Manual de instalación y gestión de AutoFirma 1.5

Índice de contenidos

[1 Introducción 4](#_Toc462848271)

[2 Requisitos mínimos 5](#_Toc462848272)

[2.1 Entorno Cliente 5](#_Toc462848273)

[2.1.1 AutoFirma 5](#_Toc462848274)

[3 Funcionamiento de AutoFirma 6](#_Toc462848275)

[4 Enlaces de descarga 6](#_Toc462848276)

[5 Instalación 6](#_Toc462848277)

[5.1 Microsoft Windows 7](#_Toc462848278)

[5.1.1 Desinstalación 11](#_Toc462848279)

[5.1.2 Despliegue masivo de la aplicación 13](#_Toc462848280)

[5.2 Linux 14](#_Toc462848281)

[5.2.1 Instalación por línea de comandos 14](#_Toc462848282)

[5.2.2 Instalación mediante el asistente de paquetes de Ubuntu/Guadalinex 15](#_Toc462848283)

[5.2.3 Desinstalación 16](#_Toc462848284)

[5.3 Apple OS X 16](#_Toc462848285)

[5.3.1 Desinstalación 16](#_Toc462848286)

[6 Gestión de AutoFirma 17](#_Toc462848287)

[6.1 Comprobaciones de nuevas versiones al inicio de la aplicación 17](#_Toc462848288)

[6.2 Configuración a través de fichero 18](#_Toc462848289)

[6.2.1 Opciones configurables 18](#_Toc462848290)

[6.2.2 Bloqueo de la configuración 26](#_Toc462848291)

[6.2.3 Firma del fichero de configuración 30](#_Toc462848292)

[6.2.4 Ejemplo de fichero de configuración 31](#_Toc462848293)

[6.3 Obtención de estadísticas con Google Analytics 31](#_Toc462848294)

[7 Compatibilidad del MiniApplet @firma con aplicaciones móviles y AutoFirma 32](#_Toc462848295)

[8 Problemas conocidos 32](#_Toc462848296)

[8.1 No se puede instalar AutoFirma no falla la instalación de los certificados de confianza SSL 32](#_Toc462848297)

[8.2 Al instalar AutoFirma en Windows se muestra el error: “Error abriendo archivo para escritura” 32](#_Toc462848298)

[8.3 Al abrir Google Chrome después del proceso de instalación de AutoFirma se muestra un mensaje notificando que la configuración de la aplicación está corrupta 33](#_Toc462848299)

[8.4 AutoFirma en OS X no muestra el título de los diálogos de cargar y guardado de ficheros 33](#_Toc462848300)

# 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 y 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 ejecutar las firmas de un trámite web.

**El presente documento se centra principalmente en el uso de AutoFirma para firmas web 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 con el JavaScript de despliegue del MiniApplet @firma. También permite el uso de dispositivos externos (tarjetas inteligentes, dispositivos USB) configurados en estos almacenes de claves (como por ejemplo, el DNI Electrónico o DNIe).

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 (EUPL 1.1) o superior.

Puede consultar la información relativa al proyecto Cliente @firma, dentro del cual se encuentra el AutoFirma y descargar el código fuente y los binarios de la aplicación en la siguiente dirección Web:

<http://administracionelectronica.gob.es/es/ctt/clienteafirma>

# Requisitos mínimos

## Entorno Cliente

### AutoFirma

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.
  + Apple OS X 10.11 o superior.
    - Soportado directamente en 10.11 y 10.11.1.
  + Linux
    - Guadalinex, Ubuntu.
* 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 (no se admiten los modos de compatibilidad con versiones anteriores, ni ninguna otra versión anterior).
    - Microsoft Edge v20.
  + Linux
    - Mozilla Firefox 41.0.1 o superior.
  + Apple OS X
    - Apple Safari 9.0 o superior.

En entornos OS X y Windows no es necesario que el usuario tenga instalado un entorno de ejecución de Java. En Linux se necesita un entorno de ejecución de Java de Oracle 8 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.

# Funcionamiento de AutoFirma

Cuando el entorno del ciudadano firmante no cuenta con un entorno de ejecución de Java instalado en su navegador Web para la ejecución de Applets de Java, 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*”.

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 subdirectorio oculto “*.afirma*” del directorio del usuario. Por ejemplo, “*C:\Users\miusuario\.afirma*”. 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.

