Manual para la configuración de los campos de firma para cada operación realizada en la aplicación de firma manuscrita en tableta.

Contenido

[1. Introducción 5](#_Toc406692216)

[2. Configuración fichero de firma 5](#_Toc406692217)

[2.1. Datos del CSV 6](#_Toc406692218)

[2.1.1. Página del CSV 6](#_Toc406692219)

[2.1.2. Texto 6](#_Toc406692220)

[2.1.3. Rotación 6](#_Toc406692221)

[2.1.4. Posición 6](#_Toc406692222)

[2.1.5. Tamaño de la fuente del texto 6](#_Toc406692223)

[2.2. Datos para el sellado de tiempo 7](#_Toc406692224)

[2.2.1. Certificado de TSA 7](#_Toc406692225)

[2.2.2. Autoridad de sellado de tiempo 7](#_Toc406692226)

[2.2.3. Algoritmo de huella digital 7](#_Toc406692227)

[2.2.4. Política de sellado 8](#_Toc406692228)

[2.2.5. Usuario de la TSA 8](#_Toc406692229)

[2.2.6. Certificado SSL cliente 8](#_Toc406692230)

[2.3. Datos del documento a firmar 9](#_Toc406692231)

[2.3.1. Directorio del documento 9](#_Toc406692232)

[2.3.2. Dirección URL para guardar el documento firmado 9](#_Toc406692233)

[2.3.3. Identificador del documento 9](#_Toc406692234)

[2.3.4. Directorio para guardar el documento firmado 9](#_Toc406692235)

[2.3.5. Nombre del documento firmado 10](#_Toc406692236)

[2.3.6. Directorio para ficheros temporales 10](#_Toc406692237)

[2.3.7. Certificado 10](#_Toc406692238)

[2.3.8. Mostrar botones en la tableta de firma 10](#_Toc406692239)

[2.4. Datos de los firmantes 11](#_Toc406692240)

[2.4.1. Datos personales 11](#_Toc406692241)

[2.4.2. Plantilla de firma 12](#_Toc406692242)

[2.4.3. Área de firma 12](#_Toc406692243)

[2.4.4. Área de firma en el documento 13](#_Toc406692244)

[2.4.5. Página de firma 13](#_Toc406692245)

[2.5. Firma adicional 14](#_Toc406692246)

[2.5.1. Firma con parámetros adicionales 14](#_Toc406692247)

[2.5.2. Firma con almacén PKCS12 14](#_Toc406692248)

[3. Plantilla de configuración 15](#_Toc406692249)

[4. Anexo 17](#_Toc406692250)

[4.1. Listado de parámetros adicionales 17](#_Toc406692251)

[4.1.1. allowCosigningUnregisteredSignatures 17](#_Toc406692252)

[4.1.2. *includeOnlySignningCertificate* 17](#_Toc406692253)

[4.1.3. alwaysCreateRevision 17](#_Toc406692254)

[4.1.4. image 17](#_Toc406692255)

[4.1.5. imagePage 17](#_Toc406692256)

[4.1.6. imagePositionOnPageLowerLeftX 18](#_Toc406692257)

[4.1.7. imagePositionOnPageLowerLeftY 18](#_Toc406692258)

[4.1.8. imagePositionOnPageUpperRightX 18](#_Toc406692259)

[4.1.9. imagePositionOnPageUpperRightY 18](#_Toc406692260)

[4.1.10. attach 18](#_Toc406692261)

[4.1.11. attachFileName 18](#_Toc406692262)

[4.1.12. attachDescription 19](#_Toc406692263)

[4.1.13. certificationLevel 19](#_Toc406692264)

[4.1.14. signatureSubFilter 19](#_Toc406692265)

[4.1.15. signatureField 19](#_Toc406692266)

[4.1.16. signaturePage 19](#_Toc406692267)

[4.1.17. signaturePositionOnPageLowerLeftX 19](#_Toc406692268)

[4.1.18. signaturePositionOnPageLowerLeftY 20](#_Toc406692269)

[4.1.19. signaturePositionOnPageUpperRightX 20](#_Toc406692270)

[4.1.20. signaturePositionOnPageUpperRightY 20](#_Toc406692271)

[4.1.21. signatureRubricImage 20](#_Toc406692272)

[4.1.22. layer2Text 20](#_Toc406692273)

[4.1.23. layer2FontFamily 21](#_Toc406692274)

[4.1.24. layer2FontSize 21](#_Toc406692275)

[4.1.25. layer2FontStyle 21](#_Toc406692276)

[4.1.26. layer2FontColor 21](#_Toc406692277)

[4.1.27. signReason 22](#_Toc406692278)

[4.1.28. signatureProductionCity 22](#_Toc406692279)

[4.1.29. signerContact 22](#_Toc406692280)

[4.1.30. policyIdentifier 22](#_Toc406692281)

[4.1.31. policyIdentifierHash 22](#_Toc406692282)

[4.1.32. policyIdentifierHashAlgorithm 22](#_Toc406692283)

[4.1.33. policyQualifier 22](#_Toc406692284)

[4.1.34. ownerPassword 22](#_Toc406692285)

[4.1.35. headLess 22](#_Toc406692286)

[4.1.36. avoidEncryptingSignedPdfs 23](#_Toc406692287)

[4.1.37. allowSigningCertifiedPdfs 23](#_Toc406692288)

