PORTAFIRMAS

Applet de firma Acepta

Documento Versión: 0.1
Nº de páginas: 13

Sèrvei d'informàtica
VNIVERSITAT DE VALÈNCIA

0. CAPTURAS DE PANTALLA

1. Introducción

En este manual se detallan las funcionalidades del applet de firma Acepta, así como la configuración del equipo requerida para poder utilizarlo. El applet Acepta se utiliza desde la pantalla de la bandeja del portafirmas, al firmar documentos con uno de los certificados digitales instalados en nuestro equipo.

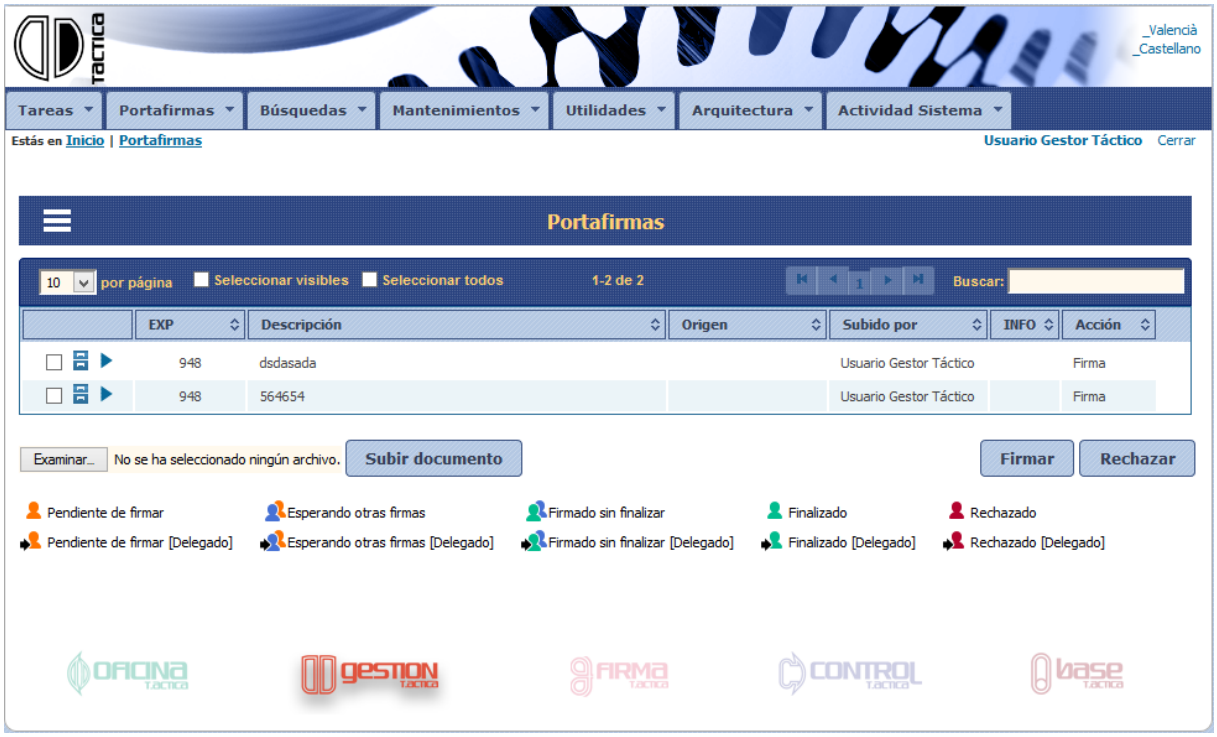

Figura 1 – Bandeja del portafirmas

También se utiliza desde la pantalla de identificación, en caso de elegir la opción de certificado digital.