# Enlaces de descarga

Para instar al usuario que se instale AutoFirma, rediríjalo a la siguiente página web:

<http://firmaelectronica.gob.es/Home/Descargas.html>

# Instalación

La instalación de AutoFirma en el sistema del usuario se asemeja a la instalación de cualquier otra aplicación. Sin embargo, el proceso de instalación incluye un paso de vital importancia para la compatibilidad del aplicativo con los despliegues MiniApplet para su uso en trámites web.

La comunicación entre la página web y AutoFirma se realiza cuando es posible a través de un socket SSL a través del cual la información viaja siempre cifrada mediante la clave privada de un certificado generado durante el proceso de instalación. Para que sea posible la comunicación entre el navegador web y AutoFirma, será necesario que durante la instalación se genere el par de claves con el que se realizará la comunicación, que este se almacene en disco y que el certificado generado sea dado de alta en los almacenes de confianza de los navegadores del sistema. Debido a las medidas de seguridad establecidas por cada navegador web, es posible que esto implique la aparición de un diálogo gráfico de seguridad en el que se debe conceder permisos para realizar esta operación.

El proceso de instalación y configuración de AutoFirma registra el resultado de la operativa de generación del par de claves y su instalación en los almacenes de confianza del sistema. Este fichero se almacena por defecto en el directorio “*.afirma*” dentro del directorio de usuario del usuario que instaló la aplicación. El nombre del fichero de trazas es “*AUTOFIRMA\_CONFIGURATOR.afirma.log.xml*”.

En el caso de Linux y OS X, la instalación se realiza con el usuario administrador y el log se guarda en el directorio temporal del sistema o, si no se puede ahí, en “*/var/tmp*“ para facilitar su acceso.

## Microsoft Windows

La instalación de AutoFirma en Windows requiere que un usuario con permisos de administrador ejecute la aplicación de instalación. Esta aplicación de instalación se distribuye con el nombre “AutoFirma\_X.Y.Z\_W.exe”, donde X, Y y Z son los números de versión y W, la arquitectura de sistema para la que está preparada. Por ejemplo, “AutoFirma\_1.5.0\_32.exe”, se correspondería con AutoFirma, versión 1.5.0 para sistema de 32bits.

AutoFirma es compatible con Windows 7 o superior en 32 y 64 bits (x86 o x64). Una vez instalada, puede usarse desde prácticamente cualquier navegador Web. Los navegadores oficialmente soportados son:

* Microsoft Internet Explorer 11
* Google Chrome 46 o superior
* Mozilla Firefox 41.0.2 o superior
* Microsoft Edge v20:

AutoFirma puede funcionar correctamente con otros navegadores (Apple Safari, Opera, etc.), pero no se ofrece soporte sobre ellos.

AutoFirma se distribuye en versiones de 32 y 64 bits para Windows. Esta diferenciación afecta únicamente a la cantidad de recursos del sistema que la aplicación es capaz de utilizar. Si se desea utilizar AutoFirma para la generación de firmas de ficheros grandes, se deberá usar la versión de 64 bits de AutoFirma.

La instalación es un sencillo asistente con los siguientes pasos:





En este punto el usuario debe aceptar el acuerdo de licencia de la aplicación.



El usuario puede en este paso cambiar el directorio de instalación por defecto.



El proceso de instalación extrae y copia los ficheros necesarios.





Cuando el asistente termina, la instalación ha finalizado, y las aplicaciones Web configuradas para el MiniApplet Cliente @firma podrán funcionar también con AutoFirma en ausencia de un entorno de ejecución de Java en el navegador.

### Desinstalación

La desinstalación del programa puede hacerse, como es habitual en Windows, desde el apartado “Programas y características” del “Panel de control” del sistema operativo (siempre por parte de un usuario con permisos de administrador):



Una vez lanzado, el desinstalador presenta un sencillo asistente:







El desinstalador muestra el proceso de desinstalación de la aplicación.

**ADVERTENCIA**: El proceso de desinstalación afecta a los perfiles de Mozilla Firefox y a la configuración de Google Chrome. Estos navegadores se cerrarán automáticamente durante el proceso de desinstalación.

Cuando el proceso termina, la aplicación habrá sido desinstalada de Windows.



### Despliegue masivo de la aplicación

AutoFirma también se distribuye en forma de instalador MSI (32 y 64bits) orientado a su despliegue masivo por parte de un administrador que gestione las aplicaciones de un conjunto de usuarios.

El instalador MSI realiza la instalación silenciosa en el equipo de los usuarios. El administrador debe asegurarse, en cualquier caso, de que el proceso de instalación no se realiza mientras los usuarios trabajan en sus equipos, ya que los navegadores Chrome y Firefox se cerrarán durante la instalación/desinstalación tal como ocurre con el instalador EXE.