[4.1.38. tsType 23](#_Toc406692289)

[4.1.39. tsaURL 23](#_Toc406692290)

[4.1.40. tsaPolicy 23](#_Toc406692291)

[4.1.41. tsaHashAlgorithm 23](#_Toc406692292)

[4.1.42. tsaRequireCert 23](#_Toc406692293)

[4.1.43. tsaUsr 23](#_Toc406692294)

[4.1.44. tsaPwd 23](#_Toc406692295)

[4.1.45. tsaSslPkcs12File 24](#_Toc406692296)

[4.1.46. tsaSslPkcs12FilePassword 24](#_Toc406692297)

[4.1.47. signingCertificateV2 24](#_Toc406692298)

[5. Ejemplo 25](#_Toc406692299)

# Introducción

La aplicación de firma manuscrita en tableta ha sido diseñada para agilizar el trámite de firma presencial de documentos. Esta implementada en forma de Applet de Java y recibe como parámetros de configuración un fichero XML.

En este fichero se deben incluir los datos necesarios para llevar a cabo la operación de firma y el almacenamiento del documento una vez haya sido firmado.

A continuación, se especifica cómo se debe definir los datos de los firmantes, la ubicación del espacio de firma en la tableta, el espacio de firma en el documento a firmar y, si fuera necesario, la firma adicional del documento por parte de una tercera entidad, como por ejemplo, un funcionario.

# Configuración fichero de firma

Como se ha comentado, se requiere la configuración de un fichero XML de firma donde se especifiquen los datos del trámite. En caso de que no se desee incluir alguno de los datos descritos, se debe dejar la etiqueta vacía, pero en ningún caso suprimirla.

Los siguientes puntos de este documento definen los tipos de datos que son necesarios especificar en el fichero XML:

* Datos del código seguro de verificación (CSV).
* Datos para el sellado de tiempo.
* Datos del documento a firmar.
* Datos de los firmantes.
* Firma adicional.

## Datos del CSV

En las primeras líneas del documento XML se describe un código de seguridad de verificación (CSV), opcional, que debe contener las etiquetas descritas a continuación.

Estructura XML que describe un CSV para esta aplicación:

<CSV>

<page></page>

<text></text>

<rotation></rotation>

<positionOnPageLowerLeftX></positionOnPageLowerLeftX>

<positionOnPageLowerLeftY></positionOnPageLowerLeftY>

<positionOnPageUpperRightX></positionOnPageUpperRightX>

<positionOnPageUpperRightY></positionOnPageUpperRightY>

<fontSize></fontSize>

</CSV>

### Página del CSV

Descripción: Indicar en un número entero la página del documento a firmar en el que situar el código CSV.

Etiqueta: page.

### Texto

Descripción: Introducir el contenido del CSV, una secuencia de caracteres.

Etiqueta: text.

### Rotación

Descripción: Posición en la que debe aparecer el texto; se define como un número entero entre 0 y 360, dependiendo del grado de rotación con el que se quiera que el código se dibuje en el documento firmado.

Etiqueta: rotation

### Posición

Descripción: Posición en la que se sitúa el CSV, es decir, las coordenadas en las que se debe situar el texto dentro del documento.

Etiqueta: positionOnPageLowerLeftX, positionOnPageLowerLeftY, positionOnPageUpperRightX, positionOnPageUpperRightY.

### Tamaño de la fuente del texto

Descripción: Definir el tamaño del texto que se imprime en el documento firmado.

Etiqueta: fontSize.

## Datos para el sellado de tiempo

Con el objetivo de poder garantizar que el documento firmado no se ha modificado desde el momento en el que se generó la firma se solicita a la Autoridad de Sellado de Tiempo (TSA) que genere un sello de tiempo con la información del documento firmado, la fecha y hora y un certificado electrónico de confianza.

En esta sección se describen los parámetros de sellado de tiempo que responden a la siguiente estructura XML:

<tsaParams>

<tsaRequireCert></tsaRequireCert>

<tsaPolicy></tsaPolicy>

<tsaURL></tsaURL>

<tsaUsr></tsaUsr>

<tsaPwd></tsaPwd>

<extensions>

<extension>

<oid></oid>

<critical></critical>

<value></value>

</extension>

</extensions>

<tsaHashAlgorithm></tsaHashAlgorithm>

<sslPkcs12File></sslPkcs12File>

<sslPkcs12FilePassword></sslPkcs12FilePassword>

</tsaParams>

### Certificado de TSA

Descripción: Indicar con un booleano – true o false – si se requiere el certificado de la Autoridad de Sellado de Tiempo. En caso de que no se establezca, se considera que no se requiere certificado.

Etiqueta: tsaRequireCert

### Autoridad de sellado de tiempo

Descripción: URL de la autoridad de sello de tiempo, en caso de que no se indique, no se añade el sello de tiempo.

Etiqueta: tsaURL

### Algoritmo de huella digital

Descripción: Algoritmo de huella digital para el cifrado de la huella. E n caso de que no se establezca se toma por defecto el algoritmo SHA-1.

Etiqueta: tsaHashAlgorithm

### Política de sellado

Descripción: Política de sellado de tiempo, obligatoria si se define una Autoridad de Sellado de Tiempo para la etiqueta tsaUrl.