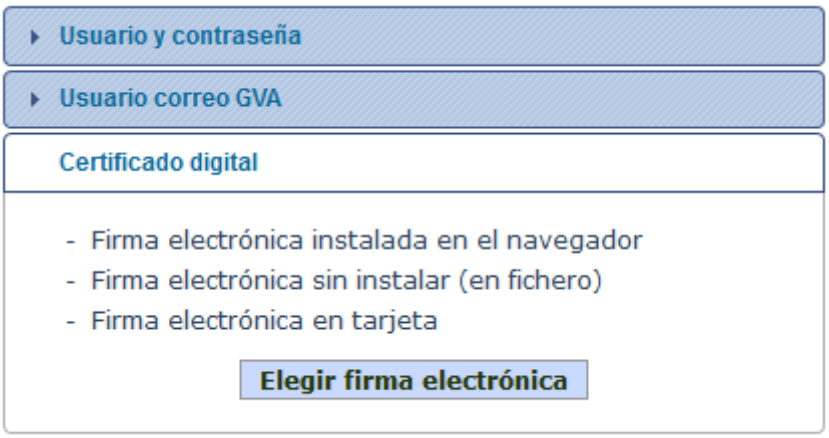

Figura 2 – Pantalla de identificación

2. Requisitos

Para el correcto funcionamiento del applet, hay una serie de requisitos que el equipo deberá cumplir.

2.1. Java

Lo primero que debe comprobar es si tiene usted instalada la última versión de Java. Esto puede hacerlo en la siguiente dirección:

http://www.java.com/es/download/installed.jsp

Si no tiene Java instalado o su versión no está actualizada, se le avisará y le darán la opción de instalar la última versión.

Si su sistema operativo es de 64 bits, es recomendable que instale tanto la versión de Java de 32 bits como la de 64 bits, ya que algunos navegadores se ejecutan de una forma o de otra, y por tanto necesitan el plugin de la arquitectura indicada. Puede descargar las diferentes versiones de Java para su sistema operativo desde la siguiente dirección:

http://www.java.com/es/download/manual.jsp

2.2. Navegador

Para que el applet pueda ejecutarse, hay que comprobar es si el plugin de Java está instalado en el navegador y si está habilitado. Dependiendo del navegador se puede comprobar en:

2.2.1. Mozilla Firefox

Abrir Menú -> Complementos -> Plugins. Debe poder ver el complemento de "Java(TM) Platform" y que a la derecha ponga "Activar siempre".

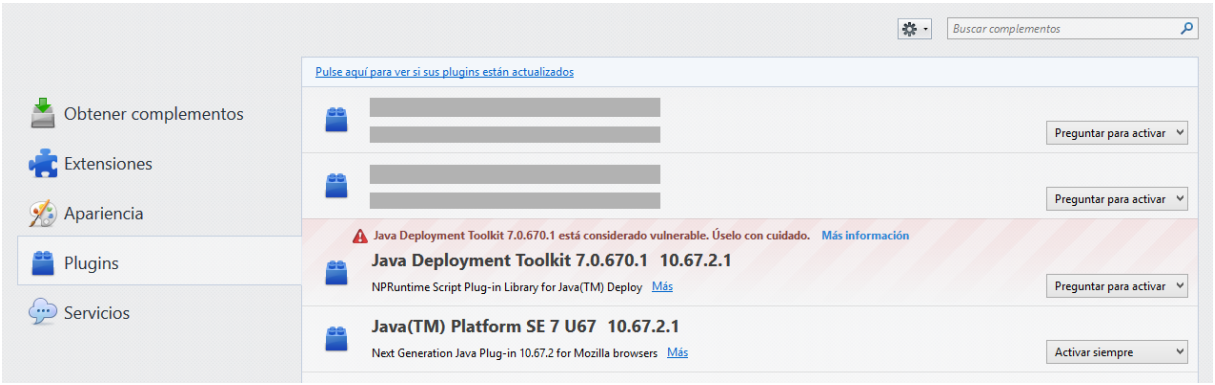

Figura 3 – Complementos navegador Firefox

2.2.2. Internet Explorer

Internet Explorer: Herramientas -> Administrar complementos. Debe poder ver "Java(tm) Plug-In SSV Helper" y "Java(tm) Plug-In 2 SSV Helper" y que aparezcan como "Habilitado".

