ASF

WEBSIGNERACTIVEX FAQS

Versión 1.4

HOJA DE CONTROL DOCUMENTAL

Resumen El propósito de este documento es proveer una guía de FAQs para resolver las preguntas mas comunes sobre este componente.

Versión	***Fecha***	***Autor***	***Revisado***	***Descripción***
1.0	05/11/2009	Óscar Flor Lozano	Óscar Flor Lozano	Primera versión
1.1	06/11/2009	Julio Gregorio de la Riva		Contenido inicial del documento
1.2	25/01/2010	Javier Romero Torcal	Daniel Vilas	Soporte a Internet Explorer 8
1.3	22/06/2010	José Romero		Añadir limitaciones detectadas en ciertos servicios con firmas de gran tamaño, indicando los servicios alternativos
1.4	13/10/2010	Javier Romero		Mensajes de seguridad en operaciones críticas silenciosas

ÍNDICE

1. INTRODUCCIÓN 4

2. FUNCIONALIDAD GENERAL 5

3. FAQS 7

3.1. Problemas durante la instalación 7

3.1.1. El usuario no tiene permisos de instalación de ActiveX 7

3.1.2. Internet Explorer no permite la ejecución 7

3.1.3. Internet Explorer no permite la ejecución de JavaScripts 9

3.1.4. No se confía en el Certificado de firma de TB-Solutions 10

3.1.5. El componente se encuentra mal instalado 10

3.1.6. Problemas con la instalación de la librería capicom.dll 11

3.2. Problemas durante la explotación 12

3.2.1. El componente esta mal instalado 12

3.2.2. No hay permisos de Ejecución / Componente deshabilitado 12

3.2.3. Versiones Incoherentes. 12

3.2.4. Petición Continua de instalación de WebSigner 13

3.2.5. Problemas en capicom al obtener los certificados 13

3.2.6. Depurador de IExplorer. 14

3.2.7. Alertas de seguridad ante operaciones críticas silenciosas 14

3.3. Desinstalación 15

3.3.1. Problemas durante la desinstalación 22

3.4. Problemas con versiones concretas del navegador: 22

3.4.1. Internet Explorer 7 23

3.4.2. Internet Explorer 7 en Windows Vista 23

3.4.3. Internet Explorer 8 23

4. LIMITACIONES 24

1. INTRODUCCIÓN

Este documento presenta los errores más típicos en la instalación y explotación del Componente WebSigner ActiveX de ASF.

Se parte de las causas principales y se describe los síntomas y causas especificas para acaba explicando la solución.

Esta redactado pensando en los integradores de ASF y es una ayuda para que redacten su propio documento especifico para el sitio Web que este integrándose con WebSigner ActiveX. Alguno de los fallos puede solucionarse o reducirse con una correcta integración.

Este documento también tiene como finalidad presentar un resumen de las limitaciones y restricciones en el uso de Websigner ActiveX, así como un resumen de las plataformas soportadas por el mismo.

Tras una descripción general del componente, se describirán las limitaciones que presenta. Finalmente, se mostrarán unas tablas que resumen las soportadas por WebSigner ActiveX.

2. FUNCIONALIDAD GENERAL

WebSigner ActiveX es el componente cliente de la plataforma. Se descarga en el navegador de los usuarios de la plataforma y permite firma, verificación, cifrado y descifrado en cliente.

Los formatos de firma soportados son:

- PKCS#7 v1.5, según se especifica en el RFC 2315.
- CMS, según se especifica en los RFCs 2630, RFC 3369 y RFC 3852.
- XMLDSig, de acuerdo con la recomendación del consorcio W3C: "XML-signature Syntax and Processing".
- XAdES, según se especifica en ETSI TS 101 903 v1.2.2, en sus subtipos BES y EPES.
- CAdES, según se especifica en ETSI TS 101 733 v1.6.3, en sus subtipos BES y EPES.

Los algoritmos de firma soportados son:

- RSA, con algoritmos de hash MD5 y SHA-1.
- DSA, con algoritmos de hash SHA-1.

Los formatos de cifrado soportados son:

- PKCS#7 v1.5, según se especifica en el RFC 2315.
- CMS, según se especifica en los RFCs 2630, RFC 3369 y RFC 3852.
- XMLEncryption, de acuerdo con la recomendación del consorcio W3C: "XML-Encryption Syntax and Processing".

Los algoritmos de cifrado soportados (con las restricciones comentadas más adelante) son:

- DES
- 3DES
- RC2

- RC4
- AES

WebSigner ActiveX basa su solución en la innovadora CAPICOM, un control ActiveX que proporciona una interfaz COM para la biblioteca criptográfica Microsoft CryptoAPI, así como invocaciones directas a dicha CryptoAPI. Para la firma XMLDSIG basa su solución en las librerías XERCES, XALAN y XSEC de Apache implementando el modulo en C++.

3. FAQS

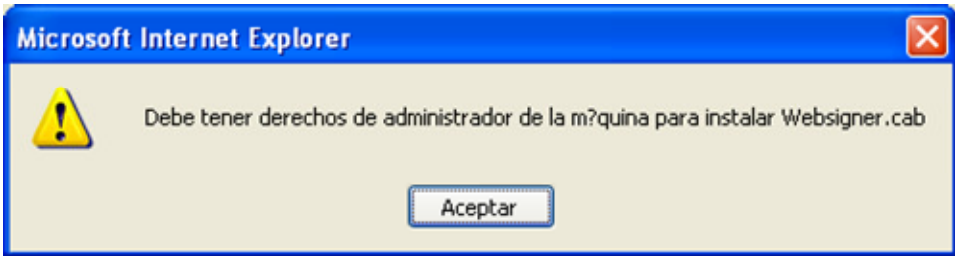
3.1. Problemas durante la instalación

Problemas típicos durante la instalación, todos estos comparten que no se puede instalar el ActiveX y algún mensaje de error ("debe tener permisos de administrador para instalar WebSigner" o un error avisando de que no se ha podido cargar el objeto). Además una vez solucionado el problema debe procederse nuevamente a la instalación del ActiveX.

3.1.1. El usuario no tiene permisos de instalación de ActiveX

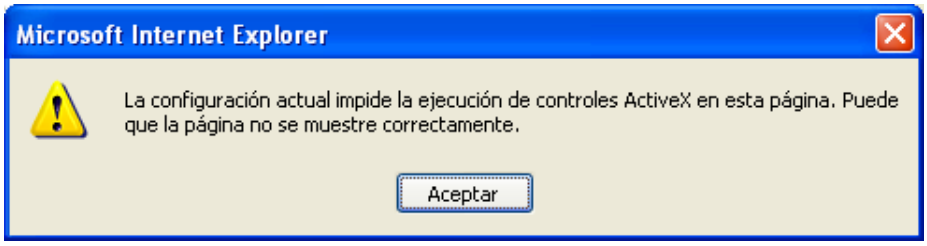
El grupo "usuarios" de un dominio NT (o Active Directory) por defecto no tiene permisos para instalar ActiveX. Debe instalarse WebSigner ActiveX por un usuario que tenga, como mínimo, permisos de Administrador de la maquina o prepararse el componente como seguro dentro del ActiveDirectory, consulte la documentación de Microsoft referente a tal efecto.

