



Consejería de Hacienda y Administración Pública

Cliente 3.1.0 @firma v5: Preguntas, problemas y respuestas

Página 2 de 15

1	Sobre el cliente de firma	4
2	Entornos soportados.....	4
3	Matriz de compatibilidad (Extensión Junta de Andalucía) .	5
4	Compatibilidad nativa del cliente de firma	6
5	Sobre la matriz de compatibilidad	7
6	Problemas con el instalador.....	8
7	Problemas con el cliente de firma.....	12
8	Recomendaciones.....	15

I Sobre el cliente de firma

¿Qué es el cliente de firma?

El cliente de firma es una aplicación distribuida de forma gratuita por la Junta de Andalucía que se ejecuta en el PC del usuario. Está basado en applets Java, por lo que se requiere una máquina virtual Java para su funcionamiento. Está compuesto por un instalador y el propio cliente de firma.

Para garantizar la autenticidad e integridad de este software, éste se distribuye firmado digitalmente por la Junta de Andalucía.

Puede obtenerse en la zona de descargas privadas de la web de soporte de administración electrónica.

¿Para qué se utiliza el cliente de firma?

Básicamente el cliente permite identificarnos de forma segura y firmar documentos y formularios utilizando certificados electrónicos reconocidos (FNMT-RCM, DNI electrónico, etc.)

2 Entornos soportados

¿Qué entornos (sistema operativo, navegador y máquina virtual Java) son soportados por el cliente de @firma?

Actualmente el cliente de @firma v3.1.0 soporta los sistemas operativos Microsoft Windows 2000 SP4, XP SP3, Vista SP2 y 7; así como Guadalinex v5, v6, v7 y Ubuntu 9.04, 9.10, 10.04 y 10.10.

En cuanto a navegadores, para entornos Windows se soportan los siguientes: Internet Explorer 6, 7 y 8, Mozilla Firefox 2.0.0.x, 3.0.x, 3.5.x y 3.6.x, Google Chrome.

Para entornos Linux, en función de la disponibilidad en el repositorio oficial de la distribución, está soportado el navegador Mozilla Firefox en sus versiones 2.0.0.x, 3.0.x, 3.5.x, 3.6.x y Chromium.

En cuanto a las máquinas virtuales se requiere disponer de JRE 1.5 (1.5.0_22 o superior) o JRE 1.6 (1.6.0_18 o superior).

3 Matriz de compatibilidad (Extensión Junta de Andalucía)

El objeto de esta tabla consiste en mostrar la compatibilidad del cliente de @firma v3.1.0 con la operación de firma de ficheros de la extensión de @firma.

En las pruebas de compatibilidad se han tenido en cuenta las siguientes configuraciones:

Sistema Operativo	Navegadores							
	IE6	IE7	IE8	Firefox 2.0	Firefox 3.0	Firefox 3.5	Firefox 3.6	Chrome/Chromium
Windows 2000 SP4	JRE 1.5 JRE 1.6	ND	ND	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	ND
Windows XP SP3	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6
Windows Vista SP2	ND	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6
Windows 7	ND	ND	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6
Guadalinux v5	ND	ND	ND	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	ND	ND	JRE 1.6
Guadalinux v6	ND	ND	ND	ND	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	ND	JRE 1.6
Guadalinux v7	ND	ND	ND	ND	ND	ND	JRE 1.6	JRE 1.6
Ubuntu 9.04	ND	ND	ND	ND	ND	JRE 1.5 JRE 1.6	JRE 1.5 JRE 1.6	JRE 1.6
Ubuntu 9.10	ND	ND	ND	ND	ND	ND	JRE 1.6	JRE 1.6
Ubuntu 10.04	ND	ND	ND	ND	ND	ND	JRE 1.6	JRE 1.6
Ubuntu 10.10	ND	ND	ND	ND	ND	ND	JRE 1.6	JRE 1.6

Leyenda

ND: Configuración no disponible.

NS: La configuración no ha superado las pruebas de compatibilidad.

OK: Se ha verificado la compatibilidad de la configuración.

Notas

- Para distribuciones Linux se ha probado con las combinaciones de JRE y navegador instalables desde el repositorio oficial de la distribución. El resto de combinaciones se indican como no disponible.
- La matriz de compatibilidad detallada puede consultarse en el documento “Matriz de compatibilidad del cliente de firma de ficheros 3.1.0 de @firma v5 (Servicios de la Extensión JA)”.