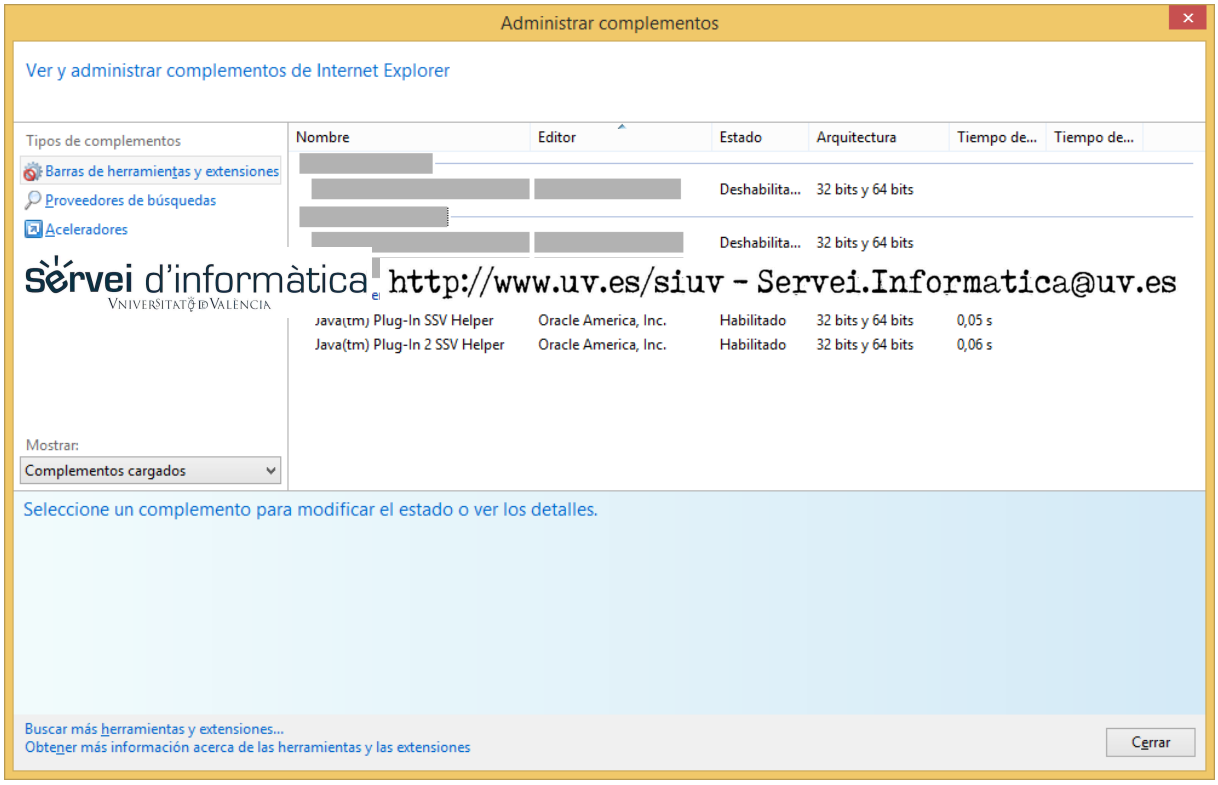

Figura 4 – Complementos navegador Internet Explorer

2.3. Certificado digital

Una vez el applet se pone en funcionamiento, lo primero que hay que hacer es seleccionar el certificado con el que el usuario va a firmar / identificarse. El applet le mostrará un listado con los certificados instalados en los certificados de Windows, Mozilla y con las tarjetas criptográficas detectadas. Además del listado, también se podrá cargar el certificado desde un fichero alojado en el equipo.