El mensaje que aparece cuando sucede esto es el siguiente (este mensaje es susceptible de se cambiado en cualquier momento):



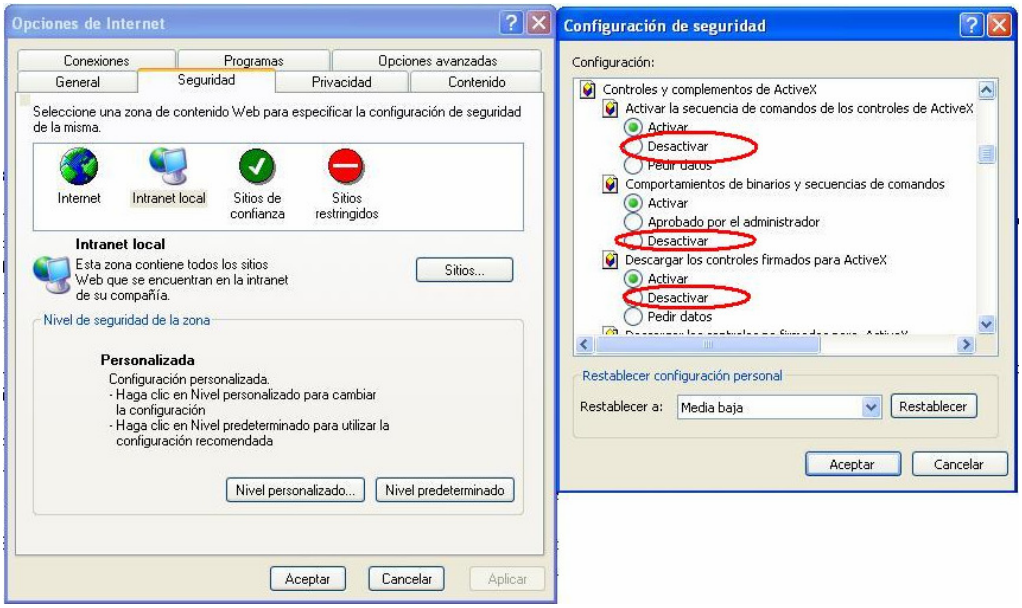
3.1.2. Internet Explorer no permite la ejecución

Este error se debe a la configuración por defecto de IExplorer no permite la ejecución de ActiveX desde paginas a las cuales no se les haya considerado como de confianza. El mensaje notificado por IExplorer es:



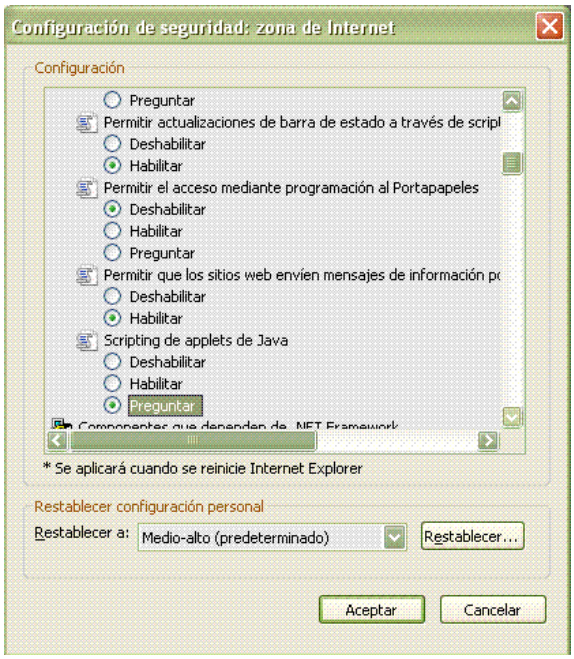
Hay que poner el servidor donde se encuentran las páginas que usan WS en una zona de seguridad (Configurar las zonas de seguridad de IExplorer) donde se tenga activado la ejecución de ActiveX. La configuración de seguridad debe permitir la instalación y ejecución, prestar especial atención a la desactivación

de los puntos que se muestran en la siguiente figura:

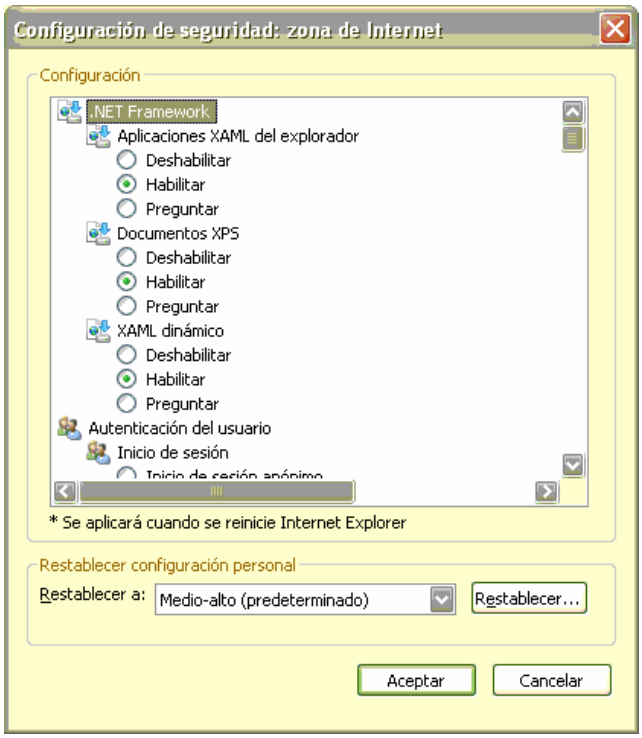


NOTA: Hay veces que se puede hacer necesario realizar otras modificaciones en la configuración de IExplorer. Estas modificaciones se dan en los apartados:

- ✓ Automatización:



✓ .Net Framework:

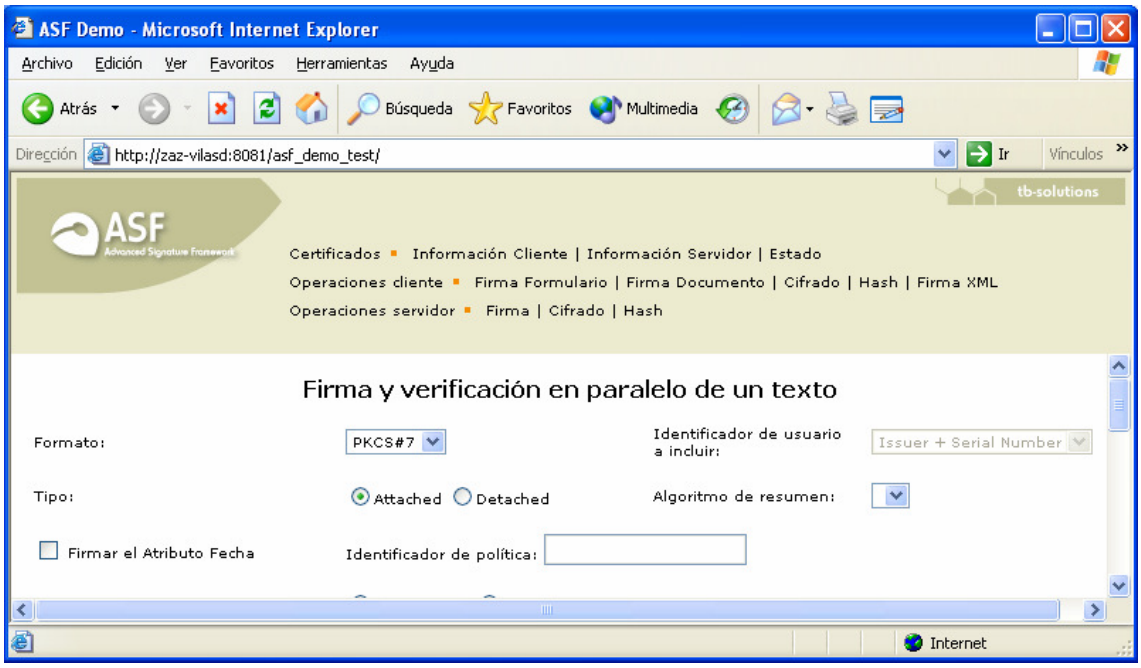


3.1.3. Internet Explorer no permite la ejecución de JavaScripts

Este error se debe a la configuración por defecto de IExplorer no permite la ejecución de JavaScript desde paginas a las cuales no se les haya considerado como de confianza.