4 Compatibilidad nativa del cliente de firma

		WINDOWS CAPI					
		IE Explorer 6 o sup.	Firefox 2 a 3.5	Firefox 3.6	Chrome 3 o sup.	Apple Safari 4	Opera 10
JRE 1.5_22 32 Bits	Windows 2000, XP, Vista (32 Bits)						
	Windows 7, Server 2003, Server 2008						
	Windows XP x64 (64 bits)						
JRE 1.6_18 32 Bits	Windows x86 (32 bits) [todos]						
	Windows x64 (64 bits) [todos]						
JRE 1.6_18 64 Bits	Windows x64 (64 bits) [todos]						
JRE 1.7 b75 [todos]	Windows [todos]						

		NSS					
		IE Explorer 6 o sup.	Firefox 2 a 3.5	Firefox 3.6	Chrome 3 o sup.	Apple Safari 4	Opera 10
JRE 1.5_22 32 Bits	Windows (32 y 64 bits) [todos]						
	Linux 2.6 x86 (32 bits)						
	Solaris 10 x86 (32 bits)						
	Mac OS X 10.x (64 bits)						
JRE 1.6_18 32 Bits	Windows (32 y 64 bits) [todos]						
	Linux 2.6 x86 (32 bits)						
	Solaris 10 x86 (32 bits)						
	Solaris 10 x64 (64 bits)						
	Solaris 10 SPARC (64 bits)						
JRE 1.6_18 64 Bits	Windows 64 Bits (todos)						
	Linux 2.6 x64 (64 bits)						
	Solaris 10 x64 (64 bits)						
	Solaris 10 SPARC (64 bits)						
JRE 1.7 b75 [todos]	[todos]						

		Apple Mac OS X KeyRing (Llavero de Mac OS X)					
		IE Explorer 6 o sup.	Firefox 2 a 3.5	Firefox 3.6	Chrome 3 o sup.	Apple Safari 4	Opera 10
Java for MacOS X 10.6 u2	Mac OS X 10.6						
Java for MacOS X 10.5 u7	Mac OS X 10.5						

Código de colores:

- Verde = Compatible, Rojo = No compatible, Gris = No aplica, Blanco = No probado

CAPI es el almacén central de los sistemas operativos Windows (usado por Internet Explorer, Google Chrome, Apple Safari y Opera en este sistema operativo), mientras que NSS es el almacén propio del navegador Mozilla / Firefox, que lo usa en cualquier sistema operativo y se establece como almacén central de los sistemas Linux / UNIX. Mac OS X KeyChain (llavero de Mac OS X) es el almacén central del sistema operativo Mac OS X, y es usado por todos los navegadores en este sistema operativo excepto Mozilla / Firefox (por defecto). Ya que no es posible acceder al almacén de certificados de Mozilla en Mac OS X debido a la incompatibilidad entre arquitecturas, el cliente @firma utilizará el llavero de Mac OS X cuando se ejecute en Mozilla Firefox desde este sistema operativo.

Nota: Puede obtener más información sobre compatibilidad nativa en el documento “Manual del integrador del cliente”.

5 Sobre la matriz de compatibilidad

La configuración del equipo del usuario no aparece en la matriz de compatibilidad, ¿es posible realizar la firma en dicho equipo?

La matriz de compatibilidad recoge el resultado de un conjunto de pruebas realizadas a las configuraciones más comunes utilizadas por los usuarios. Que una configuración concreta no aparezca en la matriz no implica que no funcione correctamente con el cliente de firma.

Una firma realizada con una configuración que aparece como no soportada en la matriz de compatibilidad, ¿es incorrecta?

Una configuración se considera no soportada cuando ocurre alguna de las siguientes circunstancias:

- Ha fallado algunas de las pruebas realizadas con dicha configuración.
- El tiempo de respuesta del componente en dicha configuración es demasiado elevado.
- Es necesario realizar una modificación significativa al sistema del usuario que invalida dicha configuración para la prestación de soporte. Por ejemplo la actualización de librerías en Linux que no se encuentran disponibles desde los repositorios oficiales de la distribución.

Dichos factores descartan una configuración para la prestación de soporte, pero no necesariamente implican que el componente funcione de manera incorrecta. Son los servicios de la plataforma @firma quienes determinan la validez de la firma realizada con el componente.

