



Consejería de Hacienda, Industria y Energía


Autofirma 1.6JAv01

Manual de Gestión

Versión: v16r01

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.


	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Autofirma 1.6JAv01 Manual de Gestión
---	--	---

HOJA DE CONTROL

Título	Manual de Gestión		
Entregable	Manual de Gestión del componente Autofirma		
Nombre del Fichero	20190624-Autofirma_Manual de Gestion_V16r01		
Autor	DGTD		
Versión/Edición	v16r01	Fecha Versión	24/06/2019
Aprobado por		Fecha Aprobación	-
		Nº Total Páginas	31


REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v16r00	Primera versión del documento	DGTD	SCAE	22/04/2019
V16r01	Revisión del documento	DGTD	SCAE	24/06/2019

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

ÍNDICE

1	Introducción.....	4
1.1	Adecuación al Esquema Nacional de Seguridad.....	5
2	Requisitos mínimos.....	6
3	Funcionamiento de AutoFirma.....	8
3.1	Uso del DNle.....	8
3.2	Comunicación con servicios externos.....	9
4	Enlaces de descarga.....	10
5	Instalación.....	11
6	Gestión de Autofirma.....	12
6.1	Comprobaciones de nuevas versiones al inicio de la aplicación.....	12
6.2	Configuración a través de fichero.....	13
6.3	Configuración a través del registro en Microsoft Windows.....	20
6.4	Opciones configurables.....	20
7	Obtención de estadísticas con Google Analytics.....	30
8	Error al importar las opciones de configuración desde un fichero.....	31

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

1 Introducción

AutoFirma es una herramienta de escritorio con interfaz gráfica que permite la ejecución de operaciones de firma de ficheros locales en entornos de escritorio: Windows, Linux (Ubuntu y Gecos) y Mac OS X. También puede utilizarse a través de consola o ser invocada por otras aplicaciones mediante protocolo para la ejecución de operaciones de firma. Esta última funcionalidad puede usarse principalmente mediante el JavaScript de despliegue del MiniApplet @firma, que permitiría que se utilizase AutoFirma en lugar del propio MiniApplet para generar las firmas de un trámite web.

Además de la versión nativa de AutoFirma, existe una versión Java WebStart que puede desplegarse para poder realizar operaciones de firma con AutoFirma desde trámites sin necesidad de que este esté instalado previamente. El despliegue de esta versión de AutoFirma también se realiza mediante el JavaScript de despliegue del MiniApplet @firma.

El presente documento se centra principalmente en el uso de AutoFirma para firmas por medio del JavaScript de despliegue del MiniApplet @firma.

El cliente AutoFirma hace uso de los certificados digitales X.509v3 y de las claves privadas asociadas a estos que estén instalados en el repositorio o almacén de claves y certificados (KeyStore) del sistema operativo o del navegador Web (Internet Explorer, Mozilla Firefox, etc.) en caso de realizarse la operación desde un trámite web. También permite el uso de dispositivos externos (tarjetas inteligentes, dispositivos USB) configurados en estos almacenes de claves (como por ejemplo, el DNI Electrónico o DNle).


El cliente AutoFirma hace uso de las claves privadas asociadas a los certificados del usuario y no permite que estos salgan en ningún momento del almacén (tarjeta, dispositivo USB o navegador) ubicado en su PC.

AutoFirma no almacena ningún tipo de información personal del usuario, ni hace uso de cookies ni ningún otro mecanismo para la gestión de datos de sesión. AutoFirma sí almacena trazas de su última ejecución a efectos de ofrecer soporte al usuario si se encontrase algún error. Estas trazas de ejecución no contienen ningún tipo de información personal y la aplicación no facilita de ninguna forma el acceso a estos datos almacenados.

AutoFirma es una aplicación de Software Libre publicado que se puede usar, a su elección, bajo licencia GNU General Public License versión 2 (GPLv2) o superior o bajo licencia European Software License 1.1 (EURL 1.1) o superior.

Puede obtener la última versión de la aplicación Autofirma desde la siguiente dirección web:

<https://ws024.juntadeandalucia.es/clienteafirma/autofirma/autofirma.html>


	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Autofirma 1.6JAv01 Manual de Gestión
---	--	---

1.1 Adecuación al Esquema Nacional de Seguridad

Los productos de la Suite de @firma pueden contener entre los algoritmos disponibles, algunos no recomendados por la Guía 807 del Esquema Nacional de Seguridad (ENS; editada por el Centro Criptológico Nacional, CCN) vigente en el momento de publicación de este documento. Por lo que queda bajo la responsabilidad de las aplicaciones que hacen uso de estos productos el configurar adecuadamente las llamadas a los mismos para generar el resultado esperado, válido y adecuado para ese momento y el nivel de seguridad deseado, utilizando para ello algoritmos de la familia SHA-2 tal y como especifica dicha norma para la generación de firmas electrónicas.