Hay que poner el servidor donde se encuentran las páginas que usan WS en un zona de seguridad (Configurar las zonas de seguridad de IExplorer) donde se tenga activado la ejecución de JavaScript

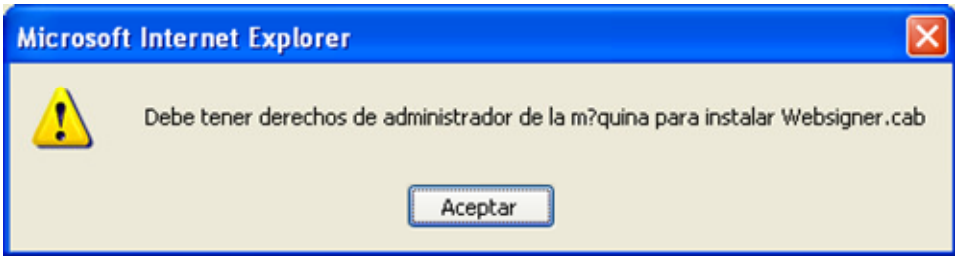
En este caso, y según configuraciones de IExplorer, no se mostrara ningún mensaje. La siguiente captura es un caso tipo, como se puede apreciar no se cargan bien algunas constantes



3.1.4. No se confía en el Certificado de firma de TB-Solutions

Este error se puede deber a que se ha cancelado la confianza en el momento de la instalación, o a que el administrador de la red no confía, o nuevas versiones de Windows que exigen una confianza Explicita por parte del usuario. O a que no se puede comprobar el estado del certificado.

El usuario debe confiar explícitamente en el certificado (habría que ponerlo en sitio publico y escribir las instrucciones). Básicamente es incluir el certificado en el almacén correspondiente de Windows.



3.1.5. El componente se encuentra mal instalado

Esto puede deberse que ha habido problemas de conexión durante instalación del mismo. Normalmente esto puede suceder con líneas de acceso a Internet de “Banda estrecha” y a una integración del componte no recomendada.

Hay que desinstalar el componente a mano y volver a realizar el proceso de desinstalación, Para borrar el registro del componente hay que ejecutar un archivo que borre las entradas del registro.

Para el integrador, para este tipo de conexiones hay que inicializar WebSigner ActiveX desde un punto que bloquee el hilo del navegador siguiendo las recomendaciones de la guía de integración.

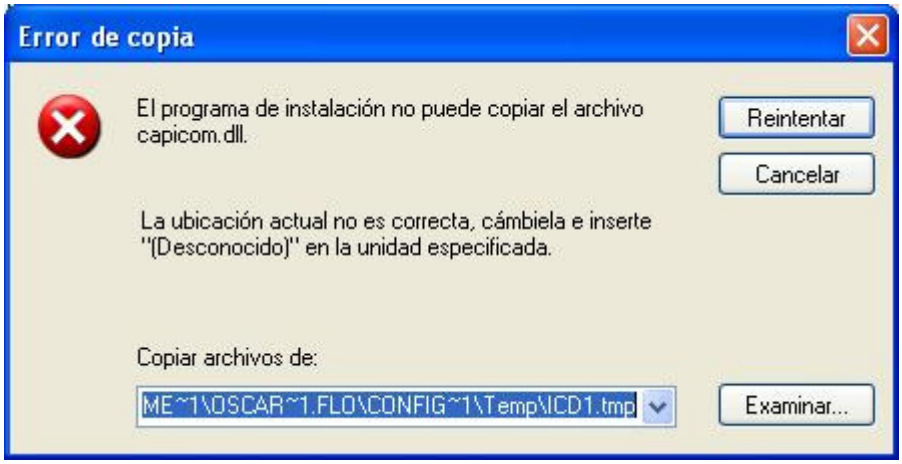
3.1.6. Problemas con la instalación de la librería capicom.dll

La librería capicom.dll es propietaria de Microsoft y hoy en día viene de serie en la mayoría de sus sistemas operativos.

Previendo que el usuario pueda tener una versión de sistema operativo donde la librería no se encuentre o que hubiese sido borrada, el componente ActiveX suministra esta librería.

El funcionamiento básicamente es el siguiente: si la máquina no tiene la librería se copia la del componente, si la máquina tiene la librería pero es de una versión inferior a la del componente se copia la del componente.

En el copiado descrito en el punto anterior en ocasiones surge el siguiente problema:



Es debido a que en el momento de la copia la librería se encuentra en ejecución, puede ser por otra aplicación que la use, puede ser por el propio sistema operativo (ejemplo: un inicio de sesión en Windows con tarjeta criptográfica), la solución para esto es asegurarnos que ninguna aplicación la esta usando, y en ese momento proceder a la descarga, si no sabemos que aplicación es podemos probar lo siguiente:

- Arrancar la máquina y proceder a la descarga antes de ejecutar nada más.

Si lo anterior no funciona podemos proceder a realizar una actualización manual, lo mas fiable es descargar la librería de la página oficial de Microsoft: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6

3.2. Problemas durante la explotación

Problemas típicos durante la ejecución, cada uno con sus síntomas.

3.2.1. El componente esta mal instalado

El comportamiento en este caso puede ser diferente según lo que este registrado y habilitado.

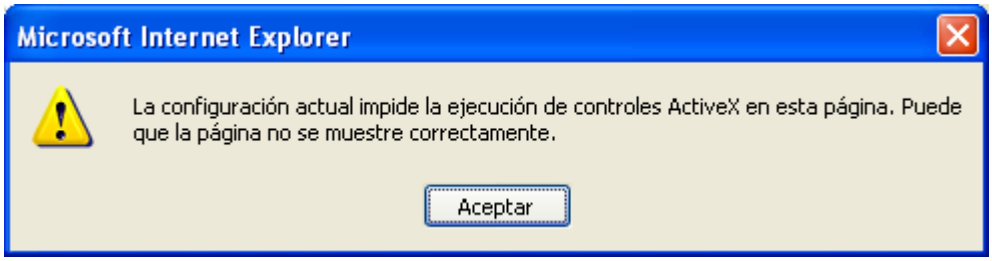
En algunos casos no se encuentra los certificados, en otros no permite firmar.

Para solucionarlo hay que desinstalar todo el componente WebSigner ActiveX y proceder a una nueva instalación.

3.2.2. No hay permisos de Ejecución / Componente deshabilitado

Si no hay permisos de ejecución de ActiveX, de JavaScript o se ha deshabilitado el componente no se mostrara ningún certificado.

El usuario debe tener permisos de ejecución de ActiveX y tener el componente habilitado. Mirar el apartado de instalación.



3.2.3. Versiones Incoherentes.

Los componentes JavaScript comprueban la versión y notifica el error en caso de que la versión instalada sea menor a la que esperan. La solución pasa por una reinstalación del componente.

Este error puede deberse a que el usuario no pueda instalar una nueva versión, revisar el apartado de instalación, o a que únicamente pueda acceder a una versión vieja del componente (caches Web, versiones antiguas del componente en el servidor,…)

Hay que asegurarse que en el servidor se encuentra la última versión y de que tenga acceso a los correspondientes ficheros.