Consulte el manual de su software de instalación masiva de aplicaciones para saber cómo realizar el despliegue.

## Linux

La instalación de AutoFirma en Linux debe ser realizada por un usuario con permisos de administrador. El archivo e instalación de la aplicación se distribuye con el nombre “AutoFirma\_X.Y.Z.deb”, donde X, Y y Z (opcional) son los números de versión. Por ejemplo “AutoFirma\_1.5.deb” correspondería a AutoFirma versión 1.5.

Para poder ejecutar AutoFirma son necesarias las siguientes dependencias, así que estás se comprueban durante el proceso de instalación:

* JRE (Java Runtine Environment) de Oracle u OpenJDK.
* Biblioteca “libnss3-tools”.

AutoFirma es compatible con Ubuntu y Guadalinex 32 y 64 bits. Una vez instalada, puede usarse con los navegadores web Mozilla Firefox y Google Chrome.

Hay dos opciones de instalación: por línea de comandos y desde la interfaz de escritorio.

La instalación por ambos medios dejará la aplicación instalada por defecto en el directorio:

/usr/lib/AutoFirma

### Instalación por línea de comandos

Para instalación por línea de comandos, en una consola ejecutaremos:

sudo dpkg –i RUTA\_INSTALABLE\_AUTOFIRMA

Donde RUTA\_INSTALABLE\_AUTOFIRMA es la ruta al instalador en función de la distribución escogida.

Si no tenemos instaladas las dependencias anteriormente listadas, se nos mostrarán mensajes de advertencia al respecto. En caso de ser así, podremos instalar estas bibliotecas con el comando:

sudo apt-get –f install

Después de esto, se debe volver a ejecutar el comando de instalación de AutoFirma para asegurar su correcta instalación:

sudo dpkg –i RUTA\_INSTALABLE\_AUTOFIRMA

### Instalación mediante el asistente de paquetes de Ubuntu/Guadalinex

Para la instalación mediante el asistente de paquetes, se debe hacer doble clic en el fichero de la distribución (.deb). Se abrirá una ventana similar a la siguiente.



Se debe pulsar el botón instalar, que se encuentra arriba a la derecha. Si no se tienen permisos de administración, el sistema solicitará la clave de “súper usuario” para poder realizar la instalación.



Si no ha ocurrido ningún problema, se mostrará un mensaje de confirmación.



### Desinstalación

Para realizar la desinstalación del sistema se deberá escribir por consola en línea de comandos el siguiente comando.

sudo apt-get remove –-purge autofirma

Cuando el proceso termina, la aplicación ha sido correctamente desinstalada del sistema.

## Apple OS X

La instalación de AutoFirma en OS X debe realizarla un usuario con permisos de administrador. El archivo de instalación se distribuye con el nombre “AutoFirma\_X.Y.Z.pkg”, donde X, Y y Z (opcional) son los números de la versión. Por ejemplo, “AutoFirma\_1.5.pkg” correspondería a AutoFirma versión 1.5.

AutoFirma es compatible con las versiones de OS X Mavericks, Yosemite y El Capitán. Los navegadores compatibles son Apple Safari, Google Chrome y Mozilla Firefox.

Para la instalación de la aplicación, se debe hacer doble clic sobre el fichero. El sistema abrirá un asistente que se encargará de realizar los pasos a seguir para la correcta instalación de la aplicación.

### Desinstalación

Para desinstalar la aplicación basta con eliminar la carpeta que se generó en el directorio /Applications.

# Gestión de AutoFirma

## Comprobaciones de nuevas versiones al inicio de la aplicación

Al arrancar, AutoFirma comprueba siempre si hay una versión más actual disponible para descarga desde la página Web del proyecto, con el objeto de que no se realicen trámites de firma con una versión obsoleta o antigua que pudiese tener instalada el ciudadano.

Es posible deshabilitar esta comprobación 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.

Esta inhabilitación de las comprobaciones de actualización debe hacerse únicamente en entornos controlados (corporativos, internos a una administración, etc.), ya que es siempre conveniente descargar e instalar las últimas versiones disponibles.

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



La URL a la que se conecta AutoFirma para comprobar la existencia de actualizaciones es:

<http://estaticos.redsara.es/comunes/autofirma/autofirma.version>

El administrador de red debe asegurar que los equipos de los usuarios tienen acceso a esta URL si se desea que sean los propios usuarios los encargados de identificar las nuevas versiones e instalarlas en sus equipos.