Puede consultar la norma vigente desde el siguiente enlace:


<https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html>

	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Autofirma 1.6JAv01 Manual de Gestión
---	--	---

2 Requisitos mínimos

El uso de AutoFirma como herramienta de firma integrada dentro del proceso de firma de trámites web tiene los siguientes requerimientos en cuanto a entorno operativo:

- Sistema Operativo
 - Microsoft Windows 7 o superior.
 - Soportado directamente en 7, 8, 8.1 y 10.
 - En 32 o 64 bits.
 - Linux
 - Gecos, Ubuntu.
 - Apple OS X Yosemite o superior.
 - Soportado directamente en Yosemite, El Capitán, Sierra, High Sierra, Mojave.
- Navegadores Web (para la invocación por protocolo)
 - Microsoft Windows
 - Google Chrome 46 o superior.
 - Mozilla Firefox 41.0.1 o superior.
 - Microsoft Internet Explorer 11. Compatibilidad parcial con versiones anteriores de Internet Explorer (8-10).
 - Microsoft Edge v20 o superior.
 - Linux
 - Mozilla Firefox 41.0.1 o superior.
 - Google Chrome 46 o superior
 - Chromium 46 o superior.
 - Apple OS X
 - Apple Safari 9.0 o superior.
 - Google Chrome 46 o superior.
 - Mozilla Firefox 41.0.1 o superior.


	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

ADVERTENCIA: El funcionamiento de AutoFirma al invocarlo desde Microsoft Edge, versiones de Internet Explorer anteriores a la 11 (o Internet Explorer 11 en modo de compatibilidad con una versión anterior) o Safari 10 está limitado a las firmas trifásicas realizadas a través de servidor intermedio (Consulte el manual del integrador del MiniApplet para más detalles) . Para asegurar el correcto funcionamiento de las operaciones de firma online utilice otro de los navegadores soportados.

En entornos OS X y Windows no es necesario tener instalado un entorno de ejecución de Java. En Linux se necesita un entorno de ejecución de Java 8 de Oracle u OpenJDK 8 (marcado como dependencia en el instalador integrado de AutoFirma).

Es obligatorio que AutoFirma sea instalado antes de iniciar el trámite web en el que se usará para ejecutar las operaciones de firma.

Es necesario cerrar las instancias y procesos de todos los navegadores antes de proceder a la instalación de Autofirma.

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

3 Funcionamiento de Autofirma

Cuando el entorno del ciudadano firmante no cuenta con un entorno de ejecución de Java instalado y un navegador Web compatible con la ejecución de Applets, el despliegue del MiniApplet deriva las tareas de firma a la aplicación Autofirma, sin necesidad de que el integrador deba gestionar por su parte esta delegación de tareas. Para aquel integrador que desee conocer los detalles del uso de Autofirma en trámites web, puede consultar el documento **“MCF_manual-integrador_ES.pdf”**.

En cualquier caso, para que Autofirma pueda asumir cualquier operación de firma, es necesario que esté instalada en el equipo local antes de iniciar el trámite de firma. Es responsabilidad del integrador alertar de este hecho cuando sea susceptible que los usuarios no tengan instalada la aplicación.

Ya se ejecute Autofirma como aplicación de escritorio o sea lanzada por el navegador web, Autofirma registra la operativa de su última ejecución en un fichero de trazas en el subdirectorío oculto “.afirma” del directorio del usuario. Por ejemplo, “C:\Users\miusuario\.afirma” en S.O. Windows. El fichero generado tiene el nombre “AUTOFIRMA.afirma.log.xml”. Los ficheros de trazas del Cliente @firma en ningún caso almacenan información de carácter personal.

3.1 Uso del DNle


El Cliente @firma utiliza la biblioteca JMulticard para permitir firmar con DNle 2.0 y 3.0 sin necesidad de que los usuarios tengan instalados los controladores de la tarjeta. Esta biblioteca se utilizará al seleccionar la opción “Continuar con DNle” al abrir Autofirma o al invocar a la aplicación desde una página web e insertar el PIN de la tarjeta.

Autofirma solicita el PIN de la tarjeta antes de listar los certificados del almacén y de que el usuario indique qué certificado desea utilizarla para firmar. Este comportamiento emula el de los controladores PKCS#11 de las tarjetas en donde el PIN es necesario para listar los certificados contenidos por la tarjeta y sigue la lógica de que si un usuario ha insertado el DNle en el lector es porque lo desea utilizar. Cuando el usuario inserta el PIN, se listan sus certificados y se abre el canal seguro con la tarjeta y, en el momento de firmar, se utiliza este canal seguro para realizar la operación. A continuación, se cierra el canal seguro.

Las operaciones de firma realizadas posteriormente solicitarán el PIN de la tarjeta sólo en el momento de realizar la firma, momento en el cual se volverá a abrir el canal seguro con la tarjeta.