3.2.4. Petición Continua de instalación de WebSigner

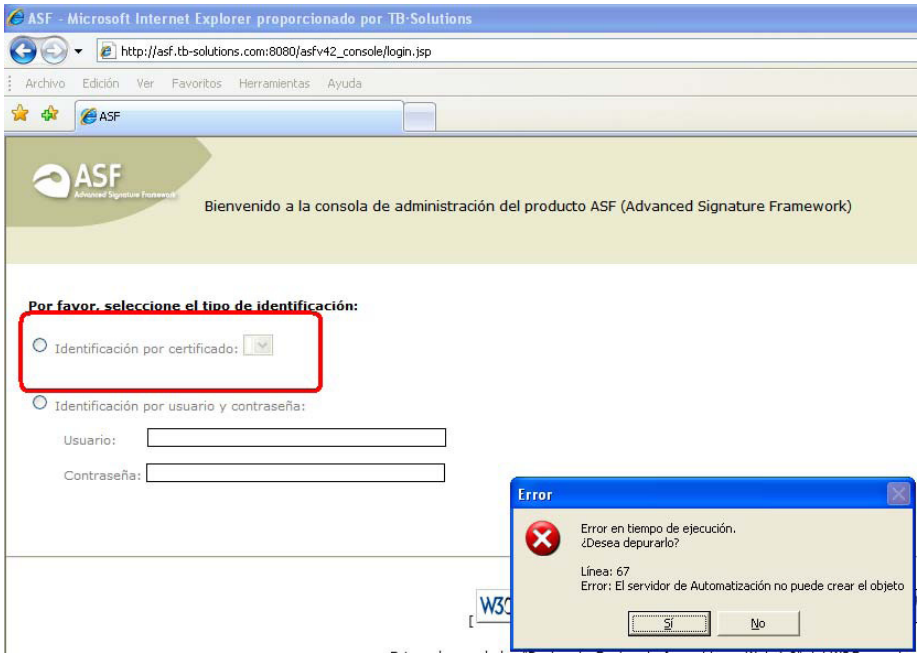
Cada vez que se cambia entre páginas que usan WebSigner ActiveX nos pide instalar el componente, aunque se haya instalado en la página anterior.

Este es el mismo caso que el anterior (salvo que en vez de notificar un error, los componentes JavaScript inician la instalación) y al igual que en este ultimo hay que revisar que en el Servidor estén las últimas versiones, el cliente tenga acceso a estas últimas versiones (si es preciso borrando todos las caches) y que pueda instalar correctamente el componente.

En el caso de que no se pueda realizar una actualización automática, hay que realizar una desinstalación total y una nueva instalación de WebSigner ActiveX.

3.2.5. Problemas en capicom al obtener los certificados

En algunos ordenadores puede verse un error similar al que se muestra en la siguiente imagen.



En este caso el error se produce en la consola pero se puede producir también ejecutando la librería Websigner ActiveX en Internet Explorer.

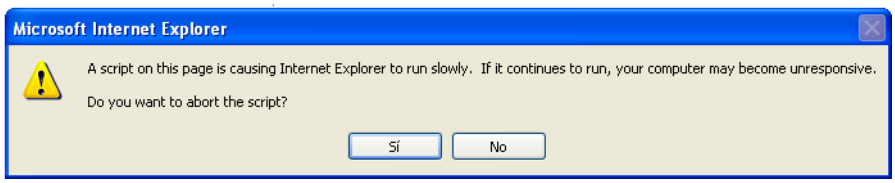
Del error no se conoce la causa pero se ha solucionado reinstalando el componente CAPICOM. Este se puede descargar de la siguiente dirección.

http://www.microsoft.com/downloads/details.aspx?displaylang=es&FamilyID=ca930018-4a66-4da

3.2.6. Depurador de IExplorer.

Se han detectado que en algunos momentos salta un mensaje indicando que la pagina Web ira lenta debido a un componente. Esto se debe a un depurador integrado en el propio Internet Explorer se puede deshabilitar

Revise que los scripts que llaman al componente no entran en un bucle sin fin. El depurador Integrado también notificara dicho mensaje si alguna salida es un "break" o hay "pauses" de por medio. El código de WebSigner ActiveX no produce por si mismo esta situación.

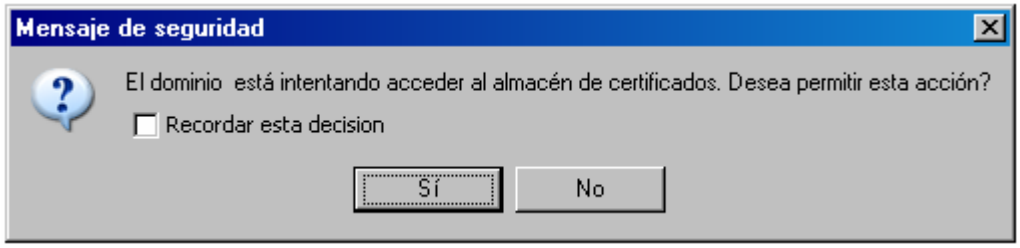


3.2.7. Alertas de seguridad ante operaciones críticas silenciosas

Al intentar realizar ciertas operaciones de manera silenciosa y automática se lanzan una serie de ventanas de aviso para que el usuario sea conciente de quién intenta ejecutar las acciones en cada momento y si quiere o no permitirlas.

Existe la opción de memorizar cada acceso permitido para que en futuras ejecuciones en la misma sesión (esto es mientras no se cierra el navegador) permita o no, de manera automática la operación requerida por un dominio en concreto.

Si por ejemplo, se intenta acceder al almacén de certificados de manera automática, salta este aviso para que sea el usuario el que decida si realmente quiere que el dominio actual pueda acceder a dicho almacén. Se puede marcar el checkbox "Recordar esta decisión" si se desea que este mensaje no aparezca y siempre se quiera ejecutar la misma opción.



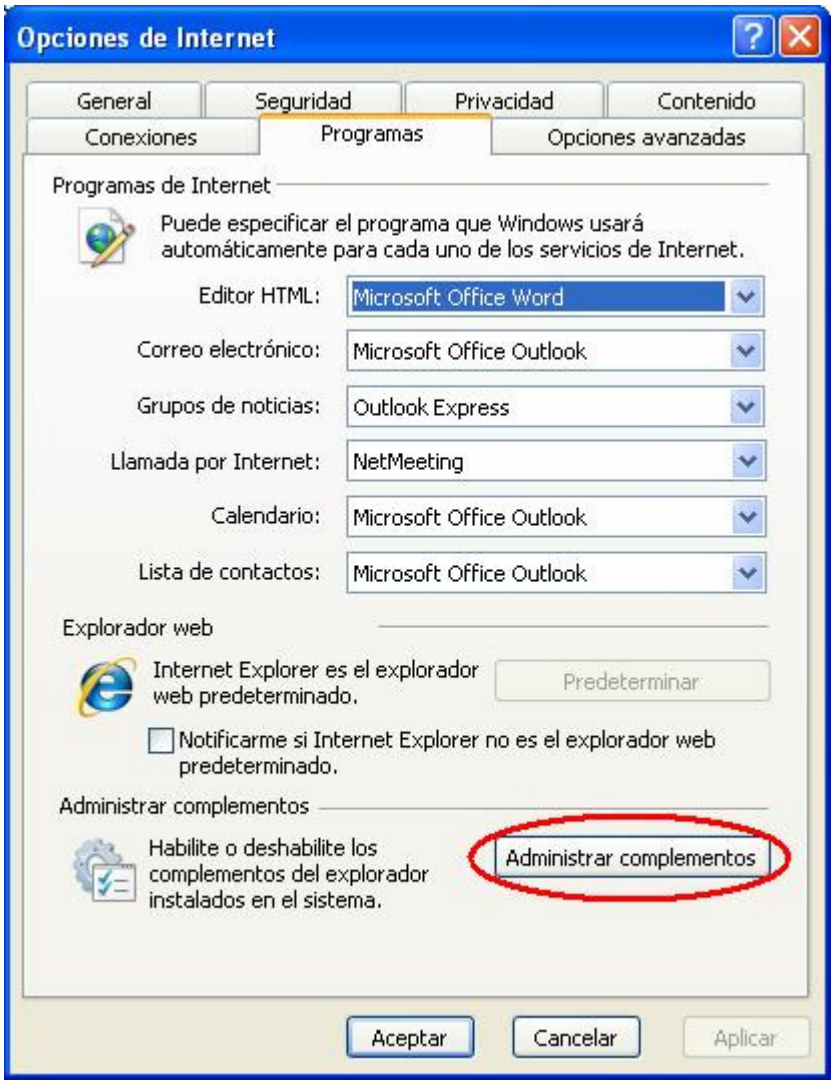
En caso de cerrar el navegador, hará falta marcar el checkbox para que vuelva a recordarlo la siguiente vez que se ejecute.