## Configuración a través de fichero

AutoFirma v1.5 y superiores 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 al 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 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.

### Opciones configurables

Las opciones de configuración que se pueden establecer mediante fichero 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.

#### Opciones Generales

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Clave** | **Tipo** | | **Descripción** | |
| **omitAskOnClose** | true/false | | Evita la confirmación al cerrar la aplicación o no. Un valor de true en esta preferencia permitirá cerrar la aplicación sin ningún diálogo de advertencia. Un valor de false (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 DNIe. Un valor de true en esta preferencia hace que nunca se muestre la pantalla inicial que sugiere al usuario el uso directo del DNIe como almacén de claves. Un valor de false (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 | | Algoritmo de firma. Esta preferencia debe tener uno de estos valores:   * SHA1withRSA * SHA256withRSA (Por defecto) * SHA384withRSA * SHA512withRSA | |
| **defaultSignatureFormatPdf** | String | | Formato en el que se firmarán los documentos PDF. Esta preferencia debe tener uno de estos valores:   * PAdES (Por defecto) * CAdES * XAdES | |
| **defaultSignatureFormatOoxml** | String | | Formato en el que se firmarán los documentos OOXML. Esta preferencia debe tener uno de estos valores:   * OOXML (Office Open XML) (Por defecto) * CAdES * XAdES | |
| **defaultSignatureFormatFacturae** | String | | Formato en el que se firmarán las facturas electrónicas. Esta preferencia debe tener uno de estos valores:   * FacturaE (Por defecto) * CAdES * XAdES | |
| **defaultSignatureFormatXml** | String | | Formato en el que se firmarán los documentos XML. Esta preferencia debe tener uno de estos valores:   * XAdES (Por defecto) * CAdES | |
| **defaultSignatureFormatOdf** | String | | Formato en el que se firmarán los documentos ODF (LibreOffice, OpenOffice.org…). Esta preferencia debe tener uno de estos valores:   * ODF (Open Document Format) (Por defecto) * CAdES * XAdES | |
| **defaultSignatureFormatBin** | String | | Formato en el que se firmarán los ficheros binarios. Esta preferencia debe tener uno de estos valores:   * CAdES (Por defecto) * XAdES | |
| **proxySelected** | | true/false | | 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. | |
| **proxyHost** | | String | | URL del servicio del servidor proxy. | |
| **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. | |

#### 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:   * 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 | Formato de firma PAdES. Esta preferencia debe tener uno de estos valores:   * 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), por defecto se realizarán firmas invisibles PDF. |

#### 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 | Algoritmo de la huella digital del identificador de la política de firma para CAdES. Esta preferencia debe tener uno de estos valores:   * SHA1 (Por defecto) * SHA-512 * SHA-384 * SHA-256 |
| **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*). |

#### 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:   * 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. |
| **xadesSignerClaimedRole** | String | Cargo supuesto para el firmante. |
| **xadesSignFormat** | String | Formato de las firmas XAdES. Esta preferencia debe tener uno de estos valores:   * XAdES Detached * XAdES Enveloping (Por defecto) * XAdES Enveloped |

#### Firmas Factura Electrónica

|  |  |  |
| --- | --- | --- |
| **Clave** | **Tipo** | **Descripción** |
| **facturaEPolicy** | String | Versión de la política de firma de factura electrónica. Los valores posibles son:   * 3.0: Policita de firma 3.0. * 3.1: Policita de firma 3.1 (por defecto).   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 |
| **facturaePolicyIdentifier** | String | Establece el identificador de la política de firma de factura electrónica.  Para configurar la política de firma 3.0 se debe establecer el valor: http://www.facturae.es/politica de firma formato facturae/politica de firma formato facturae v3\_0.pdf  Para configurar la política de firma 3.0 se debe establecer el valor: http://www.facturae.es/politica\_  de\_firma\_formato\_facturae/  politica\_de\_firma\_formato\_  facturae\_v3\_1.pdf |
| **facturaePolicyIdentifierHash** | String | Establece la huella digital de la política de firma de factura electrónica.  Para configurar la política de firma 3.0 se debe establecer el valor: xmfh8D/Ec/hHeE1IB4zPd61zHIY=  Para configurar la política de firma 3.0 se debe establecer el valor: Ohixl6upD6av8N7pEvDABhEL6hM= |
| **facturaePolicyIdentifierHashAlgorithm** | String | Establece el identificador de la política de firma de factura electrónica.  Para configurar las políticas de firma 3.0 y 3.1 se debe establecer el valor: SHA1 |
| **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:   * Emisor (Por defecto) * Receptor * Tercero |