Compatibilidad nativa y compatibilidad con la extensión de la Junta de Andalucía, ¿por qué se diferencian?

En las pruebas de validación del cliente de firma con la extensión de la Junta de Andalucía se tienen en cuenta escenarios de uso y configuraciones que no se contemplan en la matriz de compatibilidad original del componente. Por otra parte la aparición de nuevas versiones de los componentes que forman una configuración obliga a la revisión de la matriz de compatibilidad inicial.

¿Qué pruebas se realizan para la validación de cada configuración?

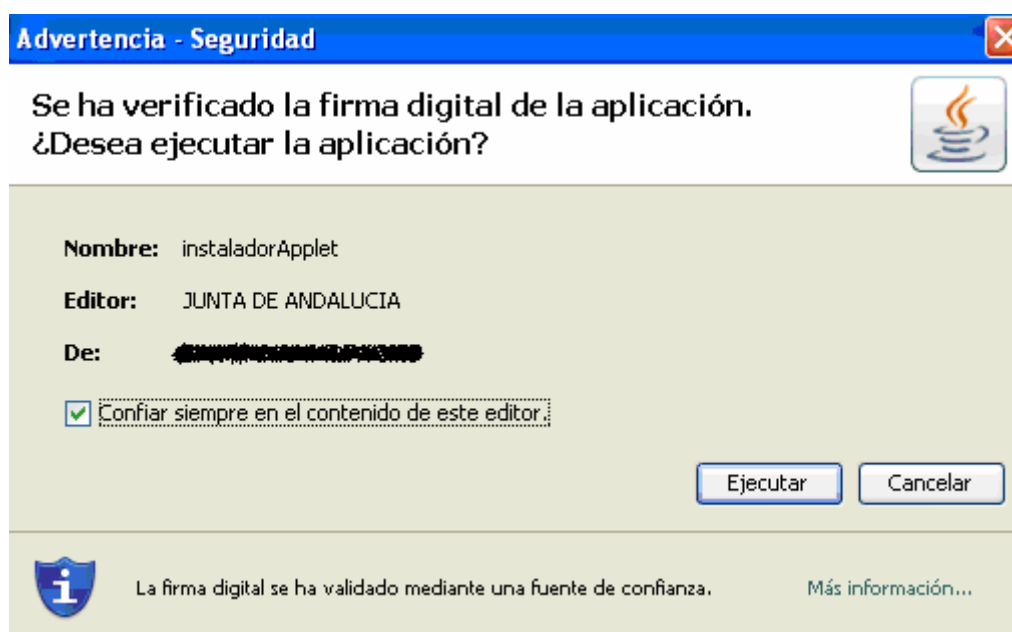
Para validar una configuración se tienen en cuenta entre otras las pruebas que se comentan a continuación.

- Firma de ficheros en aplicación de prueba integrada con la extensión de la Junta de Andalucía con certificado FNMT 1024 y 2048 bits, certificados de prestador distinto a FNMT, DNI electrónico, certificado en tarjeta FNMT, APE y tarjeta Siemens.
- Funcionamiento en aplicaciones reales: Port@firmas.

6 Problemas con el instalador

Durante la instalación del cliente aparece el error en la consola Java “SEVERE: No ha podido determinarse el directorio de usuario para la configuración del cliente”

Tanto el instalador como el cliente de firma requieren privilegios para realizar operaciones que por defecto no son permitidos por la máquina virtual Java. Para permitir dichas operaciones el usuario debe confiar en la firma del cliente.



Si el usuario dispone de Java 1.5 o 1.6 instalado en su ordenador y pulsa el botón “Cancelar” el instalador no dispondrá de los privilegios necesarios para su funcionamiento, provocando el error indicado en el párrafo anterior.