3.3. Desinstalación

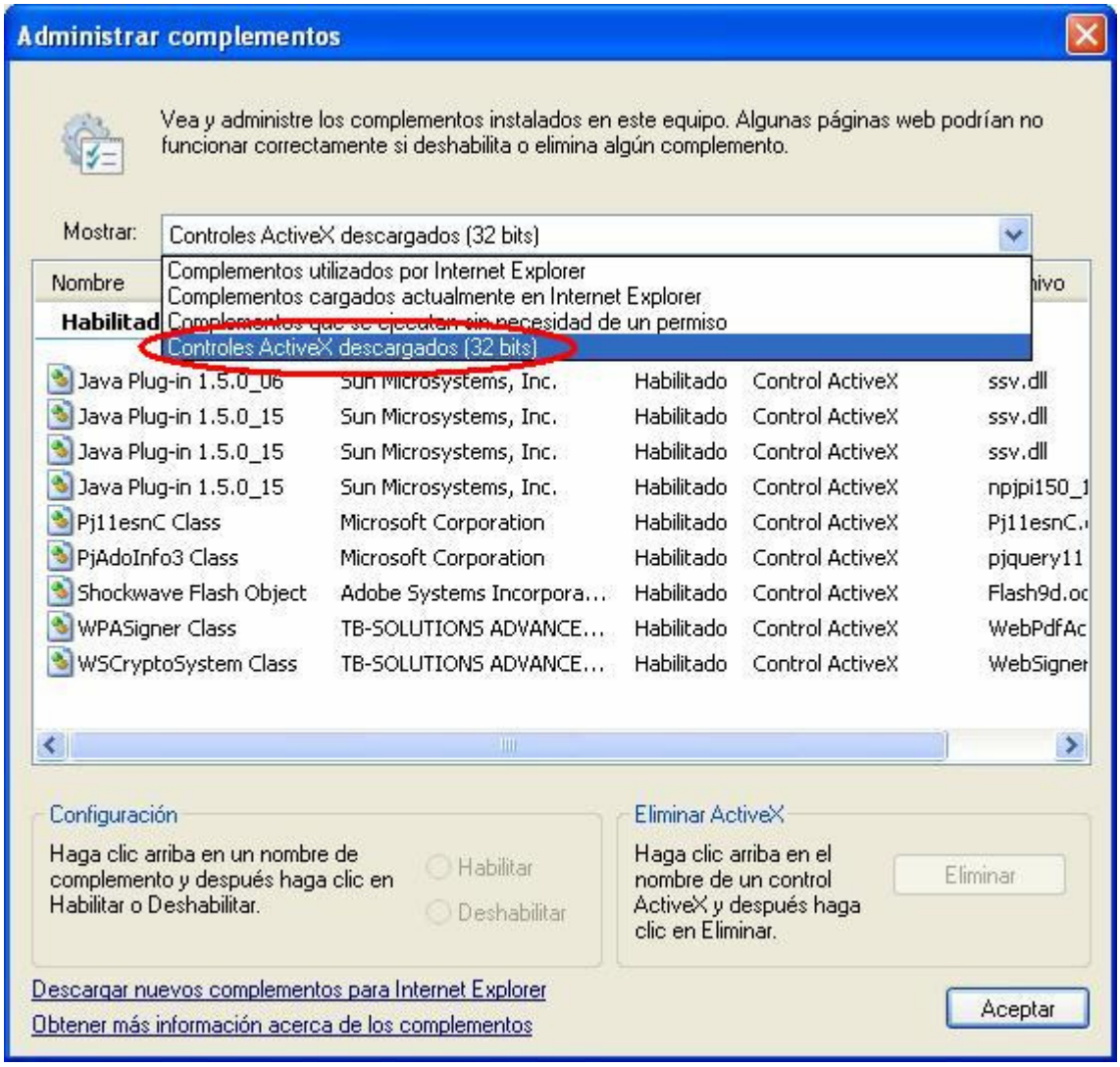
Si se desea desinstalar el componente se deberán seguir los siguientes pasos (Las pantallas y opciones concretas pueden variar según la versión del sistema operativo, XP, Vista, pero serán similares):

- Cierre todas las ventanas del navegador y cualquier aplicación que esté utilizando WebSigner ActiveX (**es muy importante que WebSigner no esté siendo usado**).

- Abra el navegador y vaya a Pestaña “Herramientas” → “Opciones de Internet” → Pestaña “Programas” → Botón “Administrar complementos”:

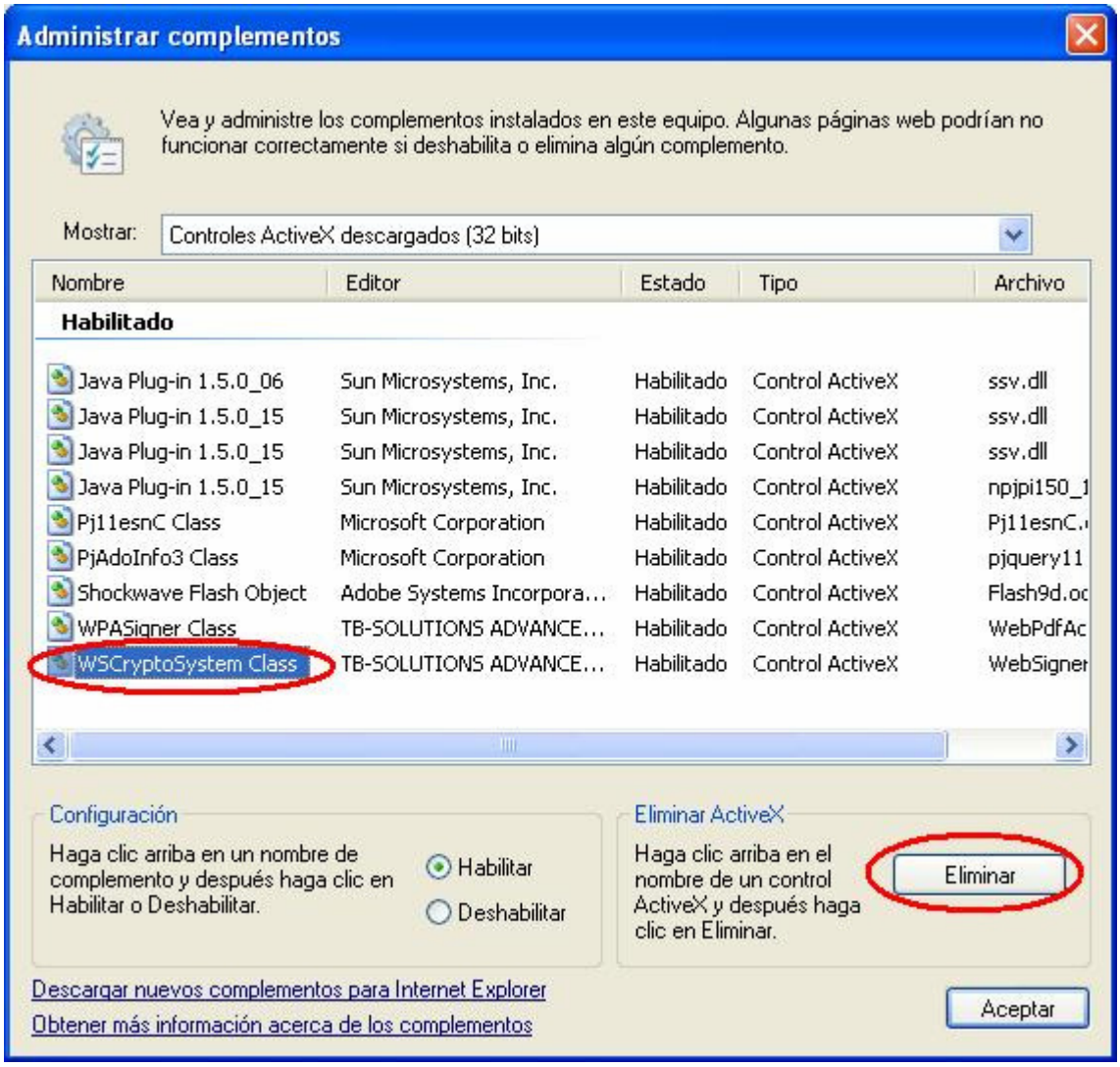


- En la Combo Box “Mostrar” escoja la opción “Controles ActiveX descargados (32 bits):