Si se recargase el almacén por medio de la opción correspondiente del diálogo de selección de certificados, el controlador se reiniciaría y volvería a pedir el PIN de la tarjeta para listar los certificados.

En el caso de ejecutar Autofirma como aplicación de escritorio en Windows y seleccionar “Usar cualquier certificado” o haberlo invocado desde Internet Explorer o Chrome y cancelar el diálogo de PIN del DNle de JMulticard, se cargará el almacén del sistema normalmente. Si se tiene instalado el controlador oficial del DNle en el equipo esto puede implicar que los certificados del DNle se listen también en el diálogo de selección de certificados ya que será el controlador oficial el que los cargue. En estos casos, también se usará el controlador oficial para realizar la firma.

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

3.2 Comunicación con servicios externos

Cuando AutoFirma se comunica con servicios externos, por ejemplo, para comprobar si existe una nueva versión o para la comunicación con el navegador web a través del servidor intermedio (consulte el apartado **“Compatibilidad con dispositivos móviles y AutoFirma”** del manual **“MCF_manual-integrador_ES.pdf”** para más información), se utiliza la configuración de proxy de red establecida en AutoFirma y el almacén de confianza de la JRE con la cual se ejecute la aplicación.

Para saber más sobre la configuración del proxy de red en AutoFirma consulte la ayuda integrada de AutoFirma (para la configuración a través de interfaz gráfica) o las opciones de configuración referentes al proxy en el apartado **“6.4.1 Opciones Generales”** (para la configuración de la aplicación por parte de un administrador).

En el caso de los certificados de confianza, AutoFirma utilizará el almacén de confianza de la JRE instalada junto a la propia aplicación (en las instalaciones de Windows o macOS) o el almacén de confianza de la JRE instalada en el sistema que se utilice para ejecutarla (en el caso de Linux y AutoFirma WebStart).

Cuando AutoFirma intente acceder a un recurso de red o servicio externo sobre una comunicación SSL, rechazará la conexión en caso de que la conexión se cifrase utilizando un certificado SSL emitido por un prestador distinto a los incluidos en el almacén de confianza o cuando fuese expedido para un dominio distinto al que se intenta acceder. Esta medida de seguridad es necesaria para evitar ataques de seguridad que redireccionen las peticiones del cliente a servidores inseguros.


Para evitar problemas de conexión, asegúrese de cifrar su comunicación SSL con certificados reconocidos por defecto por Java. En caso contrario, el usuario o el administrador de los equipos deberán incluir los certificados de la entidad emisora del certificado SSL en el almacén de confianza de la JRE utilizada.

Para facilitar el despliegue a las entidades que utilizan certificados SSL emitidos por autoridades españolas, en el almacén de confianza de las JRE con las que se distribuyen las versiones de Windows y macOS se incluyen por defecto los certificados raíces de los siguientes prestadores:

- Agencia de Tecnología y Certificación Electrónica (ACCV)
- Fábrica Nacional de Moneda y Timbre (FNMT)

Así pues, AutoFirma permitirá por defecto la conexión con los servicios desplegados sobre conexiones SSL construidas con certificados de estos prestadores.

Esta lista de prestadores podrá variar en futuras versiones de AutoFirma según las solicitudes realizadas por los propios prestadores o entidades públicas que utilicen sus certificados. Requisito indispensable para incorporar un nuevo prestador a esta lista es que se trate de un prestador reconocido por el Ministerio de Energía, Turismo y Agenda Digital.

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

4 Enlaces de descarga

Puede descargar la última versión disponible de AutoFirma desde la siguiente página web:

<https://ws024.juntadeandalucia.es/clienteafirma/autofirma/autofirma.html>

Con cada nueva versión que sea publicada en los repositorios de la Junta de Andalucía, la aplicación informará de que hay una actualización disponible durante el arranque de la misma.

Autofirma



Aplicación de firma electrónica de escritorio

Autofirma es una aplicación que le permite firmar electrónicamente para la realización de trámites administrativos con la Junta de Andalucía desde un navegador web.


Puede descargar la aplicación desde el enlace inferior:

Versión 1.6JAv01 (17/06/2019):

Windows 32: **exe msi**
 Windows 64: **exe msi**
 Linux 64 (Ubuntu 18.04 recomendado): **deb**
 Mac OS X: **pkg**
 Manual de Usuario: **pdf**

Pulsando en el enlace marcado en rojo en la imagen superior se le descargará el fichero de instalación con el nombre correspondiente a la versión indicada y para al Sistema Operativo seleccionado. Adicionalmente, también disponemos en esta página del enlace para descargar este manual.