Este error puede venir acompañado de otros mensajes en la consola Java similares a los que se muestra a continuación:

```
java.security.PrivilegedActionException: java.lang.reflect.InvocationTargetException
    at java.security.AccessController.doPrivileged(Native Method)
    at sun.plugin.liveconnect.SecureInvocation$2.run(Unknown Source)
    at java.security.AccessController.doPrivileged(Native Method)
    at sun.plugin.liveconnect.SecureInvocation.CallMethod(Unknown Source)
    at sun.plugin.liveconnect.SecureInvocation.access$300(Unknown Source)
    at sun.plugin.liveconnect.SecureInvocation$CallMethodThread.run(Unknown Source)
Caused by: java.lang.reflect.InvocationTargetException
```



```

at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
at java.lang.reflect.Method.invoke(Unknown Source)
at sun.plugin.javascript.invoke.JSInvoke.invoke(Unknown Source)
at sun.reflect.GeneratedMethodAccessor4.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
at java.lang.reflect.Method.invoke(Unknown Source)
at sun.plugin.javascript.JSCClassLoader.invoke(Unknown Source)
at sun.plugin.liveconnect.PrivilegedCallMethodAction.run(Unknown Source)
... 6 more

```

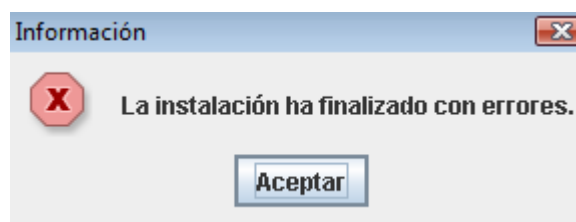
Caused by: java.security.AccessControlException: access denied (java.io.FilePermission JA3_I_0\afirma5_coreV3.jar read)

```

at java.security.AccessControlContext.checkPermission(Unknown Source)
at java.security.AccessController.checkPermission(Unknown Source)
at java.lang.SecurityManager.checkPermission(Unknown Source)
at java.lang.SecurityManager.checkRead(Unknown Source)
at java.io.File.exists(Unknown Source)
at es.gob.afirma.misc.AOBootUtil.existFile(Unknown Source)
at es.gob.afirma.install.Installer.isAlreadyInstalled(Unknown Source)
at es.gob.afirma.install.AfirmaBootLoader$6.run(Unknown Source)
at java.security.AccessController.doPrivileged(Native Method)
at es.gob.afirma.install.AfirmaBootLoader.isInstalado(Unknown Source)
... 16 more

```

Error “La instalación ha finalizado con errores”



La correcta instalación del cliente de firma puede requerir que el usuario disponga de permisos de escritura en la carpeta de la máquina virtual Java de su equipo. Dicho requerimiento depende de la construcción del cliente utilizada por la aplicación web y puede consultarse en la siguiente tabla.

Nota: Los ficheros en color rojo en ruta destino requieren privilegio de escritura para su instalación.

Windows		
Fichero	Paquete	Ruta destino
Java 5		
LITE		
afirma_5_java_5.jar		%JAVA_HOME%/lib/endorsed/afirma_5_java_5.jar
LITE_j5_afirma5_coreV3.jar		%HOME%/JA3_I_0/afirma5_coreV3.jar
LITE_j5_afirma5_coreV3.jar.pack.gz		
msvcr71.dll	msvcr71.zip	%LIBRARY_PATH%/msvcr71.dll
sunmscapi.dll	mscapi.zip	%JAVA_HOME%/bin/sunmscapi.dll
sunmscapi.jar	mscapi.jar.zip	%JAVA_HOME%/lib/ext/sunmscapi.jar
MEDIA		
afirma_5_java_5.jar		%JAVA_HOME%/lib/endorsed/afirma_5_java_5.jar
MEDIA_j5_afirma5_coreV3.jar		%HOME%/JA3_I_0/afirma5_coreV3.jar
MEDIA_j5_afirma5_coreV3.jar.pack.gz		
msvcr71.dll	msvcr71.zip	%LIBRARY_PATH%/msvcr71.dll
serializer.jar	xalan.zip	%JAVA_HOME%/lib/endorsed/serializer.jar
sunmscapi.dll	mscapi.zip	%JAVA_HOME%/bin/sunmscapi.dll
sunmscapi.jar	mscapi.jar.zip	%JAVA_HOME%/lib/ext/sunmscapi.jar
xalan.jar	xalan.zip	%JAVA_HOME%/lib/endorsed/xalan.jar
xercesImpl.jar	xalan.zip	%JAVA_HOME%/lib/endorsed/xercesImpl.jar
xml-apis.jar	xalan.zip	%JAVA_HOME%/lib/endorsed/xml-apis.jar
COMPLETA		
afirma_5_java_5.jar		%JAVA_HOME%/lib/endorsed/afirma_5_java_5.jar
COMPLETA_j5_afirma5_coreV3.jar		%HOME%/JA3_I_0/afirma5_coreV3.jar
COMPLETA_j5_afirma5_coreV3.jar.pack.gz		
msvcr71.dll	msvcr71.zip	%LIBRARY_PATH%/msvcr71.dll
serializer.jar	xalan.zip	%JAVA_HOME%/lib/endorsed/serializer.jar
sunmscapi.dll	mscapi.zip	%JAVA_HOME%/bin/sunmscapi.dll
sunmscapi.jar	mscapi.jar.zip	%JAVA_HOME%/lib/ext/sunmscapi.jar
xalan.jar	xalan.zip	%JAVA_HOME%/lib/endorsed/xalan.jar
xercesImpl.jar	xalan.zip	%JAVA_HOME%/lib/endorsed/xercesImpl.jar
xml-apis.jar	xalan.zip	%JAVA_HOME%/lib/endorsed/xml-apis.jar
Java 6		
LITE		
LITE_j6_afirma5_coreV3.jar		%HOME%/JA3_I_0/afirma5_coreV3.jar
LITE_j6_afirma5_coreV3.jar.pack.gz		
MEDIA		
MEDIA_j6_afirma5_coreV3.jar		%HOME%/JA3_I_0/afirma5_coreV3.jar
MEDIA_j6_afirma5_coreV3.jar.pack.gz		
COMPLETA		
COMPLETA_j6_afirma5_coreV3.jar		%HOME%/JA3_I_0/afirma5_coreV3.jar
COMPLETA_j6_afirma5_coreV3.jar.pack.gz		