Etiqueta: tsaPolicy

### Usuario de la TSA

Descripción: Nombre y contraseña del usuario de la TSA. Se ignora la contraseña s i previamente no se ha establecido un nombre de usuario.

Etiqueta: tsaUsr, tsaPwd

### Certificado SSL cliente

Descripción: Se define un nombre y una contraseña para el fichero PKCS#12 que contiene el certificado SSL cliente que pedirá la TSA al establecer conexiones HTTPS.

Etiqueta: tsaSslPkcs12File, tsaSslPkcs12FilePassword

## Datos del documento a firmar

La aplicación cifra los datos biométricos de los firmantes junto con la huella digital del documento original evitando de esta manera la réplica de los datos en otros documentos.

Se permite almacenar los documentos firmados tanto en un servidor, como en local, para ello es necesaria la especificación del directorio remoto en el que almacenarlo y el directorio local. La aplicación da la posibilidad de almacenar tanto en los dos directorios como en uno de ellos, no obstante, es imprescindible que se defina en el XML al menos uno de ellos.

A continuación se especifica la estructura del fichero XML en la que se describen los datos para la recuperación y almacenamiento del documento firmado.

<retrieveUrl></retrieveUrl>

<saveUrl></saveUrl>

<saveUrlPostParam></saveUrlPostParam>

<saveId></saveId>

<saveIdPostParam></saveIdPostParam>

<saveDirectory></saveDirectory>

<signedFileName></signedFileName>

<writableDirectory></writableDirectory>

<cert></cert>

<showTabletButtons></showTabletButtons>

### Directorio del documento

Descripción: Directorio desde dónde se recupera el documento original que se desea firmar. Puede estar definido en un repositorio (“http://direccion.com/fichero.pdf”) o como fichero local (“file://C:\directorio\fichero.pdf”).

Etiqueta: retrieveURL.

### Dirección URL para guardar el documento firmado

Descripción: Indicar la dirección de almacenamiento del documento firmado. Los documentos se recibirán por URL con un parámetro definido.

Etiqueta: saveUrl, saveUrlPostParam.

### Identificador del documento

Descripción: Indicar el identificador del documento, un número entero. En caso de que no se defina será nulo e indicar una etiqueta asignada a este identifacdor.

Etiqueta: saveId, saveIdPostParam.

### Directorio para guardar el documento firmado

Descripción: Indicar el directorio local en el que almacenar el documento firmado.

Etiqueta: saveDirectory.

### Nombre del documento firmado

Descripción: Nombre con el que se almacena el documento firmado. Este nombre se utiliza para guardar el documento tanto en local como en remoto.

Etiqueta: signedFileName.

### Directorio para ficheros temporales

Descripción: Nombre del directorio donde se almacenar los logs de las aplicación y las dll de las tabletas de captura de firma.

Etiqueta:writableDirectory

### Certificado

Descripción: Indicar el certificado de cifrado de los datos. Este certificado debe incluirse codificado en base 64.

Etiqueta: cert

### Mostrar botones en la tableta de firma

Descripción: Indicar mediante un booleano si se desea mostrar los botones de la tablet de firma. Estos botones permitirán al firmante aceptar, cancelar o repetir la operación de firma. En caso de que no se desee mostrar al firmante la botonera, al funcionario que realice el trámite sí que le aparecerá y por tanto, debe ser éste el que realice la acción de aceptar, repetir o cancelar.

Etiqueta: showTabletButtons.

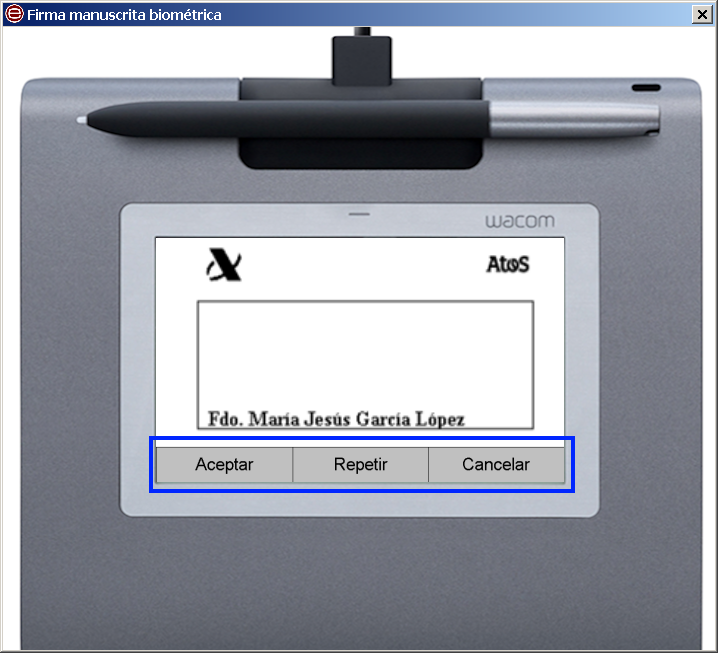


Figure 1 Imagen de una tableta de firma que contiene la botonera con las acciones de firma.

## Datos de los firmantes

Los datos de los firmantes del documento se definen en este apartado. Para cada firmante se introducen sus datos personales, la plantilla correspondiente para cada tipo de tableta con la que se trabaje y las posiciones que ocupa la rúbrica de la firma en el documento firmado.