AutoFirma 1.6JAv01 – Cuarta versión publicada por la Junta de Andalucía. (Compatible con Windows, Linux y Mac OS X)

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

5 Instalación

Para la instalación de Autofirma consulte el manual de instalación correspondiente (**Autofirma_Manual de Instalación.pdf**)

6 Gestión de Autofirma

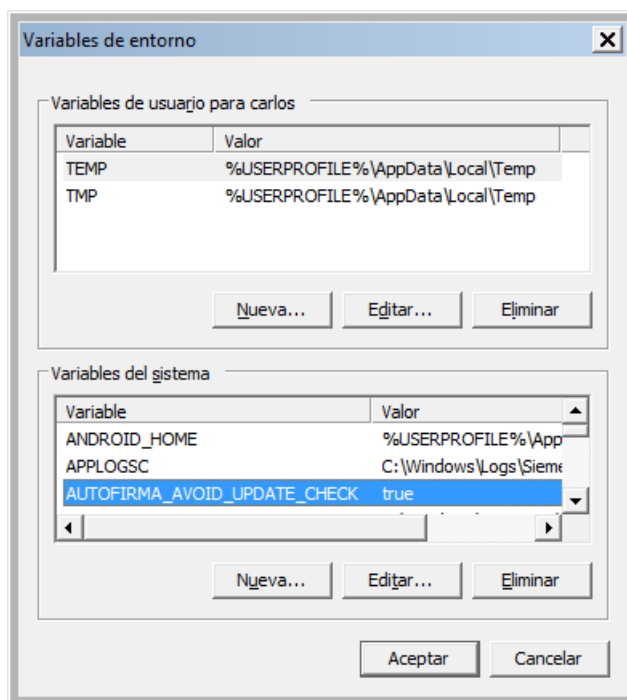
6.1 Comprobaciones de nuevas versiones al inicio de la aplicación

AutoFirma siempre comprueba al arrancar si hay una versión más actual disponible para descarga desde la página Web del proyecto para evitar que se realicen trámites de firma con una versión obsoleta o antigua que pudiese tener instalada el ciudadano.


Es posible deshabilitar esta comprobación de diversas maneras:

- Un usuario puede desactivar la actualización por medio de la opción “**Buscar actualizaciones al inicio**” en la pestaña General del menú de preferencias de la aplicación.
- Un usuario o administrador puede desactivar la actualización por medio del fichero de configuración con la opción checkForUpdates. Consulte el apartado “**Configuración a través de fichero**” para más información.
- Un usuario o administrador puede desactivar la actualización estableciendo, a nivel de sistema operativo, la siguiente variable de entorno **AUTOFIRMA_AVOID_UPDATE_CHECK** con el valor true. Es posible que sea necesario reiniciar el equipo para que la JVM detecte correctamente el nuevo valor de esta variable.

En el caso de Windows, por ejemplo, esto sería:



La inhabilitación de las comprobaciones de actualización sólo sería recomendable en entornos controlados (corporativos, internos a una administración, etc.) o cuando se sepa de problemas de incompatibilidad de las

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

nuevas versiones con alguna aplicación. Por regla general, siempre es conveniente descargar e instalar las últimas versiones disponibles.

En caso de detectarse una nueva versión, AutoFirma permitirá al usuario abrir la página de descarga de la aplicación.

6.2 Configuración a través de fichero

AutoFirma permite que se configure a través de un fichero importado desde la pestaña General del panel de Preferencias de la aplicación. Esta opción está orientada principalmente a su uso por parte de administradores que hagan despliegues de la aplicación y que requieren que sus usuarios utilicen siempre unas propiedades concretas de firma.

El fichero de configuración debe tener como extensión “**.afconfig**”.

Es importante notar que las propiedades establecidas a través del menú de preferencias sólo afectan a la ejecución de la aplicación en modo escritorio. En las operaciones de firma solicitadas desde un navegador web siempre se utilizará la configuración de firma proporcionada en la operación. Excepción a esto es la configuración de proxy, que afectará a la ejecución de la aplicación en ambas modalidades.

Este fichero no tiene porqué contener todas las propiedades que admite la aplicación, puede contener sólo aquellas que deseamos configurar. Si se importa un fichero que no define el valor de alguna propiedad, esta propiedad tendrá asignada el valor por defecto de la aplicación o, si se modificó previamente, el valor que ya tuviese asignado.

Las opciones que se podrán configurar serán todas aquellas que pueden establecerse a través del panel de preferencias de la aplicación, además de alguna opción adicional.

El listado completo de opciones configurables aparece en el apartado “**6.4 Opciones configurables**”.


El fichero de configuración en cuestión, será un fichero PList, compuesto por un diccionario con el listado de claves y valores de las propiedades. Las claves siempre se designarán mediante una cadena de texto y el valor puede ser una cadena (String) o un valor de tipo verdadero/falso (true/false).

Este fichero PList puede firmarse con una firma en formato XAdES Enveloped. Si se delega en los usuarios la importación del fichero de configuración, puede pedir que comprueben el firmante del fichero con una herramienta externa como VALIDe para que confirmen que se firmó con el certificado adecuado.

