el soporte al plugin de Java, por lo que no resulta posible la ejecución de applets en esta versión del navegador. Más información en el siguiente enlace: <https://code.google.com/p/chromium/issues/detail?id=375909>

(3) El applet no llega a ejecutarse en el navegador Firefox.

(4) La versión de Chrome para Mac OS X es de 32 bits, siendo por tanto incompatible con las versiones de Java de 64 bits.

(5) Se produce el siguiente error aún añadiendo la URL como excepción de seguridad en el panel de control de java: LiveConnect.SecurityException: JavaScript from [URL] attempted to access a resource it has no rights to.

Leyenda:

OK: Configuración que ha funcionado satisfactoriamente.

NOK: Configuración que no ha funcionado correctamente.

N/D: Configuración no disponible.

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda y Administración Pública</p> <p>Dirección General de Política Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad de applet 3.4</p>
---	---	--

5. Resumen de Problemas, errores y dependencias detectadas

5.1 Habilitar soporte de Java en Google Chrome 42 y superior.

A partir de la versión 42 del navegador Google Chrome, se ha deshabilitado por defecto la ejecución de applets java, lo que impide la ejecución de los componentes de firma "cliente de firma" y "miniapplet" en cualquiera de sus versiones.

En los entornos Windows y Mac, es posible volver a activar el soporte de Java en el navegador Chrome de forma temporal hasta septiembre de 2015, siguiendo los siguientes pasos:

1. Abra el navegador web y teclee el siguiente texto en el cuadro de direcciones web: "chrome://flags"
2. Buscar el texto "Habilitar NPAPI" en la página que aparece y pulse en el enlace que aparece justo abajo con el texto "Habilitar".
3. Pulse el botón "Reiniciar ahora" para aplicar el cambio. Esta opción cerrará el navegador.

Para más información consultar <http://www.chromium.org/developers/npapi-deprecation>

NOTA: No es posible activar la ejecución de applets java en entornos basados en linux. En este entorno, la única forma de ejecutar applets de java consiste en usar el navegador Mozilla Firefox. El soporte de java para entornos basados en linux fue retirado a partir de la versión 35: <https://code.google.com/p/chromium/issues/detail?id=375909>

5.2 Java 8 Update 25

A partir de la versión publicada por Oracle de Java 8u25, se ha introducido un nuevo cambio que afecta a la comprobación del nombre de dominio en las web https que ahora es sensible a mayúsculas y minúsculas.

Por este motivo si el certificado de servidor que se utiliza para la securización del sitio web donde se encuentra alojado el cliente de firma o miniapplet no coincide exactamente con la web securizada se produce un error de seguridad y no se ejecuta el applet.

A modo de ejemplo, si una aplicación que tenga el cliente de firma o miniapplet se publica mediante https bajo un servidor del tipo "wsxyz.juntadeandalucia.es" y el certificado que se utiliza para la securización del sitio web es "*.JUNTADEANDALUCIA.ES" se obtendrá un error de seguridad (el certificado tendría que ser del tipo "*.juntadeandalucia.es", en minúsculas).

Este problema se resuelve asegurando que el certificado utilizado concuerda, teniendo en cuenta mayúsculas y minúsculas, con el dominio publicado.

5.3 Java 7 Update 45

El pasado día 15 de octubre, Oracle publicó una actualización de la máquina virtual java, la versión 1.7.0_45 que introduce nuevos requisitos de seguridad de obligado cumplimiento para los applets java. Ciertas versiones anteriores de Java 7 fuerzan a la actualización de la máquina virtual java, motivo por el cual se considera en este documento la compatibilidad del cliente de firma a partir de esta versión (Más información en <https://ws024.juntadeandalucia.es/ae/descargar/4120>). Esta versión del cliente incluye los atributos necesarios para que el usuario pueda confiar en este componente y permitir su ejecución.

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda y Administración Pública</p> <p>Dirección General de Política Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad de applet 3.4</p>
---	---	--

5.4 Windows

- Con algunas configuraciones se producen avisos y errores en la consola de java, pero no impiden ni limitan la correcta ejecución del cliente de firma electrónica.
- En los entornos de 64 bits con JRE 6, aparece una alerta relativa al almacén de claves.

La descripción de la alerta es:

No se pudo inicializar el almacén de claves por defecto, ¿Desea intentar inicializar el almacén de Windows / Internet Explorer?

En este caso es necesario seleccionar un almacén PKCS#12/PFX de forma manual (un fichero con extensión .pfx) para continuar con la ejecución del cliente. Una vez seleccionado este fichero e indicado la contraseña de acceso, se selecciona el certificado en la ventana de selección y se completa la operación de la firma.

En los entornos de 64 bits se recomienda utilizar JRE 7.

- En Windows 8, sólo es posible utilizar el cliente de firma desde el escritorio clásico. Bajo la interfaz Modern UI no es posible la ejecución de plugins java desde el navegador web.

5.5 Guadalinex

- En Guadalinex 8 no ha sido posible completar ningún proceso de firma en ninguna de las configuraciones probadas.

5.6 Ubuntu

- A partir de la versión 35 del navegador Chrome, Google ha retirado el soporte al plugin de Java por lo que no resulta posible la ejecución de applets en esta versión del navegador. Más información en el siguiente enlace: <https://code.google.com/p/chromium/issues/detail?id=375909>.
- En ciertas configuraciones bajo Java 1.6 cuando se requiere seleccionar un certificado, se muestra el siguiente aviso en una ventana emergente:

No se pudo inicializar el almacén de claves por defecto. ¿Desea intentar inicializar el almacén PKCS#12 / PFX?

En este caso es necesario seleccionar un almacén PKCS#12/PFX de forma manual (un fichero con extensión .pfx) para continuar con la ejecución del cliente. Una vez seleccionado este fichero e indicado la contraseña de acceso, se selecciona el certificado en la ventana de selección y se completa la operación de la firma.

	Consejería de Hacienda y Administración Pública Dirección General de Política Digital	Plataforma @firma Matriz de compatibilidad de applet 3.4
---	---	---

5.7 Mac OS X

- El proceso de firma electrónica sólo se ha podido completar con JRE 1.7 y el navegador Safari.