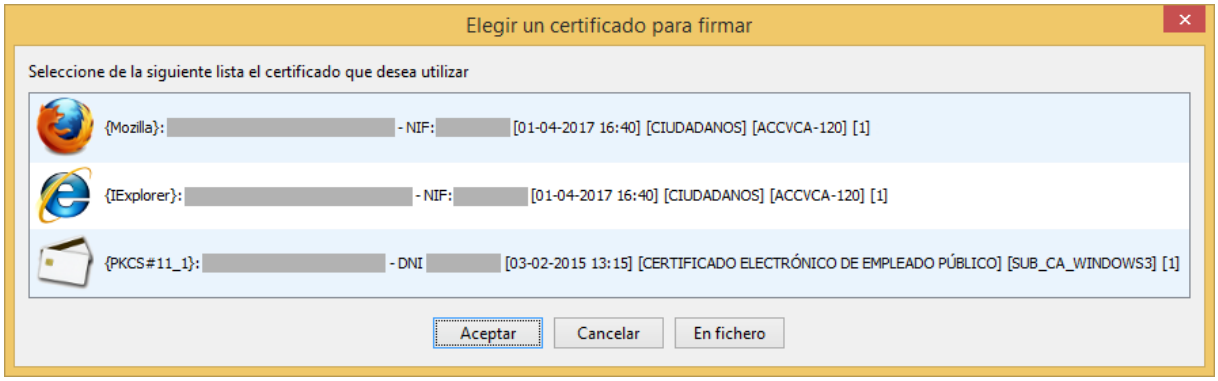

Figura 5 – Listado de los certificados disponibles

2.3.1. Instalado en el navegador

Al iniciar el applet se le mostrará un listado con los certificados instalados en los almacenes de Mozilla y de Windows. Se mostrarán los certificados instalados en ambos almacenes independientemente del navegador con que se esté trabajando. Dependiendo del almacén en que esté instalado el certificado aparecerá un icono para identificarlo.

Figura 6 – Iconos para almacenes de Windows, de Mozilla y de Apple

Si el almacén de Mozilla está protegido por contraseña, se le pedirá, y en caso de no introducirla correctamente no se mostrarán los certificados de ese almacén.

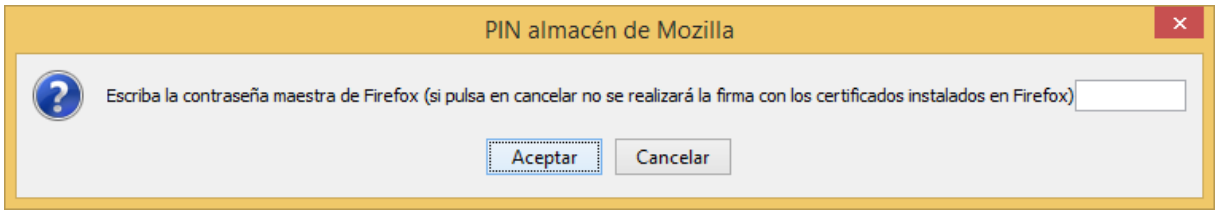

Figura 7 – Petición de contraseña almacén de Mozilla

2.3.2. En soporte software

Si dispone de su certificado guardado en un fichero (.p12), puede pulsar el botón "En fichero" (en la parte inferior derecha) y seleccionarlo en su equipo.

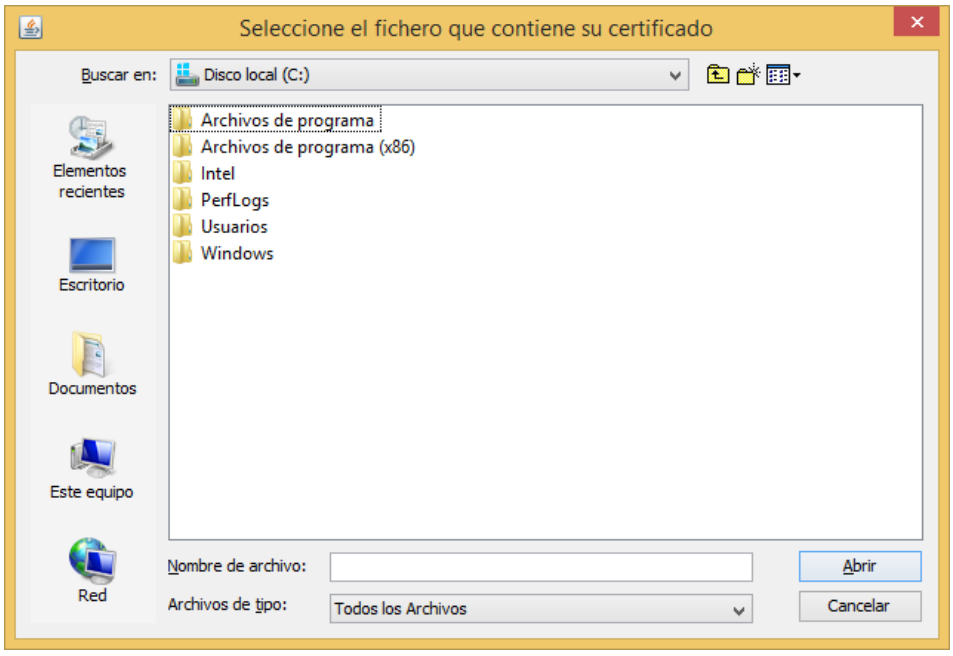

Figura 8 – Pantalla de selección de ubicación del certificado

2.3.3. Tarjeta criptográfica

El applet detectará los dispositivos en tarjeta criptográfica conectados al equipo y los mostrará en el listado.