6.2.1 Bloqueo de la configuración

Un uso interesante de la configuración de la aplicación entre los usuarios de un organismo o entidad es que permite bloquear las opciones que el usuario va a poder modificar. Hay opciones que son especialmente interesantes de fijar para que se apliquen a todas las firmas, como las políticas de firma, y otras que no se pueden bloquear debido a que afectan en gran medida al contexto de cada firma, como el lugar de realización de la firma o si se quiere hacer visible la firma de los PDF.

Las opciones de configuración de la aplicación pueden bloquearse por medio de la opción “**preferencesUnprotected**”, como se describe en el apartado 6.4.6 Opciones no configurables desde la ventana de preferencias

	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Autofirma 1.6JAv01 Manual de Gestión
---	--	---

Se indican aquí las propiedades del panel de preferencias que el usuario va a poder seguir configurando aunque se bloquee la configuración general de la aplicación:

Pestaña General

- No pedir confirmación al cerrar la aplicación
- No mostrar la pantalla inicial de DNle y trabajar siempre con cualquier certificado
- Buscar actualizaciones al inicio
- Enviar estadísticas de uso de forma anónima para ayudar a mejorar el uso de la aplicación

Preferencias de configuración de firma electrónica

General Firmas PAdES (PDF) Firmas CAdES Firmas XAdES Factura Electrónica Almacenes de claves

Opciones generales

- ☒ No pedir confirmación al cerrar la aplicación
- ☐ No mostrar la pantalla inicial de DNIe y trabajar siempre con cualquier certificado
- ☒ Buscar actualizaciones al inicio
- ☒ Enviar estadísticas de uso de forma anónima para ayudar a mejorar la aplicación

Opciones de firma

Algoritmo de firma

SHA1withRSA

Formatos de firma por defecto

Documentos PDF	PAdES
Documentos OOXML de Microsoft Office	OOXML (Office Open XML)
Facturas electrónicas	FacturaE
Ficheros XML genéricos	XAdES
Ficheros ODF de LibreOffice u OpenOffice	ODF (Open Document Format)
Ficheros binarios genéricos	CAdES

Aplicar ahora Aceptar Cancelar

Pestaña Firmas PAdES

- Metadatos para firmas PAdES
- Firma visible

Preferencias de configuración de firma electrónica

General Firmas PAdES (PDF) Firmas CAdES Firmas XAdES Factura Electrónica Almacenes de claves

Política de firma

Ninguna política

Identificador de la política (debe ser un OID)

Huella digital del identificador de la política (en Base64)

Algoritmo de la huella digital del identificador de la política

SHA1

Calificador de la política (URL)

Metadatos de las firmas PAdES

Razón por la que se firma el documento

Ciudad en la que se realiza la firma

Contacto del firmante (usualmente una dirección de correo electrónico)

Opciones de firma

Formato avanzado de firma

PAdES Básico

Firma visible

☐ Permitir firmas visibles en el PDF

Aplicar ahora Aceptar Cancelar

Pestaña Firmas XAdES

- Metadatos para firmas XAdES

Preferencias de configuración de firma electrónica

General Firmas PAdES (PDF) Firmas CAdES Firmas XAdES Factura Electrónica Almacenes de claves

Política de firma

Ninguna política

Identificador de la política (debe ser una URI)

Huella digital del identificador de la política (en Base64)

Algoritmo de la huella digital del identificador de la política

SHA1

Calificador de la política (URL)

Metadatos de las firmas XAdES

Ciudad en la que se realiza la firma

Provincia en la que se realiza la firma

Código postal del lugar en el que se realiza la firma

País en el que se realiza la firma

Cargo atribuido al firmante

Opciones de firma

Formato de las firmas XAdES

XAdES Detached

Aplicar ahora Aceptar Cancelar

Pestaña Factura electrónica

- Metadatos de las facturas electrónicas
- Papel del firmante de la factura electrónica

Preferencias de configuración de firma electrónica

General Firmas PAdES (PDF) Firmas CAdES Firmas XAdES Factura Electrónica Almacenes de claves

Política de firma

Política de Factura Electrónica 3.1

Metadatos de las facturas electrónicas

Ciudad en la que se realiza la firma

Código postal del lugar en el que se realiza la firma

País en el que se realiza la firma

Provincia en la que se realiza la firma

Opciones de firma

Papel del firmante de la factura electrónica

Emisor

Aplicar ahora Aceptar Cancelar

6.2.2 Firma del fichero de configuración

El fichero de configuración deberá estar firmado con una firma XAdES Enveloped y un certificado emitido por la autoridad intermedia definida por el Ministerio de Defensa en el momento de empaquetar la aplicación Autofirma para su distribución.