Los datos de los firmantes están definidos por la etiqueta *bioSigns* y cada firmante es descrito es por la etiqueta *bioSign*. Esta es la estructura XML que describe los datos de los firmantes del documento:

<bioSigns>

<bioSign>

<signerData>

<signerName></signerName>

<signerSurname1></signerSurname1>

<signerSurname2></signerSurname2>

<signerId></signerId>

</signerData>

<signHeader></signHeader>

<signFooter></signFooter>

<tablet>

<tabletType></tabletType>

<htmlTemplate></htmlTemplate>

<jpegTemplate></jpegTemplate>

<tablet>

<signatureArea>

<x></x>

<y></y>

<width></width>

<height></height>

</signatureArea>

<signatureRubricPositionOnPdf>

<x></x>

<y></y>

<width></width>

<height></height>

</signatureRubricPositionOnPdf>

<signatureRubricPageOnPdf></signatureRubricPageOnPdf>

</bioSign>

<bioSigns>

### Datos personales

Descripción: Indicar los datos personales del firmante, estos datos se definen bajo la etiqueta signerData y debe especificarse el nombre, primer y segundo apellido, documento de identificación (NIE/NIF) y puesto de trabajo del firmante.

Etiquetas: sigenerName, signerSurname1, signerSurname2, signerId.

### Plantilla de firma

*Descripción*: La plantilla que se muestra en la pantalla de la tableta de firma puede ser definida o bien mediante una imagen JPEG o bien por código HTML.

Para ello es necesario crear una plantilla de uno de los dos tipos (JEPG o HTML) para cada tableta de firma, según el modelo del dispositivo que se conecte. Por lo tanto, cada firmante tiene asociada una plantilla de firma para el modelo de del dispositivo con el que vaya a realizar la operación.

La plantilla dada en el documento anexo contiene los logos de la agencia tributaria, en caso de querer utilizar dicha plantilla es necesario cambiar la firma por la del firmante personalizando el campo.

Este es el aspecto que muestra la tableta en la plantilla definida en el ejemplo adjunto en el anexo:



Figure 2 Imagen de una tableta de firma con una plantilla personalizada.

Etiqueta: tablet, tabletType, htmlTemplate, jpegTemplate.

### Área de firma

Descripción: Definir el área de firma de manera que quede determinada el área de la tableta en la que el usuario tiene que firmar y que está definida por una coordenada (x, y); punto en el que se sitúa la esquina superior izquierda del rectángulo de firma y por las dimensiones del área: altura y anchura.

Etiquetas: signature Area, x, y, width, height

### Área de firma en el documento

Descripción: Área en la que se sitúa la firma en el documento, dependiendo del firmante se ubicará en diferentes coordenadas, nunca correspondiendo dos firmas en la misma área. Se define una coordenadas (x,y) en la que se sitúa la esquina inferior derecha de la firma, la altura y la anchura que ocupa dicha área.

Cabe destacar que en los documentos PDF el espacio de coordenadas parte de la esquina inferior izquierda, siendo esta (0,0).

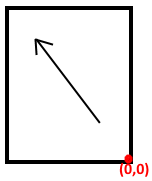


Figure 3 Coordenadas en PDF

### Página de firma

Descripción: Página del documento en la que aparece la firma.

Etiqueta: signatureRubricPageOnPdf

## Firma adicional

Los documentos que necesiten una firma adicional de una tercera entidad o de un funcionario deben tener completados los siguientes datos de la estructura XML:

<completeWithCriptoSign></completeWithCriptoSign>

<completeCriptoSignExtraParams>

<entry>

<key>pkcs12</key>

<value></value>

</entry>

</completeCriptoSignExtraParams>

<completeCriptoSignPkcs12></completeCriptoSignPkcs12>

<completeCriptoSignPkcs12Alias></completeCriptoSignPkcs12Alias>

<completeCriptoSignPkcs12Password></completeCriptoSignPkcs12Password/>

La firma del funcionario puede realizarse a través del certificado Pkcs12 que éste tenga almacenado en al almacén de claves o bien utilizando los parámetros de firma con certificado que se definan para el proceso de firma.

### Firma con parámetros adicionales

Descripción: Para una firma con certificado, se indicará con un booleano –true, false – en la etiqueta completeWithCriptoSign y se completarán los parámetros adicionales definidos en entry.

El conjunto de parámetros adicionales aceptado por la aplicación para añadir a una firma están descritos en el [anexo](#_Anexo).

Etiquetas: completeWithCriptoSign, completeCriptoSignExtraParams

### Firma con almacén PKCS12

Descripción: Esta aplicación permite la firma utilizando un almacén de claves Pkcs12. Para ello, se debe rellenar las etiquetas especificando el nombre del certificado PKCS12 almacenado en el almacén de claves, el nombre y la contraseña de la entidad a la que pertenece el certificado.

En caso de que no se definan los tres parámetros, la firma no se realiza.

Etiquetas: completeCriptoSignPkcs12, completeCriptoSignPkcs12Alias, completeCriptoSignPkcs12Password

# Plantilla de configuración

Plantilla de configuración del fichero XML que deberá codificarse en base 64 y definirlo en el applet de llamada a la aplicación.

