# Configuración a través de fichero

AutoFirma puede configurarse 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 deberá estar firmado con una firma en formato XAdES Enveloped. El certificado utilizado para la firma deberá haber sido emitido por la autoridad habilitada internamente en la aplicación.

## 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** |
| **showIcon** | true/false | Configura si debe cargarse la aplicación al inicio de Windows y dejar un icono en la bandeja del sistema. |
| **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. |
| **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. |
| **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. |
| **padesCertificationLevel** | String | Nivel de certificación que debe aplicarse al PDF. Los valores permitidos son:   * 0: Firma ordinaria. * 3: Firma certificada. El PDF firmado no podrá ser modificado ni firmado en el futuro. |
| **isTimeStampConfiguredPades** | true/false | Habilita la estampación de un sello de tiempo en las firmas PAdES generadas. Por defecto, esta propiedad está configurada a false (no se agregará sello de tiempo a las firmas). |
| **tsType** | String | Tipo de sello de tiempo a estampar. Los valores posibles son:   * 1: Sello de tiempo a nivel de firma (Por defecto). * 2: Sello de tiempo a nivel de documento. * 3: Sello de tiempo tanto a nivel de firma como de documento. |
| **tsaHashAlgorithmsPades** | String | Algoritmo de huella del sello de tiempo. Los valores admitidos son: SHA-1, SHA-256, SHA-384 y SHA-512. |
| **tsaUrlPades** | String | URL de la autoridad de sellado de tiempo. |
| **tsaPolicyPades** | String | OID de la política del servicio de sellado de tiempo. |
| **tsaUsrPades** | String | Usuario de acceso al servicio de sello de tiempo. |
| **tsaPwdPades** | String | Contraseña de acceso al servicio de sello de tiempo. |
| **tsaExtensionOidPades** | String | OID de la extensión a añadir a la petición al servidor de sello de tiempo. |
| **tsaExtensionValueBase64Pades** | String | Valor, en binario convertido a Base64, de la extensión a añadir a la petición de sello de tiempo. |
| **isCertRequiredPades** | true/false | Indica si se requiere el envío del certificado al servidor de sello de tiempo. |
| **isExtensionCriticalPades** | true/false | Indica si el OK de la extensión indicada anteriormente (tsaExtensionOidPades) es crítica. |

### 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*). |
| **isTimeStampConfiguredCades** | true/false | Habilita la estampación de un sello de tiempo en las firmas PAdES generadas. Por defecto, esta propiedad está configurada a false (no se agregará sello de tiempo a las firmas). |
| **tsaHashAlgorithmsCades** | String | Algoritmo de huella del sello de tiempo. Los valores admitidos son: SHA-1, SHA-256, SHA-384 y SHA-512. |
| **tsaUrlCades** | String | URL de la autoridad de sellado de tiempo. |
| **tsaPolicyCades** | String | OID de la política del servicio de sellado de tiempo. |
| **tsaUsrCades** | String | Usuario de acceso al servicio de sello de tiempo. |
| **tsaPwdCades** | String | Contraseña de acceso al servicio de sello de tiempo. |
| **tsaExtensionOidCades** | String | OID de la extensión a añadir a la petición al servidor de sello de tiempo. |
| **tsaExtensionValueBase64Cades** | String | Valor, en binario convertido a Base64, de la extensión a añadir a la petición de sello de tiempo. |
| **isCertRequiredCades** | true/false | Indica si se requiere el envío del certificado al servidor de sello de tiempo. |
| **isExtensionCriticalCades** | true/false | Indica si el OK de la extensión indicada anteriormente (tsaExtensionOidCades) es crítica. |

### 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 0de 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. |
| **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 |