El administrador encargado de configurar y distribuir este fichero puede firmarlo con la propia herramienta Autofirma. Los pasos para preparar la aplicación para la firma de este fichero son:

1. Disponer del certificado de firma en el almacén prioritario configurado en la aplicación o en el almacén por defecto, si no se dispone del certificado en tarjeta criptográfica.
2. Desde la pestaña de configuración "General" de las preferencias de la aplicación, configurar que los "Ficheros XML genéricos" se firmen con firma "XAdES".
3. En la pestaña "Firma XAdES" de las preferencias de la aplicación, configurar que el formato de firma XAdES sea "XAdES Enveloped".

A continuación, podrá firmarse el fichero de configuración normalmente, seleccionando como certificado de firma el configurado en el primer paso.

6.2.3 Ejemplo de fichero de configuración

A continuación se muestra el contenido de un fichero simple de configuración:

```
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
  <dict>
    <key>codesImplicitMode</key>
    <string>attached</string>
    <key>createHashAsBase64</key>
    <true/>
  </dict>
</plist>
```

En este fichero se establece que las firmas CADES contengan por defecto los datos firmados (codesImplicitMode) y que las huellas digitales realizadas se generen en base 64 (createHashAsBase64). El resto de la configuración del usuario permanecerá tal como estaba en el momento de importar el fichero de configuración.

En este ejemplo, el fichero de configuración no está firmado.

6.3 Configuración a través del registro en Microsoft Windows

Es común que en los entornos controlados de usuarios se disponga de herramientas para el despliegue masivo de aplicaciones y que estas también permitan la configuración del sistema modificando directamente el registro de Microsoft Windows. Cuando este es el caso, el administrador del sistema podrá configurar el comportamiento de AutoFirma modificando algunas claves de registro.

Autofirma almacena en el registro de Windows todas las opciones de configuración establecidas mediante el panel de preferencias o un fichero de configuración importado. Concretamente, la configuración de AutoFirma se almacena en la clave de registro:

HKEY_CURRENT_USER\Software\JavaSoft\Prefs\es\gob\afirma\standalone\ui\preferences

Un administrador puede establecer a través del registro todas las opciones declaradas en el apartado 6.4 Opciones configurables para determinar así el comportamiento de AutoFirma.

6.4 Opciones configurables

Las opciones de configuración que se pueden establecer mediante fichero o a través del registro de Windows se presentan a continuación, separadas según la pestaña del panel de preferencias en la que se encuentran y reunidas en un apartado “Opciones globales” aquellas que no puede configurar directamente el usuario.

6.4.1 Opciones Generales

Clave	Tipo	Descripción
omitAskOnClose	true/false	Evita la confirmación al cerrar la aplicación o no. Un valor <i>true</i> en esta preferencia permitirá cerrar la aplicación sin ningún diálogo de advertencia. Un valor <i>false</i> (por defecto) hará que se muestre un diálogo para que el usuario confirme que realmente desea cerrar la aplicación.
hideDnieStartScreen	true/false	No mostrar la pantalla inicial de uso de DNle. Un valor <i>true</i> en esta preferencia hace que nunca se muestre la pantalla inicial que sugiere al usuario el uso directo del DNle como almacén de claves. Un valor <i>false</i> (por defecto) hará que se muestre esta pantalla al inicio siempre que se detecte un lector de

		tarjetas en el sistema.
checkForUpdates	true/false	Buscar actualizaciones al iniciar la aplicación. Un valor de true (por defecto) en esta preferencia hace que, al iniciar la aplicación, se compruebe automáticamente si hay publicadas versiones más actuales. Un valor de false hará que no se haga esta comprobación.
useAnalytics	true/false	Envía estadísticas de uso. Un valor de true (por defecto) hace que, al arrancar, la aplicación envíe de forma anónima estadísticas de uso a Google Analytics. Un valor de false hará que no se envíe ningún dato.
signatureAlgorithm	String	<p>Algoritmo de firma. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • SHA1withRSA • SHA256withRSA (Por defecto) • SHA384withRSA • SHA512withRSA
defaultSignatureFormatPdf	String	<p>Formato en el que se firmarán los documentos PDF. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • PAdES (Por defecto) • CAdES • XAdES
defaultSignatureFormatOoxml	String	<p>Formato en el que se firmarán los documentos OOXML. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • OOXML (Office Open XML) (Por defecto) • CAdES

		<ul style="list-style-type: none"> • XAdES
defaultSignatureFormatFacturae	String	<p>Formato en el que se firmarán las facturas electrónicas. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • FacturaE (Por defecto) • CAdES
defaultSignatureFormatXml	String	<p>Formato en el que se firmarán los documentos XML. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • XAdES (Por defecto) • CAdES
defaultSignatureFormatOdf	String	<p>Formato en el que se firmarán los documentos ODF (LibreOffice, OpenOffice.org...). Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • ODF (Open Document Format) (Por defecto) • CAdES • XAdES
defaultSignatureFormatBin	String	<p>Formato en el que se firmarán los ficheros binarios. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • CAdES (Por defecto) • XAdES
proxySelected	true/false	<p>Habilita o deshabilita la configuración particular de proxy. El valor true configura que se aplique la configuración particular indicada a continuación, mientras que el valor false (por defecto) no la habilitaría.</p>
proxyHost	String	<p>URL del servicio del servidor proxy.</p>

proxyPort	String	Número de puerto para la comunicación con el servidor proxy.
proxyUsername	String	Nombre de usuario con el que acceder al servidor proxy.
proxyPassword	String	Contraseña del usuario para la conexión con el servidor proxy.