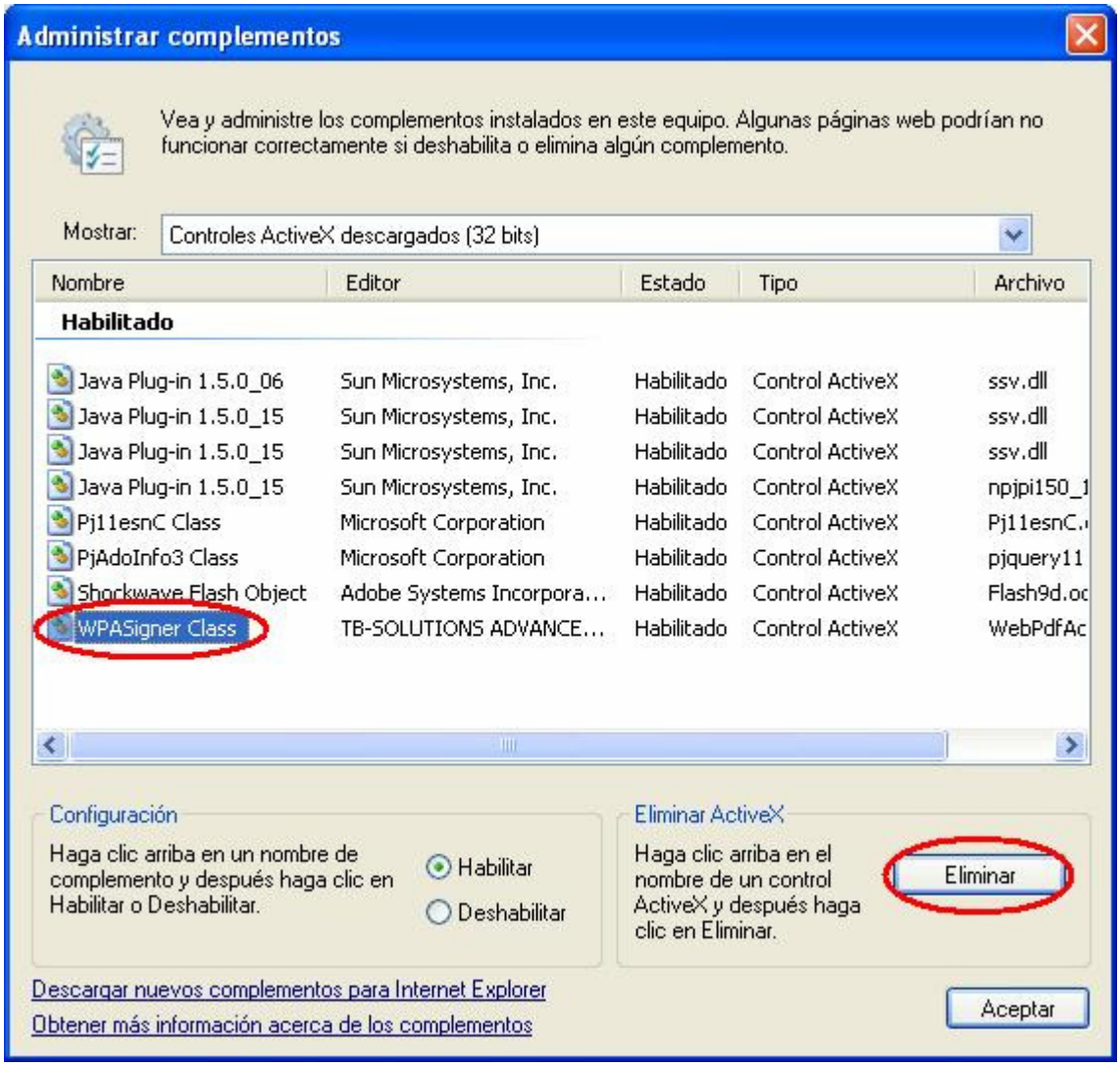


- Websigner ActiveX se compone de dos componentes, uno que es el propio componente en sí y otro que es el encargado de la firma en formato propietario de Adobe, vamos a eliminar ambos componentes, para ello:

  - ✓ Seleccionamos el componente de nombre “WSCryptoSystem Class” y pulsamos el botón “Eliminar”:



- ✓ Seleccionamos el componente “WPASigner Class” y pulsamos el botón “Eliminar”:

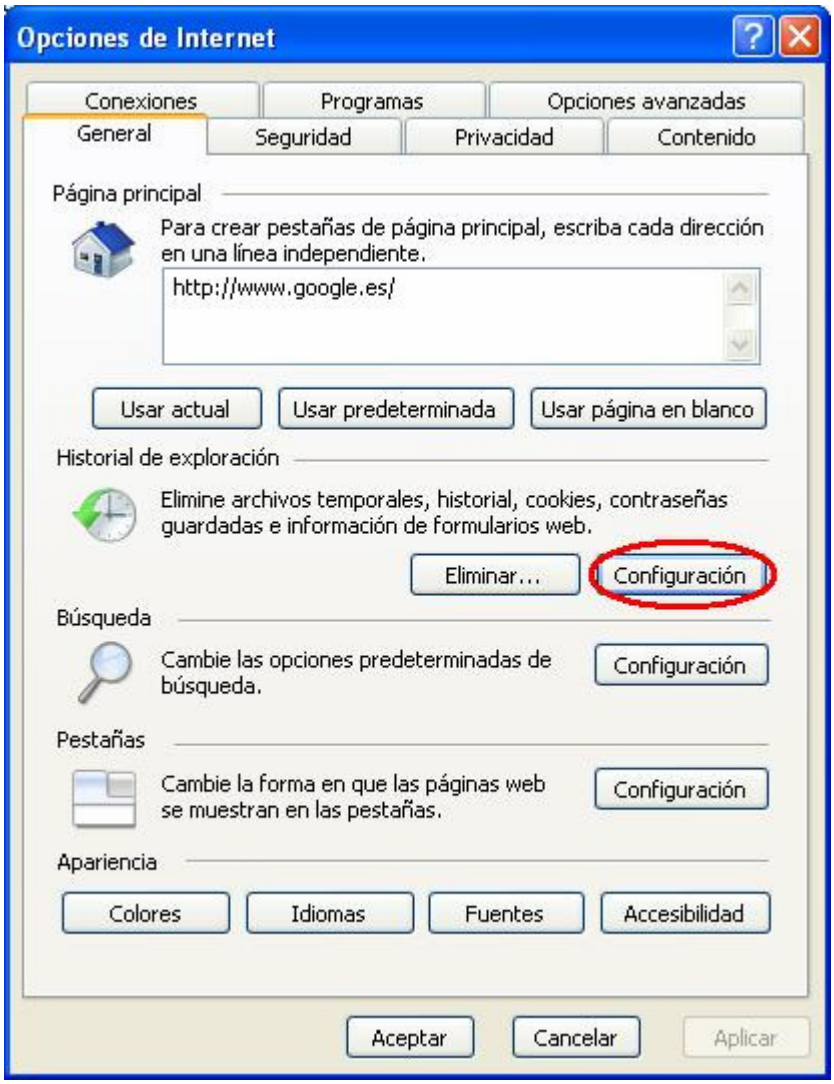


- Eliminar manualmente la carpeta "LastGood" que esta ubicada en "C:\WINDOWS", esta carpeta contiene una copia de información y librerías relativas al último WebSigner ActiveX instalado. Esta carpeta es exclusiva del componente WebSigner ActiveX por lo que puede eliminarla con la total tranquilidad de que no esta eliminando nada que no sea del componente.

