JUNTA DE ANDALUCIA

Consejería de Hacienda y Administración Pública

Plataforma @firma

Cliente de firma electrónica. Incidencia con Oracle JRE 6 Update 24

Versión: v01r02

Fecha: 25/02/2011

HOJA DE CONTROL

Título	Cliente de firma electrónica. Incidencia con Oracle JRE 6 Update 24		
Entregable			
Nombre del Fichero			
Autor	Servicio de Coordinación de Administración Electrónica		
Versión/Edición	v01r02	**Fecha Versión**	25/02/2011
Aprobado por		**Fecha Aprobación**	
		Nº Total Páginas	

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Primera versión del documento	SCAE		23/02/2011
v01r01	Revisión	SCAE		24/02/2011
v01r02	Revisión	SCAE		25/02/2011

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área
Manuel Perera Domínguez	Jefe de Servicio	Servicio de Coordinación de Administración Electrónica
José Ignacio Cortés Santos	Gabinete Administración Electrónica	Servicio de Coordinación de Administración Electrónica
Cristina Romero Bedoya		Soporte técnico de administración electrónica
Rafael Perea Viega		Soporte técnico de administración electrónica

Este documento será publicado en el apartado correspondiente a la plataforma @firma en la web de soporte técnico de la administración electrónica de la Junta de Andalucía, en la siguiente dirección: *http://www.juntadeandalucia.es/haciendayadministracionpublica/ae*

ÍNDICE

1 Objeto del documento

Es objeto de este documento la descripción técnica y alcance de los problemas surgidos con la ejecución del cliente de firma en cualquiera de sus versiones con la última liberación por parte de Oracle de la JRE 6 Update 24 el pasado 15 de febrero de 2011.

2 Funcionamiento del Cliente de Firma Electrónica

El Cliente de Firma es un componente software para la realización de firma electrónica que funciona en forma de Applet de Java integrado en una página Web mediante JavaScript.

El Cliente hace uso de los certificados digitales X.509 y de las claves privadas asociadas a los mismos que estén instalados en el repositorio o almacén de claves y certificados (*keystore*) del navegador web (*Internet Explorer, Mozilla, Firefox*) o el sistema operativo así como de los que estén en dispositivos criptográficos (tarjetas inteligentes, dispositivos *USB*) configurados en el mismo (el caso de los DNI-e).

El Cliente de Firma, como su nombre indica, es una aplicación que se ejecuta en cliente (en el ordenador del usuario, no en el servidor Web). Esto es así para evitar que la clave privada asociada a un certificado tenga que "salir" del contenedor del usuario (tarjeta, dispositivo USB o navegador) ubicado en su PC. De hecho, nunca llega a salir del navegador: el cliente le envía los datos a firmar y éste los devuelve firmados.

El cliente de firma electrónica se compone de:

- Clases que implementan la funcionalidad del cliente (ficheros .jar y .jar.pack.gz) que pueden ser almacenados en un directorio local del equipo de usuario o en un directorio remoto, dependiendo del método de despliegue utilizado.
- Librerías propias del sistema donde se ejecuta el cliente (ficheros .dll en sistemas Windows, .so y .bin en sistemas Linux y .dylib en sistemas Mac).
- Bibliotecas Javascript (ficheros .js) que contienen funciones para la automatización de los procesos de firma. Se almacenen en el servidor web que contiene la aplicación.

2.1 Despliegue clásico (todas las versiones)

El despliegue clásico del cliente se realiza mediante la carga de un applet instalador, denominado "BootLoader" desde la versión 3.0 del cliente de firma. Es un applet Java encargado de comprobar la instalación del cliente en el equipo del usuario, comprobando la versión requerida por la aplicación y las disponibles en el equipo del usuario, procediendo a su instalación en caso de ser necesario.

En caso de ser necesario este applet es el responsable de copiar las clases y librerías en la máquina del usuario.

El instalador tiene sus propias clases Java y sus bibliotecas JavaScript.