#### Opciones no configurables desde la ventana de preferencias

|  |  |  |
| --- | --- | --- |
| **Clave** | **Tipo** | **Descripción** |
| **preferencesUnprotected** | 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, 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:   * SHA1 * SHA-512 (Por defecto) * SHA-384 * SHA-256 |

### 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 se 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.

La configuración de la aplicación puede bloquearse por medio de la opción “preferencesUnprotected”, como se describe en el apartado “6.2.1.6 Opciones no configurables desde la ventana de preferencias”.

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 DNIe 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



**Pestaña Firmas PAdES**

* Metadatos para firmas PAdES
* Firma visible



**Pestaña Firmas XAdES**

* Metadatos de las firmas XAdES

**Pestaña Factura electrónica**

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



### 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.

### 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>cadesImplicitMode</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 (cadesImplicitMode) 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.

## 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.

A partir de la versión 1.5 de AutoFirma, el usuario puede deshabilitar el envío de información 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.

# Compatibilidad del MiniApplet @firma con aplicaciones móviles y AutoFirma

El MiniApplet @firma 1.5 es compatible con:

* AutoFirma v1.5 y superiores.
* Cliente @firma móvil Android v1.5
* Cliente @firma móvil iOS v1.5

# Problemas conocidos

## No se puede instalar AutoFirma no falla la instalación de los certificados de confianza SSL

AutoFirma requiere permisos de administrador para ser instalado y para insertar el certificado de confianza SSL para el funcionamiento de la firma en los trámites online. Si no puede instalar AutoFirma o el certificado de confianza, solicite al administrador de su sistema que realice la instalación de la aplicación.

## Al instalar AutoFirma en Windows se muestra el error: “Error abriendo archivo para escritura”

Es posible que durante la instalación se le muestre un error como el que sigue:



Si ya tenía instalado AutoFirma, compruebe que este no se está ejecutando, en cuyo caso el instalador no podrá sobrescribir los ficheros de instalación. Cierre AutoFirma y pulse el botón reintentar.

Si AutoFirma no se está ejecutando, es posible que el archivo en cuestión se encuentre bloqueado por una ejecución o intento de instalación previo. Reinicie su equipo y pruebe a instalar nuevamente la aplicación.

## Al abrir Google Chrome después del proceso de instalación de AutoFirma se muestra un mensaje notificando que la configuración de la aplicación está corrupta

El navegador Google Chrome incluye en su configuración un listado de protocolos que considera seguros para la llamada a aplicaciones externas. Durante el proceso de instalación de AutoFirma, se registra el protocolo “afirma” en este listado seguro de Chrome para que las invocaciones desde el navegador se realicen correctamente. Para hacer este registro el propio proceso de instalación cierra la aplicación y agrega el protocolo al listado correspondiente.

En algunas situaciones en las que el instalador podría no poder completar el proceso de registro, el fichero de configuración de Chrome podría quedar en un estado inconsistente. En estos casos, al iniciarse de nuevo el navegador, detectará el problema y anunciará al usuario esta corrupción de datos mediante una ventana de advertencia que nos permitirá restaurar las propiedades por defecto.

Seguidamente, el navegador restaurará las propiedades configuración y volverá a funcionar normalmente. En este caso, el usuario recibirá mensajes de advertencia al usar AutoFirma desde Chrome para realizar firmas, aunque esto no impedirá que funcione normalmente.

Durante el proceso de desinstalación de AutoFirma se realiza el proceso inverso al de instalación y se elimina el protocolo “afirma” del listado de protocolos seguros registrados en Chrome. Este proceso podría derivar en algunas circunstancias a la misma corrupción de la configuración del navegador.

## AutoFirma en OS X no muestra el título de los diálogos de cargar y guardado de ficheros

Las nuevas versiones de OS X omiten el título de los diálogos de carga y guardado de ficheros. En caso en que el integrador delegue en AutoFirma la selección y el guardado de las firmas generadas, debería tener la precaución de informar al usuario de esto para que en todo momento sepa que operación está realizando (carga de un fichero de datos para firma, carga de un fichero de firma para cofirma/contrafirma, guardado de una firma generada…).

[Creative Commons License](#Licencia_Creative_Commons)

Esta obra está bajo una licencia [Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0 Unported](#Licencia_Creative_Commons).