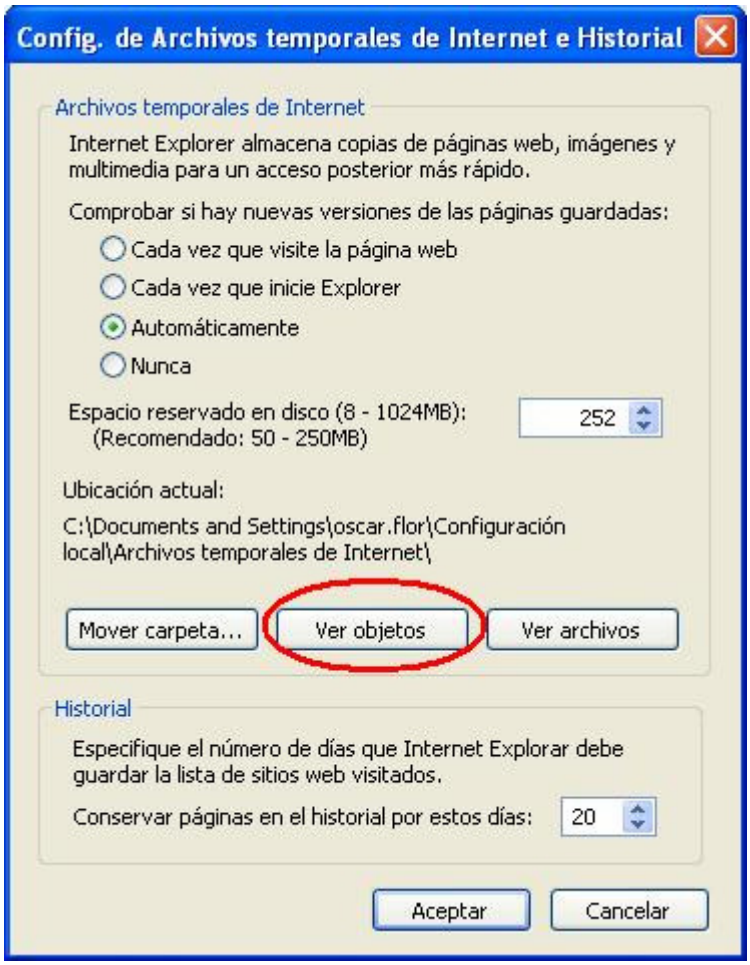
- Cierre el navegador.

Con los pasos anteriores realmente ya hemos acabado la eliminación del componente, ahora vamos a verificar que efectivamente el componente ya no aparece, para ello:

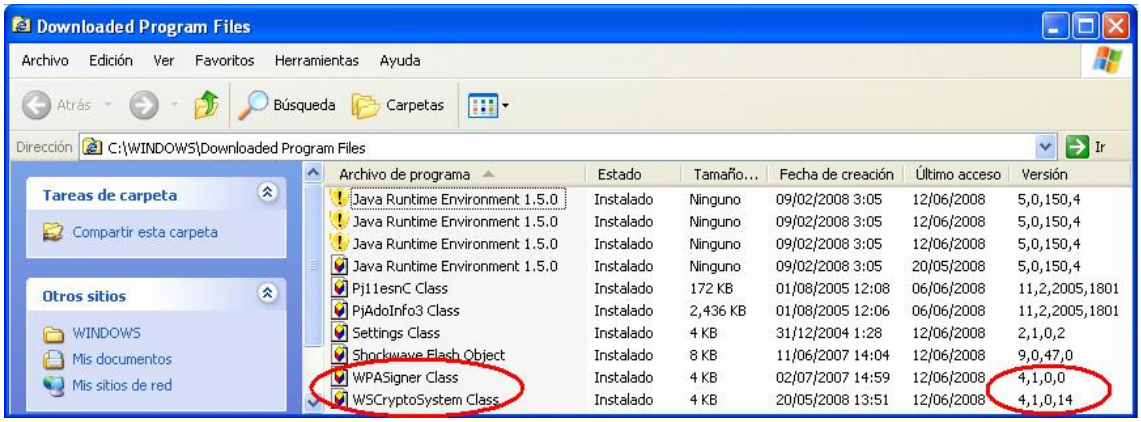
- Abra el navegador y vaya a Pestaña "Herramientas" → "Opciones de Internet" → Pestaña "General" → Botón "Configuración":



- Botón “Ver objetos”:



- En la ventana que se abre no deberían aparecer ni “WSCryptoSystem Class” ni “WPASigner Class”, se adjunta una captura donde si aparecen aunque el objetivo es reflejar lo que no debe aparecer, se puede observar también en la captura que cuando si tenemos los componentes se puede ver desde aquí si la versión que tenemos es la que deberíamos tener (cuando nos distribuyen el componente nos deben indicar que versión se nos esta distribuyendo):



- La última comprobación de que el componente WebSigner ActiveX ha sido eliminado correctamente es comprobar que la carpeta “WebSigner” dentro de la ruta “C:\Windows\System32” esta vacía.

3.3.1. Problemas durante la desinstalación

3.3.1.1. Permisos

En caso de querer desinstalar el componente se puede tener problemas en caso de no tener permisos de administrador de la maquina como en la instalación.

3.3.1.2. Borrado mientras están cargados

Un problema típico se debe a tener cargado el componente al intentar borrar los archivos, cierre el navegador y proceda según lo explicado en el apartado de desinstalación.

Según versiones de Internet Explorer avisa de que no se han podido borrar todos los ficheros o al recargar la página se siguen mostrando los certificados.

El resultado en este caso será equivalente a una mala instalación.

3.3.1.3. Desinstalación parcial

Al desinstalar el componente se borran todos los ficheros pero se sigue cargando el componente, se puede apreciar desde la ficha de habilitar/deshabilitar componentes.

Hay que proceder a una desinstalación total habilitando todo el componente y eliminando además desde la ficha de componentes.

(Ver punto 2.3 Desinstalación)

En caso de que siguiera sin desinstalarse bien se deberían borrar entradas del registro.

IMPORTANTE: Se debe hacer una copia de seguridad del registro antes de modificarlo. **Esta opción debe evitarse a ser posible.**

Puede ser que el componente al ser eliminado, se quede aun registrado (ocurre al intentar eliminar el componente teniendo en uso el mismo). Para poder volver a instalarlo correctamente se debe eliminar en el registro de Windows (regedit en ejecutar) la clave correspondiente. Para encontrarla ir a: HKLM/SOFTWARE/Classes/Interface . En esta clave se encuentra nuestro componente. Para eliminarlo usaremos la opción “Buscar” en esa carpeta y buscaremos por WSCryptoSystem. Borraremos la clave que contiene el resultado de la busqueda inmediatamente inferior a Interface. Tendrá un aspecto similar a: “{E0D41DA6-259F-36BA-A781-CE2BC08C61EB}”.