Este componente está disponible para todas las versiones del cliente (2.3.5 y superior).

El modelo de seguridad de la máquina virtual Java exige que ciertas operaciones como el proceso de copiado y carga del cliente de firma tengan asignados ciertos privilegios para permitir su ejecución.

Además es posible que se requiera la instalación de clases y librerías nativas en carpetas de sistema, lo que conlleva a una necesidad de permisos de usuario más elevados de los que dispone un usuario estándar.

2.2 Despliegue basado en JNLP (a partir de la versión 3.1)

A partir de la versión v3.1 del cliente de firma se ha implementado un nuevo modo de despliegue vía JNLP para evitar su instalación en la máquina local del usuario.

Java Networking Launching Protocol es un mecanismo disponible en Java que permite la instanciación de clases ubicadas en un servidor remoto. Este mecanismo permite hacer uso del cliente de firma sin necesidad de tenerlo previamente instalado en la máquina del usuario. El despliegue JNLP evita por tanto que los usuarios deban instalar o actualizar el cliente de firma de forma explícita, permitiendo su uso en entornos con permisos restringidos.

Este método de carga introduce las siguientes ventajas:

- No necesita el proceso previo de instalación del cliente.
- Usa la tecnología JNLP para ejecutar el applet integrado en la página web.
- Mantiene un caché de aplicaciones JNLP evitando en posteriores ocasiones volver a descargar los ficheros.
- No interfiere con instalaciones locales del cliente.
- No se requieren permisos especiales de usuario, únicamente el acceso a los certificados que se vayan a utilizar.

El despliegue vía JNLP requiere que se configuren correctamente los descriptores de este servicio (ficheros "*COMPLETA_afirma.jnlp*", "*MEDIA_afirma.jnlp*" y "*LITE_afirma.jnlp*") con la ruta al directorio en donde se encuentran los ficheros con el núcleo del Cliente @firma. Estos ficheros están codificados en XML y definen entre otras cosas la ruta donde se ubica el despliegue del cliente de firma en cada una de sus versiones disponibles (lite, media y completa).

El modo de despliegue vía JNLP se activará automáticamente cuando el cliente detecte que el usuario dispone una configuración compatible (ver apartado 3.4.1 de este documento). En caso de no disponer de dicha configuración, el cliente se desplegará siguiendo método tradicional a través del BootLoader.

3 Problema con JRE 6 Update 24

3.1 Actualización JRE 6 Update 24

Oracle publica periódicamente actualizaciones de la máquina virtual Java para corrección de errores, implementación de nuevas características funcionales, eliminación de características obsoletas y modificación de directivas de seguridad.

Debido a que el cliente se apoya en JRE y sus librerías para su correcto funcionamiento, es "sensible" a los cambios que se introducen en la máquina virtual.

La última actualización de la JRE 6 es la "Update 24", liberada el pasado 15 de febrero de 2011. Esta revisión introduce actualizaciones de seguridad críticas, algunas públicas y otras no publicadas para evitar la explotación de defectos de revisiones anteriores.

Lo más importante que solventa es una Alerta de Seguridad Crítica CVE-2010-4476 que se detalla en el siguiente apartado.

3.2 Alerta de Seguridad Crítica CVE-2010-4476

La principal novedad de esta revisión de JRE es la resolución de la alerta de seguridad crítica CVE-2010-4476 (*http://blogs.oracle.com/security/2011/02/security_alert_for_cve-2010-44.html*) que afecta tanto a las versiones de Oracle Java SE y Oracle Java for Business para aplicaciones Java que se ejecutan en un servidor como a aplicaciones de escritorio. Es una alerta más grave en entornos de servidor donde se puede explotar esta vulnerabilidad para provocar una denegación de servicio.