<?xml version=*"1.0"* encoding=*"UTF-8"* standalone=*"yes"*?>

<ns2:signTask xmlns:ns2=*"es.gob.afirma.crypto.handwritten"*>

<CSV>

<page></page>

<text></text>

<rotation></rotation>

<positionOnPageLowerLeftX></positionOnPageLowerLeftX>

<positionOnPageLowerLeftY></positionOnPageLowerLeftY>

<positionOnPageUpperRightX></positionOnPageUpperRightX>

<positionOnPageUpperRightY></positionOnPageUpperRightY>

<fontSize></fontSize>

</CSV>

<tsaParams>

<tsaRequireCert></tsaRequireCert>

<tsaPolicy></tsaPolicy>

<tsaURL></tsaURL>

<tsaUsr></tsaUsr>

<tsaPwd></tsaPwd>

<extensions>

<extension>

<oid></oid>

<critical></critical>

<value></value>

</extension>

</extensions>

<tsaHashAlgorithm></tsaHashAlgorithm>

<sslPkcs12File></sslPkcs12File>

<sslPkcs12FilePassword></sslPkcs12FilePassword>

</tsaParams>

<writableDirectory></writableDirectory>

<retrieveUrl></retrieveUrl>

<saveUrl></saveUrl>

<saveUrlPostParam></saveUrlPostParam>

<saveId></saveId>

<saveIdPostParam></saveIdPostParam>

<saveDirectory></saveDirectory>

<signedFileName></signedFileName>

<cert></cert>

<showTabletButtons></showTabletButtons>

<bioSigns>

<bioSign>

<signerData>

<signerName></signerName>

<signerSurname1></signerSurname1>

<signerSurname2></signerSurname2>

<signerId></signerId>

</signerData>

<signHeader></signHeader>

<signFooter></signFooter>

<tablet>

<tabletType></tabletType>

<htmlTemplate></htmlTemplate>

<jpegTemplate></jpegTemplate>

<tablet>

<signatureArea>

<x></x>

<y></y>

<width></width>

<height></height>

</signatureArea>

<signatureRubricPositionOnPdf>

<x></x>

<y></y>

<width></width>

<height></height>

</signatureRubricPositionOnPdf>

<signatureRubricPageOnPdf></signatureRubricPageOnPdf>

</bioSign>

</bioSigns>

<completeWithCriptoSign></completeWithCriptoSign>

<completeCriptoSignExtraParams>

<entry>

<key></key>

<value></value>

</entry>

</completeCriptoSignExtraParams>

<completeCriptoSignPkcs12></completeCriptoSignPkcs12>

<completeCriptoSignPkcs12Alias></completeCriptoSignPkcs12Alias>

<completeCriptoSignPkcs12Password></completeCriptoSignPkcs12Password/>

</ns2:signTask>

# Anexo

## Listado de parámetros adicionales

Valores aceptados como parámetros adicionales para las firmas PAdES:

### allowCosigningUnregisteredSignatures

Si se establece a true se permite firmar un PDF incluso si este contiene firmas previas no registradas dentro de campos Acrobat (*AcroFields*), condición obligatoria sin la cual es muy probable que se corrompan las firmas previas.  
Si no se establece o se establece a o false, al intentar firmar un PDF que contenga firmas no registradas se lanza una excepción de tipo PdfHasUnregisteredSignaturesException.

### *includeOnlySignningCertificate*

Si se establece a true se incluye en la firma únicamente el certificado del firmante (y no la cadena de certificación completa). Si no se establece o se establece a o false se incluirá toda la cadena de certificación.

### alwaysCreateRevision

Si se establece a true siempre crea una revisión del PDF incluso cuando el documento no contiene ninguna firma previa.  
Esto requiere que los documentos de entrada cumplan estrictamente la especificación PDF 1.7 (ISO 32000-1:2008), y puede crear incompatibilidades con documentos PDF acordes a la especificación 1.3 creados con bibliotecas antiguas, como por ejemplo [QPDF](http://qpdf.sourceforge.net/).  
Si se establece a false, no crea revisiones en documentos que no contengan firmas previas y sí las crea en documentos que ya contengan alguna firma.

### image

Imagen que se desea insertar en el PDF antes de que este sea firmado. La imagen debe proporcionarse en formato JPEG codificado en Base64.  
SI el documento ya contiene firmas es posible que se invaliden, por lo que conviene usarlo únicamente en documentos sin firmas previas.

### imagePage

Página donde desea insertarse la imagen indicada mediante el parámetro image. La numeración de las páginas comienza en uno.  
Si se indica -1 como número de página se inserta la imagen en la última página del documento. Si se indica 0 como número de página se inserta la imagen en todas las páginas del documento. Este parámetro es obligatorio, si no se indica una página válida no se insertará la imagen.

### imagePositionOnPageLowerLeftX

Coordenada horizontal inferior izquierda de la posición de la imagen (indicada mediante el parámetro image) dentro de la página.  
Es necesario indicar el resto de coordenadas de la imagen mediante los parámetros imagePositionOnPageLowerLeftY, imagePositionOnPageUpperRightX e imagePositionOnPageUpperRightY.  
Es necesario indicar también una página de inserción en el parámetro imagePage.

### imagePositionOnPageLowerLeftY

Coordenada vertical inferior izquierda de la posición de la imagen (indicada mediante el parámetro image) dentro de la página.  
Es necesario indicar el resto de coordenadas de la imagen mediante los parámetros imagePositionOnPageLowerLeftX, imagePositionOnPageUpperRightX e imagePositionOnPageUpperRightY.  
Es necesario indicar también una página de inserción en el parámetro imagePage.