Figura 9 – Icono para tarjeta criptográfica

2.4. Autoridades certificadoras soportadas

En estos momentos el applet Acepta soporta los certificados emitidos bajo las siguientes autoridades certificadoras.

2.4.1. Certificados expedidos por la ACCV

Cualquier certificado de ciudadano, empleado público, pertenencia a empresa… de la ACCV, ya sea en tarjeta criptográfica, fichero p12 o instalado en el navegador.

2.4.2. DNIe

Utilizando un lector de tarjetas, el applet es capaz de detectar el DNIe y utilizarlo para firmar documentos.

3. Código firmado y advertencias

La aparición de Java 1.7.0 Update 45 ha hecho que los usuarios de applets en entornos cliente se vean sorprendidos por mensajes en los que se duda de la seguridad de dichas aplicaciones. Mensajes como los siguientes:

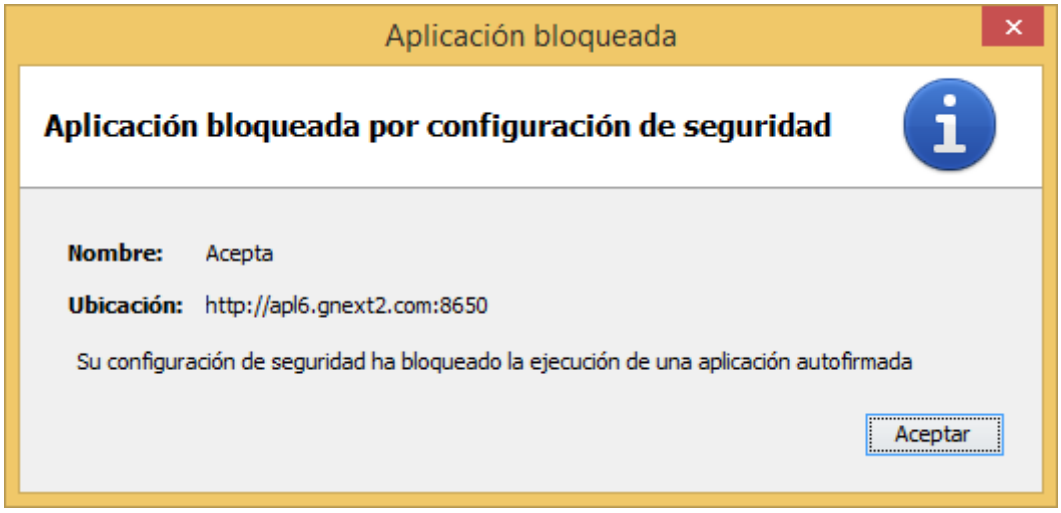

Figura 10 – Mensaje información applet bloqueado

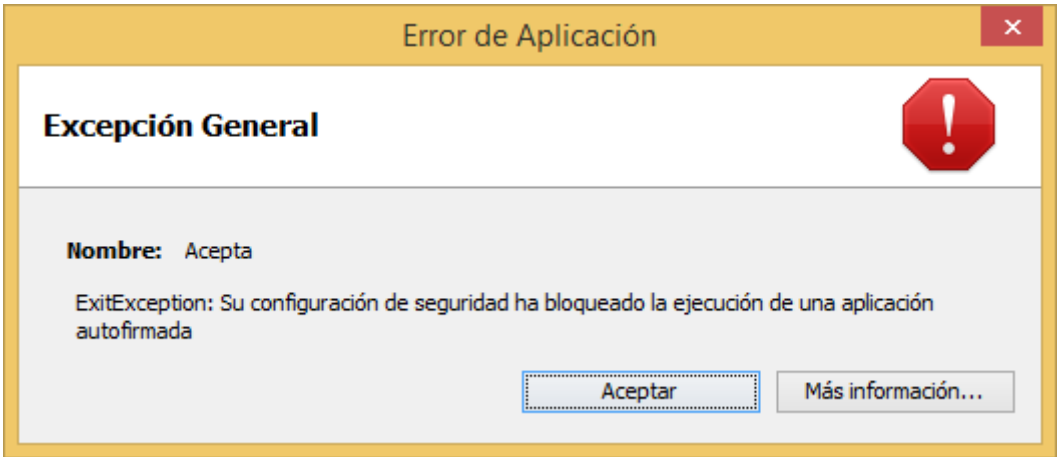

Figura 11 – Mensaje error applet bloqueado

El applet de firma electrónica que utiliza la plataforma, está firmado con un certificado emitido por la ACCV. El certificado es válido y correcto y su validez dependerá de que Java sea capaz de acceder a los certificados raíz de la Agencia de Tecnología y Certificación Electrónica.