3.4. Problemas con versiones concretas del navegador:

3.4.1. Internet Explorer 7

Internet Explorer 7 es más restrictivo en cuanto a temas referentes a seguridad que sus versiones predecesoras.

Dado que los problemas que esto ocasiona no son de este componente sino de cualquiera de estas características se deja a continuación un link de la página oficial del servicio de certificación Ceres de la Fabrica Nacional de Moneda y Timbre, en dicho link se describen los pasos a seguir para que funcione:

http://www.cert.fnmt.es/index.php?cha=cit&sec=4&page=186&lang=es

3.4.2. Internet Explorer 7 en Windows Vista

Internet Explorer 7 es más restrictivo en cuanto a temas referentes a seguridad que sus versiones predecesoras, y mas aún cuando el sistema operativo es un Windows Vista.

Dado que los problemas que esto ocasiona no son de este componente sino de cualquiera de estas características se deja a continuación un link de la página oficial del servicio de certificación Ceres de la Fabrica Nacional de Moneda y Timbre, en dicho link se describen los pasos a seguir para que funcione:

http://www.cert.fnmt.es/index.php?cha=cit&sec=4&page=186&lang=es

3.4.3. Internet Explorer 8

Internet Explorer 8 se comporta de la misma manera que Internet Explorer 7, por lo que se aplica lo dicho las secciones anteriormente comentadas.

4. LIMITACIONES

- En la generación de firma en formato PKCS#7, CMS o CAdES, no tiene sentido:
    - Añadir un firmante detached a algo ya firmado.
- En la generación de firma en formato CAdEs o XAdES, no tiene sentido:
    - Añadir un firmante de un subtipo (BES, EPES) distinto a los subtipos de los firmantes ya existentes.
    - No pueden existir varios firmantes CAdES-EPES o XAdES-EPES en paralelo ni en secuencial que tengan diferentes políticas, es decir, todas las firmas CAdES-EPES/XAdES-EPES de un objeto firmado deben tener la misma política.
- En la generación de firma en formato XMLDSig, no tienen sentido los siguientes tipos de firma:
    - Firma detached y enveloped. La firma detached siempre debe ser enveloping.
    - Firma múltiple secuencial enveloped. La firma múltiple secuencial debe ser enveloping.
    - Firma múltiple paralela enveloping. La firma múltiple paralela debe ser enveloped.
    - Firma múltiple secuencial de una parte del documento, y no del documento completo. Cuando se añade un firmante de forma secuencial a algo ya firmado, no puede firmarse solamente una parte del xml, debe firmarse el xml entero, ya que se está firmando el resultado de una firma anterior.
    - Añadir un firmante detached. Cuando se añade un firmante al resultado de una firma anterior, debe ser firma attached, ya que la firma detached en el caso del XMLDSig firma un documento accesible por una URI, y se está firmando una firma anterior, no un documento.
    - Añadir firmante en paralelo al resultado de una firma enveloping anterior.
- Existe alguna limitación por un problema de rendimiento o limitación de hardware que proviene de alguna librería utilizada:
    - Limitación de la librería XSEC en el rendimiento de ciertas transformaciones XPath (más concretamente la limitación es de la librería XALAN).
    - XSEC es una la librería encargada de generar y procesar una parte importante de la firma XML.

- La librería XALAN es la encargada de realizar las transformaciones XSLT y XPath a través de XSEC.

- Se detecta la ralentización del proceso de firma al realizar la transformación not(ancestro-or-self) cuando se declara algún namespace en un documento con una cantidad elevada de nodos en un documento XML.

- Al insertar una firma XML en un nodo del documento que tenga un namespace por defecto se debe tener en cuenta lo siguiente a la hora de seleccionarlo por una ruta XPath:

  - Para XPath 1.0 (XSLT 1.0) no está permitida la búsqueda a un nodo que tenga un namespace por defecto (es decir, sin prefijo), ya que se toma el namespace como nulo en vez del asignado.

  - Las versiones XalanC y XalanJ utilizadas son procesadores XSLT 1.0, por lo que no se permiten las búsquedas anteriormente citada.

  - Para obtener este tipo de nodos con namespace por defecto es necesario utilizar una expresión XPath del siguiente tipo: *[local-name()="node"]

  - Al utilizar la función local-name() se debe tener especial cuidado cuando tengamos nodos con mismo nombre pero diferente namespace, ya que con esta función no se distinguen los diferentes namespaces y prefijos.

    Nota: Esto afecta a los formatos XAdES y XMLDSig.

- No soporta la lectura y firma de documentos PDF de las siguientes versiones: 1.5 y superiores sí son PDF's dinámicos no compatibles con la versión 1.4, es decir, al generarlos contienen internamente "Cross Reference Streams" (la referencia del objeto está implícita en el propio objeto cuando se declara) en vez de tener una "Cross Reference Table" (Tabla que contiene la referencia de todos los objetos internos del PDF).

- No soporta cifrado y descifrado con el algoritmo AES en WindowsXP e inferiores.

- En formato XMLDSig sólo soporta (para firmar y para verificar) el algoritmo de hash SHA-1.

- El algoritmo de hash SHA-256 sólo es soportado en Windows 2003 y Windows Vista (y posteriores).

- En formato XMLDSig, para firmar partes de documentos, sólo reconoce como identificadores los atributos Id. Los atributos ID, id o cualquiera de ellos con un prefijo delante no los reconoce, salvo que el XML lleve incorporado el DTD e indique estos atributos como identificadores.

- Los encodings soportados para formatos XML son: ASCII, UTF-8, UTF-16 (Big/Small Endian), UCS4 (Big/Small Endian), EBCDIC code pages IBM037, IBM1047 and IBM1140 encodings, ISO-8859-1 (aka Latin1) and Windows-1252. No se incluye soporte ICU para tener soporte para más encodings debido al elevado tamaño de esta librería que debe ser incluida en el CAB del componente WebSigner ActiveX. La inclusión del archivo icudt32.dll (9 MB) dentro del archivo .cab causa que se genere un CAB de 7 MB en vez de los 2,70 MB actuales.

- Tabla de relación de velocidades con el tamaño del documento a firmar:

- IMPORTANTE: Estos tiempos han sido obtenidos bajo WindowsXP SP2 en una máquina con 2 GB de RAM y 1,6 GHz doble núcleo. El documento XML firmado tiene aproximadamente 60000 nodos. Estas mediciones variarán según la máquina y el entorno dónde se estén realizando las firmas, pudiendo variar en función de la capacidad de procesado del equipo utilizado.

	XMLDsig / XAdES	
Tamaño de documento	Enveloped	Enveloping
1500 KB (6000 nodos)	2 min	10 sg
PKCS7 / CMS /CAdES (Presentan tiempos similares en secuencial y en paralelo)		
Signing time 1MB : 0.281000 sg Signing time 2MB : 0.578000 sg Signing time 4MB : 1.156000 sg Signing time 8MB : 2.328000 sg Signing time 16MB : 4.593000 sg Signing time 32MB : 9.138000 sg		

- Existe una limitación de tamaño en las variables javascript. (En las pruebas realizadas se observan problemas a partir de 4 ó 7MB en función del equipo) JavaScript. Por este motivo, no es posible asignar 4MB en Base64 a una variable JavaScript.

- Esta limitación aplica a las funciones cuyo resultado se debería "almacenar" en una variable. (getFile, firma attached, etc.).

- Para evitar esta limitación a partir de la versión 5.6.0.3, se dispone de funciones que realizan operaciones “fichero a fichero”, donde el tamaño máximo del fichero depende de la memoria asignada al componente ActiveX. Estas funciones incluyen en su nombre la cadena “*FileToFile*”, salvo la verificación de ficheros de gran tamaño que se puede realizar con el método: “*verifyFileOneStep*”. En el manual de Integración de Websigner se enumeran estas funciones y se aporta la información necesaria para su uso.