### imagePositionOnPageUpperRightX

Coordenada horizontal superior derecha de la posición de la imagen (indicada mediante el parámetro image) dentro de la página.  
Es necesario indicar el resto de coordenadas de la imagen mediante los parámetros imagePositionOnPageLowerLeftX, imagePositionOnPageLowerLeftY e imagePositionOnPageUpperRightY.  
Es necesario indicar también una página de inserción en el parámetro imagePage.

### imagePositionOnPageUpperRightY

Coordenada vertical superior derecha de la posición de la imagen (indicada mediante el parámetro image) dentro de la página.  
Es necesario indicar el resto de coordenadas de la imagen mediante los parámetros imagePositionOnPageLowerLeftX, imagePositionOnPageLowerLeftY e imagePositionOnPageUpperRightX.  
Es necesario indicar también una página de inserción en el parámetro imagePage.

### attach

Contenido a añadir como adjunto al PDF, en formato Base64 (el adjunto será el binario decodificado). Este parámetro requiere que se haya establecido también el parámetro attachFileName.

### attachFileName

Nombre de fichero para adjuntar el contenido binario indicado mediante attach. Este parámetro requiere que se haya establecido también el parámetro attach.

### attachDescription

Descripción del contenido binario indicado mediante attach.

### certificationLevel

Nivel de certificación de la firma PDF.  
Los valores admitidos son numéricos, correspondiendo:

* *0* = Firma ordinaria no certificada (por defecto)
* *1* = Firma de autor. No se permite ningún cambio posterior en el documento
* *2* = Firma de autor certificada para formularios. Se permite únicamente el relleno posterior de los campos del formulario
* *3* = Firma certificada. Se permite únicamente el relleno posterior de los campos del formulario o el añadido de firmas de aprobación

### signatureSubFilter

Nombre del sub-filtro en el diccionario PDF para indicar el tipo de la firma. Si no se indica este parámetro por defecto se usa adbe.pkcs7.detached (firma PAdES básica). Es posible indicar ETSI.CAdES.detached para generar una firma PAdES-BES, si bien el hacerlo puede causar que al añadir firmas adicionales al PDF se invaliden las ya existentes.

### signatureField

Nombre del campo en donde insertar la firma. Si el documento PDF tiene ya un campo de firma pre-creado es posible utilizarlo para insertar la firma generada, referenciándolo por su nombre.  
Si se indica un nombre de campo de firma que no exista en el documento PDF proporcionado, se generará una excepción.

### signaturePage

Página del documento PDF donde insertar la firma. Puede usarse la constante LAST\_PAGE para referirse a la última página del documento PDF si se desconoce el número total de páginas de este.  
Este parámetro se ignora si se ha establecido valor al parámetro signatureField, y necesita que se establezcan valores válidos a los parámetros signaturePositionOnPageLowerLeftX, signaturePositionOnPageLowerLeftY, signaturePositionOnPageUpperRightX y signaturePositionOnPageUpperRightY.

### signaturePositionOnPageLowerLeftX

Coordenada horizontal inferior izquierda de la posición del recuadro visible de la firma dentro de la página.  
Es necesario indicar el resto de coordenadas del recuadro mediante los parámetros signaturePositionOnPageLowerLeftY, signaturePositionOnPageUpperRightX y signaturePositionOnPageUpperRightY.  
Si no se indica una página en el parámetro signaturePage la firma se inserta en la última página del documento.

### signaturePositionOnPageLowerLeftY

Coordenada vertical inferior izquierda de la posición del recuadro visible de la firma dentro de la página.  
Es necesario indicar el resto de coordenadas del recuadro mediante los parámetros signaturePositionOnPageLowerLeftX, signaturePositionOnPageUpperRightX y signaturePositionOnPageUpperRightY.  
Si no se indica una página en el parámetro signaturePage la firma se inserta en la última página del documento.

### signaturePositionOnPageUpperRightX

Coordenada horizontal superior derecha de la posición del recuadro visible de la firma dentro de la página.  
Es necesario indicar el resto de coordenadas del recuadro mediante los parámetros signaturePositionOnPageLowerLeftX, signaturePositionOnPageLowerLeftY y signaturePositionOnPageUpperRightY.  
Si no se indica una página en el parámetro signaturePage la firma se inserta en la última página del documento.

### signaturePositionOnPageUpperRightY

Coordenada vertical superior derecha de la posición del recuadro visible de la firma dentro de la página.  
Es necesario indicar el resto de coordenadas del recuadro mediante los parámetros signaturePositionOnPageLowerLeftX, signaturePositionOnPageLowerLeftY y signaturePositionOnPageUpperRightX.  
Si no se indica una página en el parámetro signaturePage la firma se inserta en la última página del documento.

### signatureRubricImage

Imagen JPEG codificada en Base64 de la rúbrica de la firma manuscrita que se desea aparezca como firma visible en el PDF.

### layer2Text

Texto a escribir dentro de la "capa 2" de la firma visible.  
Este texto se escribe únicamente si no se ha especificado una imagen de rúbrica, y necesita que se indique la página y la situación dónde mostrar el recuadro de firma mediante los parámetros signaturePositionOnPageLowerLeftX, signaturePositionOnPageLowerLeftY, signaturePositionOnPageUpperRightX, signaturePositionOnPageUpperRightY y signaturePage.