Linux		
Fichero	Paquete	Ruta destino
Java 5		
LITE		
afirma_5_java_5.jar		\$JAVA_HOME/lib/endorsed/afirma_5_java_5.jar
LITE_j5_afirma5_coreV3.jar		\$HOME/JA3_I_0/afirma5_coreV3.jar
LITE_j5_afirma5_coreV3.jar.pack.gz		
MEDIA		
afirma_5_java_5.jar		\$JAVA_HOME/lib/endorsed/afirma_5_java_5.jar
MEDIA_j5_afirma5_coreV3.jar		\$HOME/JA3_I_0/afirma5_coreV3.jar
MEDIA_j5_afirma5_coreV3.jar.pack.gz		
serializer.jar	xalan.zip	\$JAVA_HOME/lib/endorsed/serializer.jar
xalan.jar	xalan.zip	\$JAVA_HOME/lib/endorsed/xalan.jar
xercesImpl.jar	xalan.zip	\$JAVA_HOME/lib/endorsed/xercesImpl.jar
xml-apis.jar	xalan.zip	\$JAVA_HOME/lib/endorsed/xml-apis.jar
COMPLETA		
afirma_5_java_5.jar		\$JAVA_HOME/lib/endorsed/afirma_5_java_5.jar
COMPLETA_j5_afirma5_coreV3.jar		\$HOME/JA3_I_0/afirma5_coreV3.jar
COMPLETA_j5_afirma5_coreV3.jar.pack.gz		
serializer.jar	xalan.zip	\$JAVA_HOME/lib/endorsed/serializer.jar
xalan.jar	xalan.zip	\$JAVA_HOME/lib/endorsed/xalan.jar
xercesImpl.jar	xalan.zip	\$JAVA_HOME/lib/endorsed/xercesImpl.jar
xml-apis.jar	xalan.zip	\$JAVA_HOME/lib/endorsed/xml-apis.jar
Java 6		
LITE		
LITE_j6_afirma5_coreV3.jar		\$HOME/JA3_I_0/afirma5_coreV3.jar
LITE_j6_afirma5_coreV3.jar.pack.gz		
MEDIA		
MEDIA_j6_afirma5_coreV3.jar		\$HOME/JA3_I_0/afirma5_coreV3.jar
MEDIA_j6_afirma5_coreV3.jar.pack.gz		
COMPLETA		
COMPLETA_j6_afirma5_coreV3.jar		\$HOME/JA3_I_0/afirma5_coreV3.jar
COMPLETA_j6_afirma5_coreV3.jar.pack.gz		

7 Problemas con el cliente de firma

Error en el proceso de firma con tarjeta Siemens

Durante la firma con un certificado almacenado en tarjeta Siemens aparece el mensaje de error 'Ocurrió un error generando la firma'. En la consola Java aparece una traza similar a alguna de las siguientes:

GRAVE: Error durante el proceso de firma: java.security.SignatureException: **Tipo especificado no es válido.**

GRAVE: Ocurrió un error generando la firma PKCS#7: es.gob.afirma.exceptions.AOException: Error durante el proceso de firma: java.security.SignatureException: **Invalid type specified.**

GRAVE: Ocurrió un error generando la firma PKCS#7: es.gob.afirma.exceptions.AOException: Error durante el proceso de firma: java.security.SignatureException: **Tipo especificado no es válido.**

Para solucionar el problema es necesario actualizar el driver de la tarjeta Siemens a HiPath Security Card API V3.2 o superior.

Error al iniciar el proceso de firma con Java 1.5.

Al intentar firmar con el cliente de firma en un equipo con Java 1.5 aparece el siguiente mensaje de error en la consola Java

GRAVE: Error inicializando la firma, clave de tipo: sun.security.mscapi.RSAPrivateKey

30-jul-2010 13:28:42 es.gob.afirma.signers.AOCMSSigner sign

GRAVE: Ocurrió un error generando la firma PKCS#7: es.gob.afirma.exceptions.AOException: Error al obtener la clave de firma para el algoritmo 'SHA1withRSA':

java.lang.NoSuchMethodError: sun.security.rsa.RSAKeyFactory.checkKeyLengths(ILjava/math/BigInteger;II)V

30-jul-2010 13:28:42 es.gob.afirma.cliente.SignApplet\$18 run

GRAVE: Ocurrió un error generando la firma PKCS#7: es.gob.afirma.exceptions.AOException: Ocurrió un error generando la firma PKCS#7

El error se resuelve actualizando la máquina virtual Java del equipo del usuario a JRE 1.5.0_22 o superior.

Posicionamiento de los cuadros de diálogo del cliente

Los cuadros de diálogo del cliente de firma pueden aparecer en una posición de pantalla inadecuada. El problema tiene su origen en el modo de despliegue de la librería deployJava.js. Esta librería

provoca que se instancie el cliente “a la altura” de la etiqueta donde se inserta la llamada a la función “cargarAppletFirma()” y es dicha posición la que se utiliza para localizar las ventanas modales.

Para corregir la posición de la ventana es necesario reubicar el código de llamada a la función “cargarAppletFirma()” en la página que instancia el cliente.

Error en el proceso de firma: “Ocurrió un error generando la firma PKCS#7”

Al realizar una firma aparece el mensaje de error “Ocurrió un error generando la firma PKCS#7” y en la consola Java la traza

```
GRAVE: Ocurrió un error generando la firma PKCS#7: java.lang.NoSuchMethodError:
org.bouncycastle.asn1.ASN1InputStream.<init>([B)V
06-oct-2010 9:53:53 es.gob.afirma.cliente.SignApplet$18 run
GRAVE: Ocurrió un error generando la firma PKCS#7:
es.gob.afirma.exceptions.AOException: Ocurrió un error generando la firma PKCS#7
```

Dicho mensaje de error suele tener su origen en librerías instaladas por terceras aplicaciones en la máquina del usuario que interfieren con las utilizadas por el cliente de firma.

Para estudiar el problema deberá crear una incidencia en el sistema de gestión de incidencias técnicas de administración electrónica (iTracker) disponible en la URL

<https://ws025.juntadeandalucia.es/itracker/inicio.jsp>

Aviso de certificado caducado en selección de certificado vigente

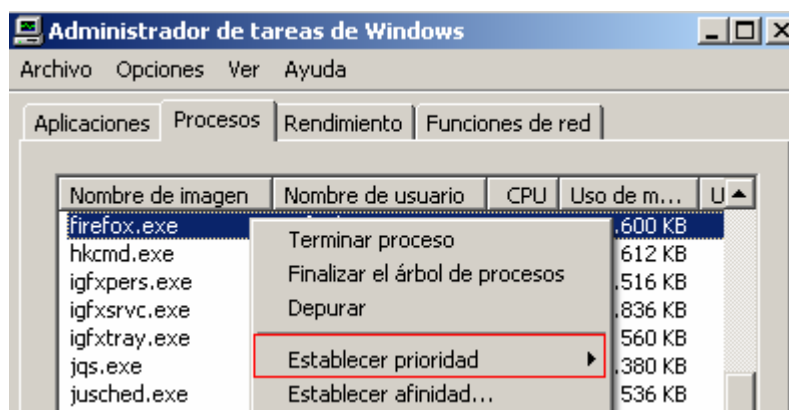
El cliente de firma visualiza un mensaje de advertencia cuando detecta que el certificado seleccionado para realizar una operación de firma está caducado respecto a la hora local del equipo en el que se ejecuta el componente. En equipos en los que se encuentran instalados un certificado caducado y su renovación puede ocurrir que el mensaje de advertencia se presente tras la selección del certificado vigente.