Aunque este fallo también afecta a las aplicaciones de escritorio y applets que se ejecutan en un navegador, es menos importante ya que únicamente puede provocarse en este caso que la aplicación o applet deje de responder y tenga que ser reiniciado, pero en ningún caso compromete la seguridad del equipo del usuario en modo alguno. Sin embargo, aunque el impacto sea menos importante, Oracle la ha catalogado como "crítica" y por tanto recomienda su actualización.

Los cambios aplicados a las directivas de seguridad de JRE introducidos en esta versión son consecuencia de la solución de esta vulnerabilidad, por lo que es previsible que este comportamiento se mantenga en futuras revisiones de JRE.

3.3 Descripción del problema

Entre los cambios incorporados en esta revisión de JRE 6 Update 24 se incluyen modificaciones en las directivas de seguridad que impiden entre otras cosas que un applet pueda instanciar librerías Java alojadas localmente, obteniéndose en este caso un error por falta de permisos.

Esta situación impide el despliegue del cliente de firma por el método tradicional, descrito en el apartado 2.1 de este documento y afecta por tanto a todas las aplicaciones que hacen uso del cliente de firma anteriores a la versión 3.1 y aquellas que utilizando la última versión del cliente no dispongan de una configuración compatible con JNLP (apartado 3.4.1 de este documento).

En los casos afectados, se obtiene siempre el mismo error al instanciar el cliente de firma mediante el despliegue tradicional:

java.lang.SecurityException: Permission denied: file:xxxxx

Indicar que este error no afecta al BootLoader que funciona correctamente, instalando el cliente en la máquina del usuario si es necesario.

Se ha comprobado el funcionamiento del cliente en una beta de la próxima versión de JRE 6 Update 25 build b01 (*http://download.java.net/jdk6/*) liberada el 31 de enero de 2011. Con esta revisión el cliente de firma electrónica funciona correctamente, no obteniéndose el error descrito anteriormente.

Este problema fue reportado a ORACLE SDN (Sun Developer Network) con identificador 7020285 (*http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7020285*) con fecha 17 de febrero, siendo aceptado por ORACLE SDN y clasificado con prioridad "Alta". El 22 de febrero se cerró la incidencia anterior por parte de Oracle indicando que el comportamiento actual es el "correcto" y que no va a ser posible la carga de un applet desde un servidor web con referencias a objetos (clases, librerías, etc.) ubicados localmente en el equipo del usuario. Por tanto, cabe suponer que éste será el comportamiento de JRE para esta revisión y las próximas.

3.4 Posibles soluciones al problema

Para solventar el problema descrito en el apartado 3.2 se consideran dos posibles vías de resolución:

- Adaptar la aplicación al despliegue JNLP.
- No actualizar a la última revisión JRE 6 Update 24.

3.4.1 Adaptar la aplicación al despliegue JNLP

El despliegue JNLP requiere de una configuración compatible con este método, concretamente:

1. Utilizar la versión 3.1 del cliente de firma electrónica u otra superior.
2. Disponer de una JRE 6 Update 10 o superior en el equipo del usuario en arquitectura de 32 bits.
3. Configurar los descriptores del servicio JNLP para que puedan ser utilizados por el cliente.
4. Si la aplicación utiliza el cliente de firma con las librerías Javascript será necesario invocar la función **cargarAppletFirma** de alguna de estas tres formas:
   - Sin parámetros.
   - Indicando únicamente la construcción.
   - Especificando la construcción y el parámetro *oldDeployment* con valor *false*.

Como se describe en el apartado 2.2 de este documento, el cliente utiliza de forma transparente el despliegue JNLP si se detecta una configuración compatible. En caso contrario, el cliente opta por el despliegue clásico a través del applet "Bootloader".