Dependiendo del navegador en el que se ejecute el applet se pueden dar dos situaciones:

- Firefox: el plugin de Java trabaja sólo con el almacén de certificados de Java en el que no están los certificados raíz de la Agencia de Tecnología y Certificación Electrónica. Dichos certificados se encuentran en estado de revisión por Oracle y se espera que sean añadidos a las distribuciones de Java en próximas versiones.

- Internet Explorer: el plugin de Java se integra muy bien con el almacén de claves de Internet Explorer, donde ya están instalados los certificados raíz de la Agencia de Tecnología y Certificación Electrónica.

3.1. Reconocimiento de certificados de la ACCV mediante Java

Para que Java acepte los certificados de la ACCV como válidos, hay que añadir el certificado raíz de la ACCV como "Firmante de confianza". Esto se puede hacer desde el panel de control de java, dentro de certificados elegir "CA de firmantes" e importarlo. Estos son los pasos a seguir:

- Descargar el certificado ACCV Raíz 1 de la ACCV. Para descargar el certificado de la ACCV, hay que entrar en:

  http://www.accv.es/ayuda/descargar-certificados-digitales/

  Ahí seleccionar el primer certificado (Certificado de la Autoridad de Certificación Raíz: ACCV Raíz 1 (CRT 4KB) - Vigente hasta 31/12/2030), hacer click derecho y "Guardar como…".

- Abrir el panel de control de Java (Menú Inicio -> Panel de Control -> Java).

- Seleccionar la pestaña de "Seguridad" y pulsar en "Gestionar Certificados...".

- En el menú de selección de arriba ("Tipo de Certificado"), seleccionar "CA de Firmante".

- Estando seleccionada la pestaña de "Usuario", pulsar en "Importar".
- Seleccionamos el certificado ACCV Raíz 1 (es posible que se tenga que cambiar el tipo de archivo que se muestra a "Todos los archivos", por defecto muestra sólo .csr y .p12 y el certificado raíz de la ACCV es un .crt).
- Pulsar en "Abrir", y el certificado ya está importado.

3.2. Excepcionar URL

Si los mensajes de advertencia siguen apareciendo y el applet no se llega a ejecutar, otra opción es excepcionar la URL de la aplicación para que se permita la ejecución de los applets descargados desde esa URL. Los pasos a seguir son:

- Abrir el panel de control de Java (Menú Inicio -> Panel de Control -> Java).
- Seleccionar la pestaña de "Seguridad" y pulsar en "Editar lista de sitios...".
- En esta nueva ventana pulsamos en "Agregar" e introducimos la URL base de la aplicación.
- Aceptamos los cambios y ahora ya debería poder ejecutarse el applet de firma.

3.3. Publicador reconocido

Si todo ha funcionado correctamente, ahora al ejecutar el applet la máquina de Java debería reconocer el publicador de la aplicación correctamente. El mensaje que aparecería en pantalla debería ser parecido al de la siguiente figura:

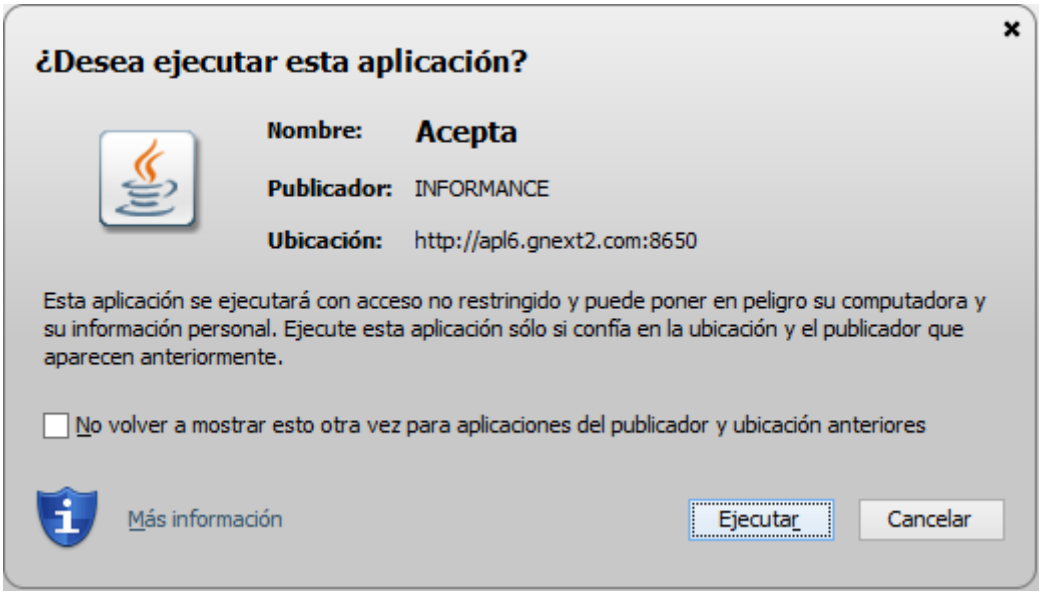

Figura 12 – Mensaje información applet publicador reconocido

4. Uso de tarjetas criptográficas en sistemas UNIX

Mientras que en los sistemas operativos Windows las tarjetas criptográficas se detectan automáticamente y aparecen en el repositorio de Windows al introducirlas, esto no pasa así en los sistemas UNIX, por lo que hay que configurar el módulo criptográfico de Mozilla Firefox para que detecte las tarjetas y las cargue en su repositorio.

4.1. Tarjeta criptográfica Siemens

Para utilizar una tarjeta criptográfica siemens debemos realizar los siguientes pasos:

4.1.1. Instalar los drivers del lector

Estos son los pasos a seguir:

- Descargamos de la ACCV los drivers:

  http://www.accv.es/fileadmin/Archivos/software/scmccid_linux_32bit_driver_V5.0.21.tar.gz

- Instalamos los módulos pcscd, libpcsclite1 y libccid.

  > *sudo apt-get -y install pcscd libpcsclite1 libccid*

- Extraemos el archivo tar.gz.

  > *tar -xzvf <ruta_al_fichero>/scmccid_linux_32bit_driver_V5.0.21.tar.gz*

- Cambiamos al directorio creado al extraer.

  > *cd <ruta_al_fichero>/scmccid_5.0.21_linux_rel/*

- Ejecutamos install.sh para instalar los drivers.

  > *sudo sh ./install.sh*

  > *sudo /etc/init.d/pcscd restart*

4.1.2.Instalar los controladores de la tarjeta criptográfica SIEMENS

Estos son los pasos a seguir:

- Descargamos de la ACCV los drivers:

  http://www.accv.es/fileadmin/Archivos/software/CardOS_API_V3_2_41_Linux2_6_22_glibc2_6_1_pcsc1_5_1.tar.gz

- Extraemos el .tar.gz en el directorio raíz.

  > *cd /*

  > *sudo tar -xzvf <ruta_al_fichero>/CardOS_API_V3_2_41_Linux2_6_22_glibc2_6_1_pcsc1_5_1.tar.gz*

- Ejecutamos ldconfig.

  > *sudo ldconfig*

4.1.3. Dependencias de la librería libsiecap11.so

En este momento hay que resolver las dependencias de la librería libsiecap11.so. Según la información de la ACCV, hay que crear los siguientes enlaces dinámicos:

> *sudo ln -s /usr/lib/i386-linux-gnu/libxcb.so.1 /usr/lib/libxcb-xlib.so.0*

> *sudo ln -s /usr/lib/libXaw.so.7 /usr/lib/libXaw8.so.8*

4.1.4. Registro del módulo criptográfico en Mozilla Firefox

Estos son los pasos a seguir:

- Acceda al menú Editar > Preferencias... de Mozilla Firefox.
- Seleccione el menú Avanzado. Dentro de este menú seleccione la pestaña Cifrado y pulse sobre el botón Dispositivos de Seguridad.
- Haga clic sobre el botón Cargar e introduzca los siguientes datos en la ventana que se le abrirá:

  Nombre del módulo: "ACCV Siemens PKCS#11"

  Nombre del archivo del módulo: /usr/local/lib/libsiecap11.so
- Pulse Aceptar y confirme la instalación. Firefox le informará que el módulo se ha instalado correctamente.