6.4.2 Firmas PadES (PDF)

Clave	Tipo	Descripción
padesPolicyIdentifier	String	Identificador de la política de firma para PAdES.
padesPolicyIdentifierHash	String	Huella digital, en Base64, del identificador de la política de firma para PAdES.
padesPolicyIdentifierHashAlgorithm	String	Algoritmo de la huella digital del identificador de la política de firma para PAdES. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> • SHA1 (Por defecto) • SHA-512 • SHA-384 • SHA-256
padesPolicyQualifier	String	Calificador de la política de firma para PAdES.
padesSignReason	String	Motivo de la firma en firmas PAdES.

padesSignProductionCity	String	Ciudad de firma para firmas PAdES
padesSignerContact	String	Contacto del firmante en firmas PAdES.
padesBasicFormat	String	<p>Formato de firma PAdES. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • PAdES-BES • PAdES Básico (Por defecto)
padesVisibleSignature	true/false	Si está establecido a true, establece por defecto que se pida al usuario que determine mediante diálogos gráficos los parámetros de una firma visible PDF y se inserte como tal en el documento. Si está a false (valor por defecto), se realizarán firmas invisibles PDF.

6.4.3 Firmas CAdES


Clave	Tipo	Descripción
cadesPolicyIdentifier	String	Identificador de la política de firma para CAdES.
cadesPolicyIdentifierHash	String	Huella digital, en Base64, del identificador de la política de firma para CAdES.
cadesPolicyIdentifierHashAlgorithm	String	<p>Algoritmo de la huella digital del identificador de la política de firma para CAdES. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> • SHA1 (Por defecto) • SHA-512 • SHA-384 • SHA-256

	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Autofirma 1.6JAv01 Manual de Gestión
---	--	---

cadesPolicyQualifier	String	Calificador de la política de firma para CAdES
cadesImplicitMode	String	Indica si la firma CAdES debe realizarse en modo implícito (attached) (por defecto) o no (detached).

6.4.4 Firmas XAdES

Clave	Tipo	Descripción
xadesPolicyIdentifier	String	Identificador de la política de firma para XAdES.
xadesPolicyIdentifierHash	String	Huella digital, en Base64, del identificador de la política de firma para XAdES.
xadesPolicyIdentifierHashAlgorithm	String	Algoritmo de la huella digital del identificador de la política de firma para XAdES. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> • SHA1 (Por defecto) • SHA-512 • SHA-384 • SHA-256
xadesPolicyQualifier	String	Calificador de la política de firma para XAdES.
xadesSignatureProductionCity	String	Ciudad en la que se realiza la firma.
xadesSignatureProductionProvince	String	Provincia en la que se realiza la firma.
xadesSignatureProductionPostalCode	String	Código postal en la que se realiza la firma.
xadesSignatureProductionCountry	String	País en la que se realiza la firma.

	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Autofirma 1.6JAv01 Manual de Gestión
---	--	---

xadesSignerClaimedRole	String	Cargo supuesto para el firmante.
xadesSignFormat	String	Formato de las firmas XAdES. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> • XAdES Detached • XAdES Enveloping (Por defecto) • XAdES Enveloped

6.4.5 Firmas Factura Electrónica


Clave	Tipo	Descripción
facturaEPolicy	String	<p>Versión de la política de firma de factura electrónica. Los valores posibles son:</p> <ul style="list-style-type: none"> • 3.0: Política de firma 3.0. • 3.1: Política de firma 3.1 (por defecto). <p>Esta propiedad configura el resto de propiedades de la política de firma de factura cuando se establece desde la interfaz gráfica. Al establecerlo mediante fichero de configuración es necesario establecer también las siguientes 3 propiedades: facturaePolicyIdentifier, facturaePolicyIdentifierHash y facturaePolicyIdentifierHashAlgorithm</p>
facturaePolicyIdentifier	String	Establece el identificador de la política de firma de factura