La estructura de estos ficheros .jnlp es la que sigue:

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

<jnlp spec="1.0+" codebase="**RUTA_DIRECTORIO_DESPLIEGUE**">

```
<information>
  <title>Cliente @firma</title>
  <vendor>Junta de Andalucía</vendor>
  <homepage href="http://www.juntadeandalucia.es" />
  <description>Cliente de firma @firma</description>
</information>
<offline-allowed/>
<security>
  <all-permissions/>
</security>
<resources>
  <property name="jnlp.packEnabled" value="true"/>
  <j2se version="1.6+" href="http://java.sun.com/products/autodl/j2se" />
  <jar href="COMPLETA_j6_afirma5_coreV3.jar" main="true"/>
</resources>
<applet-desc
  name="Cliente @firma"
  main-class="es.gob.afirma.cliente.SignApplet"
  width="1"
  height="1">
 <update check="background"/>
</jnlp>
```

El integrador únicamente deberá modificar la cadena "**RUTA_DIRECTORIO_DESPLIEGUE**", de cada uno de estos ficheros, por la ruta absoluta al directorio en donde se encuentren los ficheros "COMPLETA_j6_afirma5_coreV3.jar", "COMPLETA_j6_afirma5_coreV3.jar.pack.gz", "MEDIA_j6_afirma5_coreV3.jar", "MEDIA_j6_afirma5_coreV3.jar.pack.gz" y "LITE_j6_afirma5_coreV3.jar", "LITE_j6_afirma5_coreV3.jar.pack.gz"etc.

Las aplicaciones integradas con la **extensión de compatibilidad** de @firma requieren el uso de la librería Javascript "scriptfirma.js" para interactuar con el cliente de firma. Dicha librería no incluye actualmente soporte para el despliegue JNLP. No obstante, está en estudio la viabilidad de adaptar este script para incluir esta nueva funcionalidad. De la evolución de este asunto, se informará en la web de soporte técnico de la administración electrónica de la Junta de Andalucía.

Toda la información detallada de este proceso está descrita en el manual del integrador del cliente 3.1 (manual_integrador_1_1_RC7.pdf, secciones 5 y 6). Para obtener información complementaria sobre el proceso de actualización del cliente de firma en aplicaciones integradas con la extensión de @firma consultar el documento "Migración cliente extensión.pdf" incluido en la distribución del cliente de firma 3.1.

3.4.2 No actualizar a la última revisión JRE 6 Update 24

En el caso de no poder cumplir los requisitos necesarios descritos en el apartado anterior para realizar un despliegue mediante JNLP, será necesario garantizar el funcionamiento del despliegue clásico descrito en el apartado 2.1 de este documento. Debido a que los cambios introducidos en JRE 6 Update 24 no son en forma alguna "solventables" via software, se recomienda **NO** actualizar a esta revisión de JRE.

Se recomienda por tanto permanecer en la versión JRE 6 Update 23 hasta el desarrollo de un mecanismo alternativo de instanciación del cliente de firma electrónica.

Para aquellos usuarios que estén actualizados a esta última revisión 24 se les puede instar a que desinstalen esta revisión e instalen la anterior (Update 23) desde el siguiente enlace:

https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=jre-6u23-oth-JPR@CDS-CDS_Developer

3.5 Propuesta de modificación del cliente

Se está considerando la realización de una acción de mantenimiento adaptativo y aumentativo para el cliente de firma electrónica, en particular el desarrollo de un método de instanciación "a prueba de fallos" consistente en que no se instale nada en el equipo del usuario, por lo que cada vez que se requiera el uso del cliente de firma, el navegador accederá a las clases y librerías de forma remota. Este nuevo modo de despliegue convivirá con los dos ya existentes con carácter complementario y no alternativo. El orden de prioridad en cuanto a la utilización de uno u otro tipo de despliegue, de manera automática, sería el siguiente:

1. Despliegue del cliente mediante JNLP.

2. Despliegue clásico.

3. Despliegue "a prueba de fallos".

Este asunto está en estudio para determinar su viabilidad tecnológica y el efecto que tendría sobre las aplicaciones y servicios de administración electrónica ya existentes.

En la situación actual, se recomienda a los integradores de aplicaciones y servicios de administración electrónica, la adaptación al despliegue del cliente de firma electrónica mediante JNLP así como la no instalación de revisiones de JRE posteriores a la Update 23.