### Almacenes de claves

|  |  |  |
| --- | --- | --- |
| **Clave** | **Tipo** | **Descripción** |
| **useOnlySignatureCertificates** | true/false | Configura que en el diálogo de selección de certificados sólo se muestren los certificados habilitados para firma (*keyusage nonrepudiation*) cuando se vaya a realizar una firma electrónica con él. Por defecto, true. |
| **useOnlyAliasCertificates** | true/false | Configura que en el diálogo de selección de certificados sólo se muestren los certificados de seudónimo. Por defecto, false. |
| **useOnlyAcceptedPoliciesCertificate** | true/false | Indica si deben aplicarse filtros de certificado en base a directivas de certificado. Los OID de las directivas admitidas se configuran a través de la propiedad “acceptedCertPoliciesList”. |
| **acceptedCertPoliciesList** | String | Directivas de políticas de certificado admitidas. Este valor establece todas las políticas admitidas, para lo cual se le debe establecer como valor una cadena con los OID de políticas separados por el carácter punto y coma (‘;’). |
| **prioritaryStore** | String | Almacén de claves prioritario. Es el almacén extraíble que se intentará cargar al inicio de la aplicación. Los valores posibles son:   * Ninguno * DNIe y tarjetas FNMT-TIF * Tarjeta FNMT-RCM CERES * TEMD (Tarjeta del Ministerio de Defensa) |
| **closeKeyStore** | true/false | Configura si debe cerrarse o no el almacén de claves prioritario. Este valor sólo aplica cuando el almacén de claves prioritario es la tarjeta del Ministerio de defensa. El tiempo que debe transcurrir hasta el cierre es el indicado en la propiedad “closeKeyStoreTimeout”. |
| **closeKeyStoreTimeout** | String | Tiempo en minutos que deben transcurrir hasta que el almacén se cierre auténticamente. Si el tiempo es 0, siempre se cerrará. |
| **defaultStore** | String | Almacén de claves por defecto. Es el almacén que se carga cuando no se encuentra el almacén prioritario. Los valores posibles son:   * Windows / Internet Explorer * Mac OS X / Safari * Mozilla / Firefox (unificado) * NSS   Estos almacenes sólo podrán configurarse cuando estén disponibles en el sistema. Por ejemplo, en Windows no se podrá cargar el almacén de OS X. |

### 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

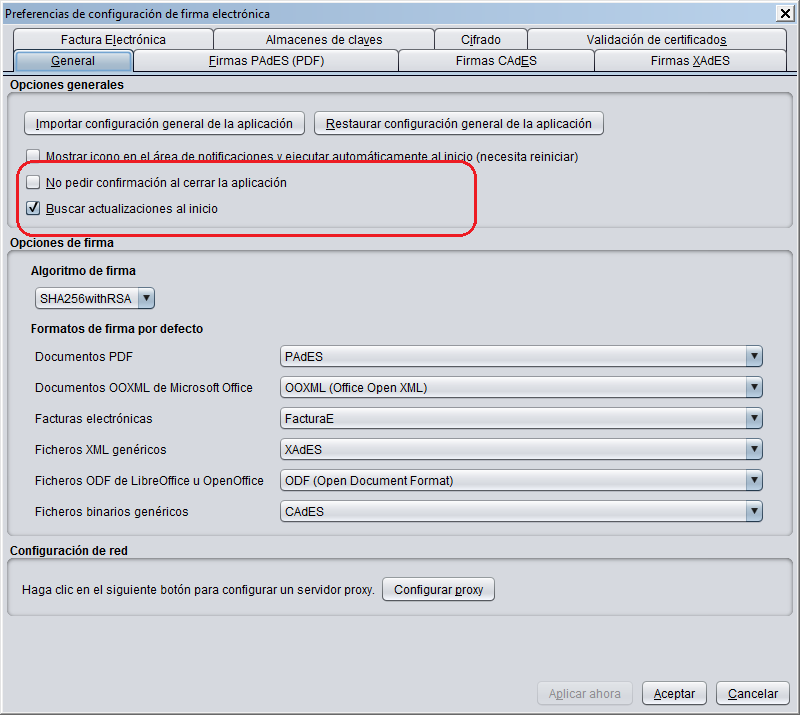
Un uso interesante de la configuración de la aplicación entre los usuarios de un organismo o entidad es que permite bloquear las opciones que el usuario va a poder modificar. Hay opciones que se son especialmente interesantes de fijar para que se apliquen a todas las firmas, como las políticas de firma, 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 “1.1.6 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:

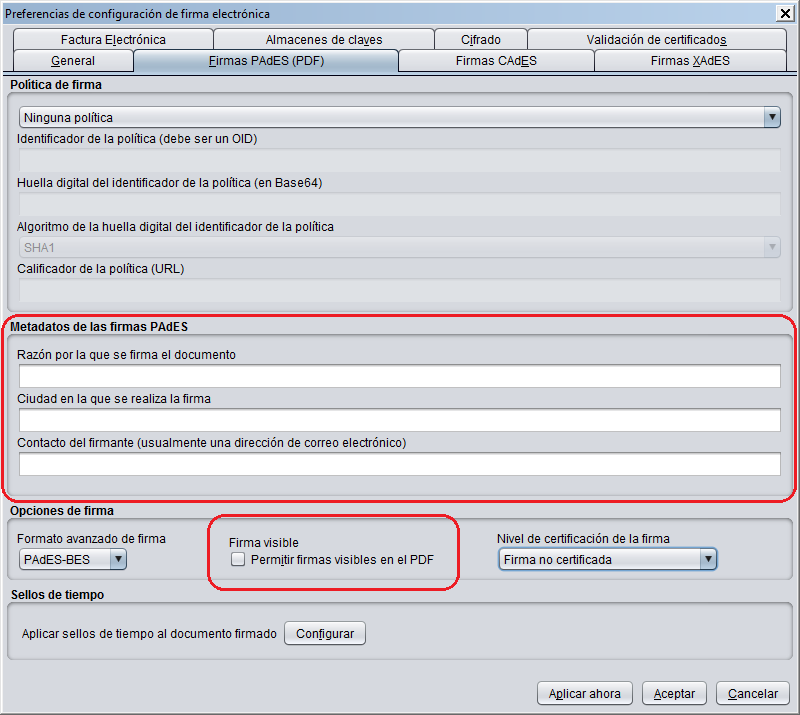
**Pestaña General**

* No pedir confirmación al cerrar la aplicación
* Buscar actualizaciones al inicio