### layer2FontFamily

Tipo de letra a usar en el texto de la "capa 2" de la firma visible. Este parámetro requiere que se haya establecido también el parámetro layer2Text.  
Los valores admitidos son numéricos, correspondiendo:

* *0* = Courier (tipo por defecto)
* *1* = Helvética
* *2* = Times Roman
* *3* = Symbol
* *4* = ZapfDingBats

### layer2FontSize

Tamaño de letra a usar en el texto de la "capa 2" de la firma visible. Este parámetro requiere que se haya establecido también el parámetro layer2Text.  
Los valores admitidos son numéricos (y el valor por defecto es 12).

### layer2FontStyle

Estilo del tipo de letra a usar en el texto de la "capa 2" de la firma visible. Este parámetro requiere que se haya establecido también el parámetro layer2Text.  
Los valores admitidos son numéricos, correspondiendo:

* *0* = Normal (estilo por defecto)
* *1* = Negrita
* *2* = Cursiva
* *3* = Negrita y cursiva
* *4* = Subrayado
* *8* = Tachado

Es posible combinar estilos aplicando la operación lógica o sobre los valores numéricos a combinar.

### layer2FontColor

Color del texto de la "capa 2" de la firma visible. Este parámetro requiere que se haya establecido también el parámetro layer2Text.  
Los valores admitidos son textuales (se ignora entre mayúsculas y minúsculas), soportándose:

* *black* = Negro (color por defecto)
* *white* = Blanco
* *gray* = Gris
* *lightGray* = Gris claro
* *darkGray* = Gris oscuro
* *red* = Rojo
* *pink* = Rosa

### signReason

Razón por la que se realiza la firma (este dato se añade al diccionario PDF, y no a la propia firma).

### **signatureProductionCity**

Ciudad en la que se realiza la firma (este dato se añade al diccionario PDF, y no a la propia firma).

### signerContact

Contacto del firmante, usualmente una dirección de correo electrónico (este dato se añade al diccionario PDF, y no a la propia firma).

### policyIdentifier

Identificador de la política de firma. Debe ser un OID (o una URN de tipo OID) que identifique unívocamente la política en formato ASN.1 procesable.

### policyIdentifierHash

Huella digital del documento de política de firma (normalmente del mismo fichero en formato ASN.1 procesable). Si no se indica una huella digital y el parámetro policyIdentifier no es una URL accesible universalmente se usará 0, mientras que si no se indica una huella digital pero el parámetro policyIdentifier es una URL accesible universalmente, se descargara el fichero apuntado por la URL para calcular la huella digital *al vuelo*.

### policyIdentifierHashAlgorithm

Algoritmo usado para el cálculo de la huella digital indicada en el parámetro policyIdentifierHash. Es obligatorio indicarlo cuando se proporciona una huella digital distinta de 0.

### policyQualifier

URL que apunta al documento descriptivo de la política de firma (normalmente un documento PDF con una descripción textual).

### ownerPassword

Contraseña de apertura del PDF (contraseña del propietario) si este estaba cifrado.  
No se soporta la firma de documentos PDF cifrados con certificados o con algoritmo AES256.

### headLess

Evita cualquier interacción con el usuario si se establece a true, si no se establece o se establece a false actúa normalmente (puede mostrar diálogos, por ejemplo, para solicitar las contraseñas de los PDF cifrados). Útil para los procesos desatendidos y por lotes.

### avoidEncryptingSignedPdfs

Si se establece a true no cifra los PDF firmados aunque el original estuviese firmado, si no se establece o se establece a false los PDF se cifran tras firmarse si el original lo estaba, usando la misma contraseña y opciones que este.

### allowSigningCertifiedPdfs

Si se establece a true permite la firma o cofirma de PDF certificados sin consultarlo al usuario, si se establece a false o cualquier otro valor se lanza una excepción en caso de intentar firmar o cofirmar un PDF certificado y si no se establece se mostrará un diálogo al usuario para que confirme que desea realizar la firma a pesar de que el resultado serán una firma no válida.  
**Si el parámetro headLess está establecido a true, no podrá mostrar el diálogo de confirmación así que llegados a este punto se lanzará una excepción.**  
No se soporta el cifrado de documentos PDF con certificados o con algoritmo AES256.

### tsType

Tipo de sello de tiempo a aplicar:

* 1 = Solo sello a nivel de firma.
* 2 = Solo sello a nivel de documento.
* 3 = Dos sellos, uno a nivel de firma y otro a nivel de documento.

### tsaURL

URL de la autoridad de sello de tiempo (si no se indica no se añade sello de tiempo).

### tsaPolicy

Política de sellado de tiempo (obligatoria si se indica tsaURL).

### tsaHashAlgorithm

Algoritmo de huella digital a usar para el sello de tiempo (si no se establece se usa SHA-1).

### tsaRequireCert

true si se requiere el certificado de la TSA, false en caso contrario (si no se establece se asume true).

### tsaUsr

Nombre de usuario de la TSA.

### tsaPwd

Contraseña del usuario de la TSA. Se ignora si no se ha establecido además tsaUsr.

### tsaSslPkcs12File

Nombre del fichero PKCS#12 que contiene el certificado SSL cliente que pedirá la TSA al establecer la coneciós HTTPS.