Para evitar dicho problema se recomienda configurar el parámetro showExpiredCertificates del cliente con el valor false para que no se presenten y validen certificados caducados en el cuadro de diálogo de selección de certificados.

Problema de rendimiento con Mozilla Firefox 3.6 en Windows

Se han detectado problemas de rendimiento en el funcionamiento del cliente de firma en algunas aplicaciones que integran dicho componente en equipos con Windows y Firefox 3.6. Dicho problema tiene su origen en un consumo excesivo de CPU por parte del navegador durante la ejecución de código Javascript.

Es posible acelerar la ejecución del cliente de firma reduciendo la prioridad del proceso del navegador (firefox.exe) en el administrador de tareas de Windows. Para acceder al administrador es necesario hacer clic con el botón derecho del ratón sobre la barra de tareas y seleccionar la opción 'Administrador de tareas'. En la ventana que aparezca hacer clic en la pestaña 'Procesos', seleccionar en la columna 'Nombre de imagen' el proceso firefox.exe y hacer clic con el botón derecho. En el menú que aparezca seleccionar la opción 'Establecer prioridad' y elegir un valor inferior al actual.



Firma con DNI electrónico en Linux

La firma electrónica con el cliente 3.1.0 en distribuciones Linux se soporta únicamente para la versión 1.4.6 de los controladores del DNLe, distribución Ubuntu Jaunty Jackalope. Puede obtener tanto el software como las instrucciones de instalación en el área de descargas del portal oficial del DNLe (<http://www.dnielectronico.es/>).

Para el correcto funcionamiento del cliente tras la instalación es necesario que el parámetro lock_login del fichero de configuración /etc/opensc/opensc.conf se encuentre no comentado y con el valor false. Puede obtener más información sobre la configuración de este parámetro en el documento "Guía de incidencias del cliente".

Compatibilidad con tarjetas CERES en Linux

Existe un bug en las librerías OpenSC-CERES versión 2.3 que se distribuyen en el área de descarga de software del portal CERES que impide la firma con tarjetas FNMT-RCM y APE en Linux. Se recomienda no utilizar el cliente de firma con las tarjetas comentadas hasta que se publique una actualización que resuelva el problema.

Otras incidencias

Puede obtener información sobre otras incidencias relacionadas con el uso del cliente de firma 3.1.0 en el documento “Guía de incidencias del cliente”.

8 Recomendaciones

Configuración de Chromium y Google Chrome en Linux

Como se indica en el documento “Guía de uso del cliente” apartado “5.3. Instalación de certificados software en Google Chrome y Apple Safari” el cliente de firma en los navegadores Chromium y Google Chrome para Linux utiliza el almacén de certificados de Mozilla Firefox. La instalación de certificados y configuración de tarjetas criptográficas requiere el uso de las herramientas proporcionadas por dicho navegador.

En el proceso de autenticación con fachada de tickets el almacén de certificados utilizado por Chromium y Google Chrome es distinto al de Mozilla Firefox por lo que los certificados configurados en dicho navegador no se encontrarán disponibles en este proceso.

La utilización de almacenes distintos en aplicaciones que integren autenticación mediante fachada de tickets y firma con cliente dificulta el uso de dichas aplicaciones, dificultad que aumenta con la necesidad de configurar el almacén de Chromium y Google Chrome con herramientas de línea de comandos como se indica en <http://code.google.com/p/chromium/wiki/LinuxCertManagement>.

Es posible simplificar el uso de tales aplicaciones mediante el uso compartido del almacén de Mozilla Firefox para ambos procesos. Para ello es necesario seguir las instrucciones proporcionadas en el enlace https://wiki.mozilla.org/NSS_Shared_DB_Howto.