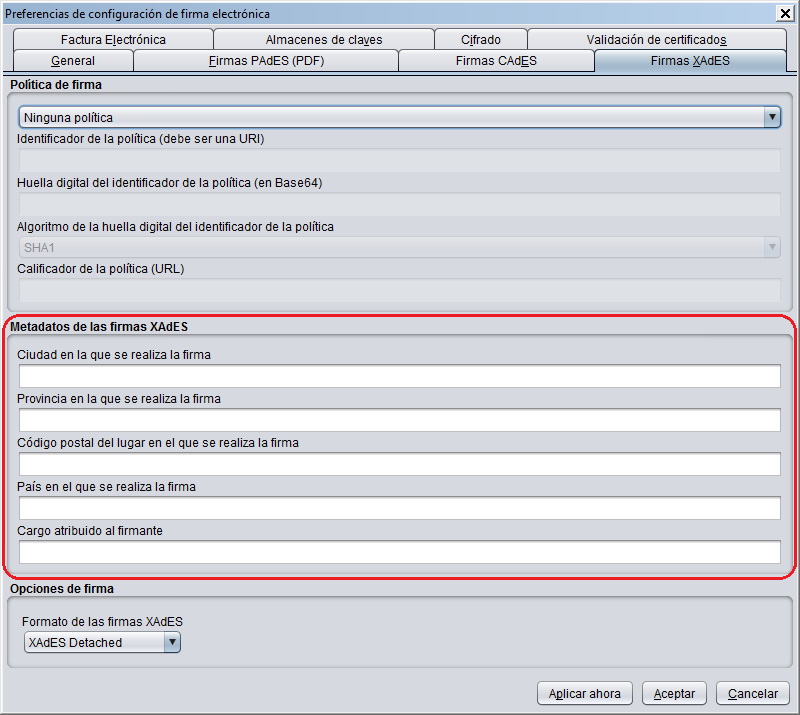
**Pestaña Firmas PAdES**

* Metadatos para firmas PAdES
* Firma visible



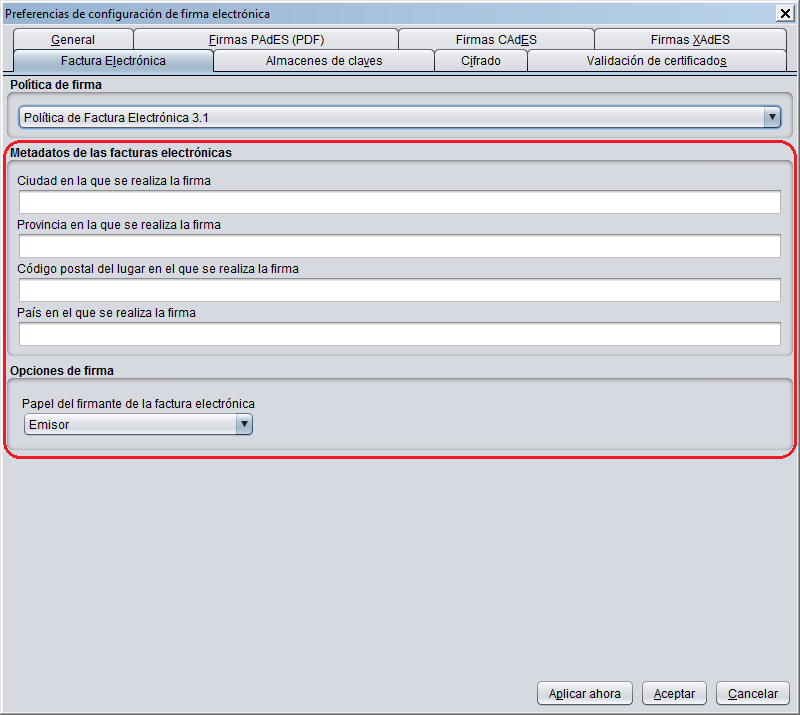
**Pestaña Firmas XAdES**

* Metadatos de las firmas XAdES



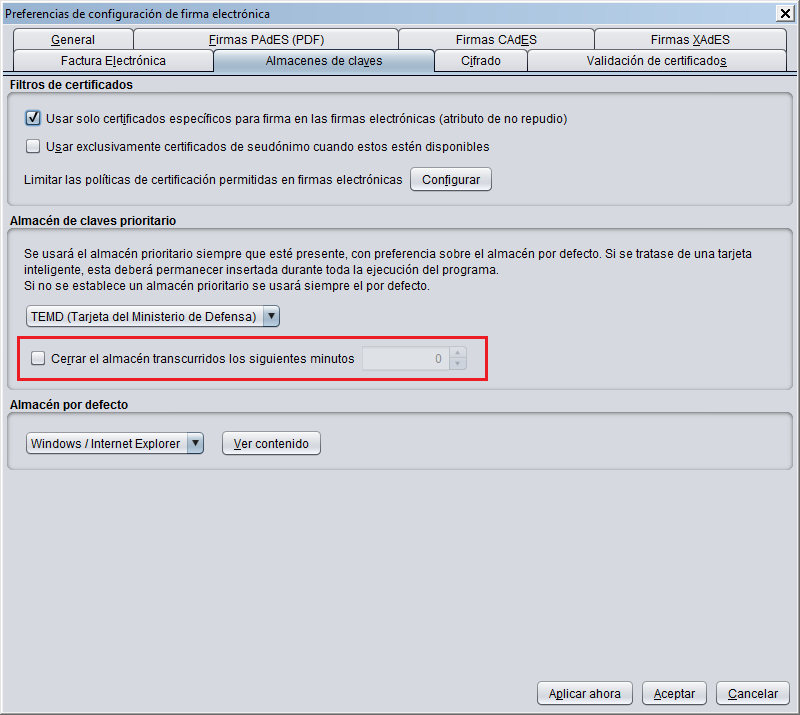
**Pestaña Factura electrónica**

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



**Pestaña Almacenes de claves**

* Cerrar el almacén transcurridos los siguientes minutos



## 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.