### tsaSslPkcs12FilePassword

Contraseña del fichero PKCS#12 que contiene el certificado SSL cliente para las conexiones HTTPS.

### signingCertificateV2

Si se indica a true se utilizará SigningCertificateV2, si se indica cualquier otra cosa SigningCertificateV1. Si no se indica nada, se utilizará V1 para las firmas SHA1 y V2 para el resto.

# Ejemplo

Este documento anexo es un ejemplo de documento XML para la firma de un documento por una entidad firmante e incluye la firma del funcionario por medio de un certificado PKCS12 ya definido.

Ejemplo:

<?xml version=*"1.0"* encoding=*"UTF-8"* standalone=*"yes"*?>

<ns2:signTask xmlns:ns2=*"es.gob.afirma.crypto.handwritten"*>

<!-- PARTE 1 -->

<CSV>

<page>1</page>

<text>CSV123812347823748946</text>

<rotation>90</rotation>

<positionOnPageLowerLeftX>200</positionOnPageLowerLeftX>

<positionOnPageLowerLeftY>20</positionOnPageLowerLeftY>

<positionOnPageUpperRightX>200</positionOnPageUpperRightX>

<positionOnPageUpperRightY>300</positionOnPageUpperRightY>

<fontSize>15</fontSize>

<text>CSV-1231208</text>

<rotation>0</rotation>

<positionOnPageLowerLeftX>100</positionOnPageLowerLeftX>

<positionOnPageLowerLeftY>100</positionOnPageLowerLeftY>

<positionOnPageUpperRightX>200</positionOnPageUpperRightX>

<positionOnPageUpperRightY>200</positionOnPageUpperRightY>

<fontSize>15</fontSize>

</CSV>

<!-- PARTE 2 -->

<tsaParams>

<tsaRequireCert>true</tsaRequireCert>

<tsaPolicy>4.3.2.1</tsaPolicy>

<tsaURL>http://aeat.aeat</tsaURL>

<tsaUsr>user</tsaUsr>

<tsaPwd>password</tsaPwd>

<extensions>

<extension>

<oid>1.2.3.4</oid>

<critical>false</critical>

<value>//o=</value>

</extension>

</extensions>

<tsaHashAlgorithm>SHA-512</tsaHashAlgorithm>

<sslPkcs12File>AAECAw==</sslPkcs12File>

<sslPkcs12FilePassword>p12password</sslPkcs12FilePassword>

</tsaParams>

<!-- PARTE 3 -->

<writableDirectory>C:\Temp</writableDirectory>

<retrieveUrl>file://C:\Temp\formulario1.pdf</retrieveUrl>

<saveUrl></saveUrl>

<saveUrlPostParam></saveUrlPostParam>

<saveId>001</saveId>

<saveIdPostParam>id</saveIdPostParam>

<saveDirectory>C:\Temp</saveDirectory>

<writableDirectory>C:\Temp</writableDirectory>

<retrieveUrl>file://C:\Temp\formulario1.pdf</retrieveUrl>

<saveUrl></saveUrl>

<saveUrlPostParam></saveUrlPostParam>

<saveId>004</saveId>

<saveIdPostParam>idd</saveIdPostParam>

<saveDirectory>C:\Temp\</saveDirectory>

<signedFileName>PDF firmado</signedFileName> <cert></cert>

<showTabletButtons>false</showTabletButtons>

<!-- PARTE 4 -->

<bioSigns>

<bioSign>

<signerData>

<signerName>Ana</signerName>

<signerSurname1>Pérez</signerSurname1>

<signerSurname2>García</signerSurname2>

<signerId>12345678Z</signerId>

<signerPost></signerPost>

</signerData>

<signHeader>Ejemplo de cabecera</signHeader>

<signFooter>Ejemplo de pie de firma</signFooter>

<tablet>

<tabletType>STU-430</tabletType>

<htmlTemplate>

&lt;p style="font-weight: bold; font-size:12px; margin-left:20px;"&gt; Firme en el recuadro y pulse aceptar:

&lt;/p&gt;

&lt;div style="margin-left:20px; margin-top:58px;" &gt;

&lt;p style="font-weight: bold; font-size:12px;"&gt;

Fdo. Ana Pérez García

&lt;/p&gt;

&lt;/div&gt;

</htmlTemplate>

</tablet>

<signatureArea>

<x>20</x>

<y>50</y>

<width>275</width>

<height>100</height>

</signatureArea>

<signatureRubricPositionOnPdf>

<x>75</x>

<y>220</y>

<width>150</width>

<height>55</height>

</signatureRubricPositionOnPdf>

<signatureRubricPageOnPdf>1</signatureRubricPageOnPdf>

</bioSign>

</bioSigns>

<!-- PARTE 5 -->

<completeWithCriptoSign>true</completeWithCriptoSign>

<completeCriptoSignExtraParams>

<entry>

<key>clave</key>

<value>valor</value>

</entry>

</completeCriptoSignExtraParams>

<completeCriptoSignPkcs12></completeCriptoSignPkcs12>

<completeCriptoSignPkcs12Alias>anf usuario activo</completeCriptoSignPkcs12Alias>

<completeCriptoSignPkcs12Password>12341234</completeCriptoSignPkcs12Password>

</ns2:signTask>