		<p>electrónica.</p> <p>Para configurar la política de firma 3.0 se debe establecer el valor: http://www.facturae.es/politicade_firma_formato_facturae/politica_de_firma_formato_facturae_v3_0.pdf</p> <p>Para configurar la política de firma 3.1 se debe establecer el valor: http://www.facturae.es/politica_de_firma_formato_facturae/politica_de_firma_formato_facturae_v3_1.pdf</p>
facturaePolicyIdentifierHash	String	<p>Establece la huella digital de la política de firma de factura electrónica.</p> <p>Para configurar la política de firma 3.0 se debe establecer el valor: <code>xmfh8D/Ec/hHeE1IB4zPd61zHIY=</code></p> <p>Para configurar la política de firma 3.1 se debe establecer el valor: <code>Ohixl6upD6av8N7pEvDABhEL6hM=</code></p>
facturaePolicyIdentifierHashAlgorithm	String	<p>Algoritmo de la huella digital del identificador de la política de firma de factura electrónica.</p> <p>Para configurar las políticas de firma 3.0 y 3.1 se debe establecer el valor: SHA1</p>
facturaeSignatureProductionCity	String	Ciudad en la que se realiza la firma.
facturaeSignatureProductionProvince	String	Provincia en la que se realiza la firma.
facturaeSignatureProductionPostalCode	String	Código postal en el que se realiza la firma.
facturaeSignatureProductionCountry	String	País en el que se realiza la firma.
facturaeSignerRole	String	Rol ejercido por el firmante en el proceso de firma. Debe tener uno


		de estos valores: <ul style="list-style-type: none"> • Emisor (Por defecto) • Receptor • Tercero
--	--	---

6.4.6 Opciones no configurables desde la ventana de preferencias

Clave	Tipo	Descripción
preferencesBlocked	true/false	Proteger cambios en preferencias. Un valor de true en esta preferencia indica que deben limitarse las opciones de configuración mediante interfaz gráfico, apareciendo de forma deshabilitada (solo para consulta). Un valor de false habilitará que cualquier opción de configuración pueda ser alterada por parte del usuario mediante el interfaz gráfico.
createHashAsBase64	true/false	Si está establecido a true (valor por defecto), se generan las huellas digitales de fichero en base64. Si es false, se generarán en binario.
createHashDirectoryAlgorithm	String	Algoritmo de huella digital por defecto para la creación de huellas digitales. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> • SHA1 • SHA-512 (Por defecto) • SHA-384 • SHA-256
updater.url.version	String	URL remota del fichero que define el código de versión de la versión

	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Autofirma 1.6JAv01 Manual de Gestión
---	--	---

		<p>más reciente de AutoFirma.</p> <p>Consulte el apartado “Comprobaciones de nuevas versiones al inicio de la aplicación” para más detalles.</p>
updater.url.site	String	<p>URL de la página web desde la que descargar las nuevas versiones de AutoFirma.</p> <p>Consulte el apartado “Comprobaciones de nuevas versiones al inicio de la aplicación” para más detalles.</p>

	<p>Consejería de Hacienda, Industria y Energía</p> <p>Dirección General de Transformación Digital</p>	<p>Autofirma 1.6JAv01</p> <p>Manual de Gestión</p>
---	---	--

7 Obtención de estadísticas con Google Analytics


AutoFirma utiliza Google Analytics para recoger información acerca de su uso. Esta información se limita al hecho de haber ejecutado AutoFirma y la IP del equipo. En ningún momento se recoge información personal del usuario u otra información del equipo más que la IP asignada.

A la información recabada sólo puede acceder el grupo de trabajo del Cliente @firma y este se compromete a que su uso se limita a conocer el número aproximado de usuarios de la herramienta.

La obtención de estos datos se realiza en segundo plano al ejecutarse AutoFirma y el resultado de su obtención y envío no afecta al uso de la propia herramienta. Así pues, AutoFirma podría no llegar a enviar los datos obtenidos, por ejemplo, por encontrarse detrás de un proxy de red, sin que esto afecte a su funcionalidad.

El usuario puede deshabilitar el envío de información a Google Analytics desde el panel de preferencias de la herramienta. También se puede configurar que deje de enviarse esta información por medio de la variable de entorno “es.gob.afirma.doNotSendAnalytics”. En caso de establecer esta variable a “true” se deshabilitará el envío de información. En caso contrario, se seguirá enviando.

En caso de configurarse la mencionada variable, no se enviará ninguna información a Google Analytics, independientemente de que el usuario haya configurado o no el envío de los datos a través del menú de preferencias de AutoFirma.

	Consejería de Hacienda, Industria y Energía Dirección General de Transformación Digital	Autofirma 1.6JAv01 Manual de Gestión
---	--	---

8 Error al importar las opciones de configuración desde un fichero

Si generase un fichero de configuración para la importación de las opciones de configuración en AutoFirma y al importarlo se mostrase el mensaje de error “El fichero de preferencias es inválido, no se realizará ningún cambio en la configuración”, es probable que el fichero utilizado no sea un XML válido o que tenga algún problema de codificación. Verifique que su fichero de configuración está bien formado y que la codificación utilizada es correcta.