



Consejería de Hacienda, Industria y Energía


Plataforma @firma

Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01

Versión:v01r00

Fecha: 24/06/2019

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, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01</p>
---	---	---

HOJA DE CONTROL


Título	Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01		
Entregable	Matriz de compatibilidad del cliente Miniapplet y AutoFirma		
Nombre del Fichero	20190624-MCF_Matriz-compatibilidad_Resumida_1_6_JAv01r00		
Autor	DGPD		
Versión/Edición	v01r00	Fecha Versión	24/06/2019
Aprobado por		Fecha Aprobación	
		Nº Total Páginas	8

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Primera versión del documento	DGTD	SCAE	24/06/2019


CONTROL DE DISTRIBUCIÓN

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

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01</p>
---	---	---

Índice de contenido

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
4.1	Entornos de escritorio (miniapplet y autofirma).....	7
4.2	Entornos móviles.....	7
4.3	Compatibilidad de formatos de firma.....	8

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01</p>
---	---	--


1 Objeto de este documento

El presente documento tiene por objeto mostrar de forma resumida la matriz de compatibilidad del cliente de firma Miniapplet 1.6JAv01 y de AutoFirma v1.6JAv01 conforme a las pruebas de aceptación realizadas.

Para los formatos trifásicos se ha utilizado la versión de los servlets MiniApplet 1.6JAv01-Server.

Estas versiones de los componentes “miniapplet” y “autofirma” contienen modificaciones sobre el código de las versiones liberadas por el Ministerio de Hacienda y Administraciones Públicas. Estas modificaciones tienen como finalidad la corrección de errores y la implementación de nuevas funcionalidades.

Este documento constituye una versión resumida del equivalente en versión “Matriz de compatibilidad de Miniapplet 1.6JAv01 y Autofirma 1.6JAv01”

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01</p>
---	---	---

2 Descripción de las pruebas realizadas


El plan de pruebas que se contempla en este documento se realiza mediante la firma por defecto utilizada por el Miniapplet y AutoFirma, conformando la primera fase de pruebas de las distribuciones.

- Formato de generación monolíticos: CAdES-BES, PAdES-BES, PadES-BES
- Formatos de generación trifásica: CAdES-TRI, XAdES-TRI, PAdES-TRI
- Algoritmo de resumen: SHA256
- Algoritmo de firma: SHA256withRSA

Posteriormente, en una segunda fase se realizarán firmas más complejas utilizando las mismas herramientas.

- Formatos de firma: CAdES, XAdES, PAdES, CMS, XMLDSig, etc...
- Multifirmas: Firma en cascada y en paralelo.
- Firma masiva: Firma de varios ficheros en una sola solicitud.
- Algoritmos de firma: SHA256withRSA y SHA512withRSA.

La "**GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-807) CRIPTOLOGÍA DE EMPLEO EN EL ESQUEMA NACIONAL DE SEGURIDAD**" en su última versión (v. 1.7 de abril de 2015) indica en su apartado 5.7. FIRMA ELECTRÓNICA que a partir del 1 de enero de 2017 no se permite el uso de función resumen SHA-1

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01</p>
---	---	---

3 Descripción de los entornos de prueba

Para la realización de las pruebas se han creado máquinas virtuales usando el Software Oracle VirtualBox conforme a la metodología especificada en el documento “Plan de Pruebas del Miniapplet v3.0”.

Los entornos considerados para verificar la compatibilidad de la firma en un entorno de escritorio han sido los siguientes:


- **Sistemas operativos:** Windows 7, Windows 10, Ubuntu 18.04 LTS, Gecos 3 y Mac OS X.
- **Navegadores:** Microsoft Internet Explorer 11, Microsoft Edge (Windows 10), Mozilla Firefox 66, Google Chrome 73 y Safari (Mac OS X).
- **Java:** Se ha utilizado la versión 8u181.

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

- **Android.** Se han utilizado versiones compatibles con el cliente móvil publicado en Google Play. El cliente de firma móvil es compatible con la versión de Android 7 y superiores.
 - Autofirma Junta de Andalucía 1.6JAv01
- **iOS:** Se ha utilizado con la versión 12 de iOS.
 - Autofirma Junta de Andalucía 1.6JAv01

Para el certificado se ha utilizado el almacén del navegador o, en su defecto, el almacén del propio sistema operativo.

Para más detalles sobre las configuraciones utilizadas en las pruebas consultar el documento “Matriz de compatibilidad de Miniapplet y Autofirma 1.6JAv01

 <p>JUNTA DE ANDALUCÍA</p>	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Plataforma @firma</p> <p>Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01</p>
---	---	---

4 Matriz de compatibilidad

A continuación se muestra la matriz de compatibilidad para los diferentes escenarios

4.1 Entornos de escritorio (miniapplet y autofirma)

S.O.	Firefox	Chrome	IE	Edge	Chromium	Safari
Windows 7	AF	AF	AP AF	N/D	N/D	N/D
Windows 10	AF	AF	AP AF	AF	N/D	N/D
Ubuntu 18.04	AF	AF	N/D	N/D	AF	N/D
Gecos v3	AF	AF	N/D	N/D	AF	N/D
Mac OS X 10.14 Mojave	AF	AF	N/D	N/D	N/D	AF

Leyenda:

AP: Compatible con APLET.

AF: Compatible con AUTOFIRMA.

N/D: Configuración no disponible.

NF: No funciona con ningún cliente (applet ni autofirma).

Colores:

Verde: Configuración compatible.

Amarillo: Configuración parcialmente compatible. Puede presentar algún problema.


Rojo: Configuración no compatible.

Gris: Configuración no soportada, no disponible o no probada.

4.2 Entornos móviles

La siguiente matriz recopila la información de compatibilidad a la hora de generar las firmas mediante dispositivos móviles contemplados en el plan de pruebas.

S.O.	Compatible
Android 7 o superior	OK
IOS 12	OK

	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Plataforma @firma Matriz de compatibilidad Resumida de Miniapplet y Autofirma 1.6.JAv01
---	--	--

4.3 Compatibilidad de formatos de firma

En este apartado se muestra las matrices de compatibilidad respecto al formato y modalidad de firma:

S.O.	Formato de firma					
	CAAdES		XAdES		PAdES	
	Mono	Tri	Mono	Tri	Mono	Tri
Miniapplet / Autofirma	OK	OK	OK	OK	OK	OK
Android 7 o superior	OK	OK	NOK	OK	OK	OK
IOS 12	OK	OK	OK	OK	OK	OK

Legenda:

OK: Configuración que ha funcionado satisfactoriamente.

NOK: Configuración que no ha funcionado correctamente.

N/D: Configuración no disponible.