5. Interfaz del applet

Una vez seleccionado el certificado a utilizar, el proceso de firma comienza. En el caso de estar utilizando el applet para identificarse en la aplicación, si el proceso finaliza correctamente entrará en la aplicación con el usuario que tenga el mismo DNI al del certificado utilizado.

En el caso de utilizar el applet desde la bandeja del portafirmas, se mostrará una nueva pantalla en la que podremos seguir el progreso de las operaciones de firma.

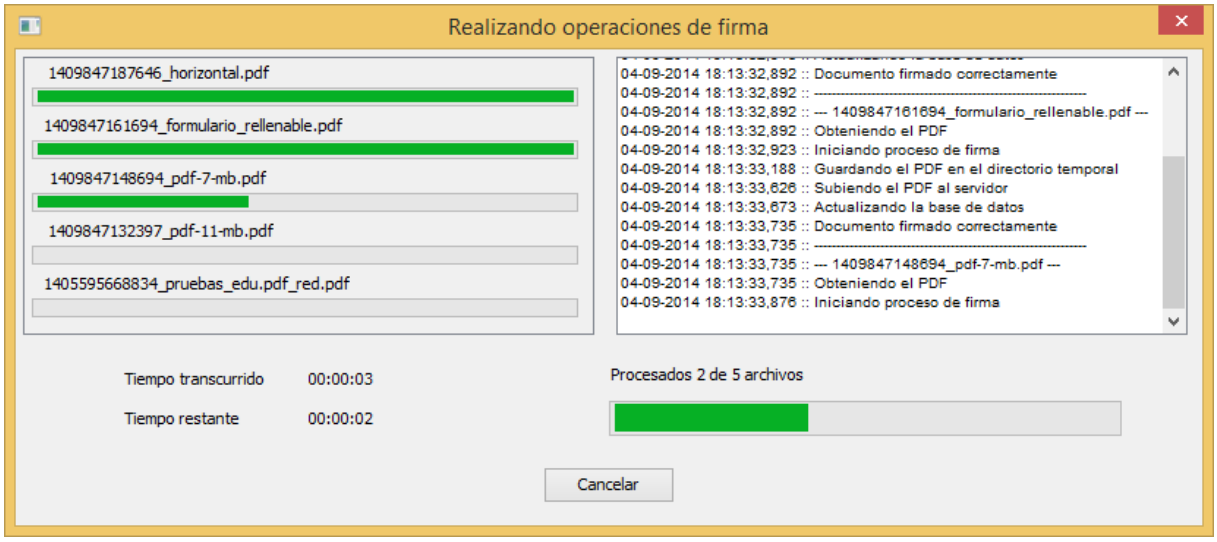

Figura 13 – Progreso operaciones de firma

A la izquierda de la ventana aparece el listado de documentos para firmar, cada uno con su respectiva barra de progreso. A la derecha hay tenemos un log donde irá apareciendo la información sobre las operaciones realizadas en cada momento. En la parte inferior tenemos un contador del tiempo transcurrido y restante para finalizar las operaciones y la barra de progreso general.

Una vez finalice el proceso nos aparecerá un mensaje informándonos y podremos salir del applet, volviendo a la bandeja del portafirmas.

6. Firma PAdES-LTV

Las firmas que se realizan desde esta herramienta se implementan acorde al estándar PAdES-LTV, que cumple con los requisitos para ser una firma longeva, para favorecer el almacenamiento de los documentos firmados.

Este estándar especifica cómo incluir información de validación en un documento PDF y cómo protegerlo utilizando sellos de tiempo, de manera que sea posible verificar la firma de un PDF mucho después de ser firmado.

La validez de una firma longeva se halla limitada a la vida del certificado del último sello de tiempos de documento que contiene el PDF, aunque erróneamente se suele pensar que una firma longeva puede validarse eternamente.

Por ejemplo, el certificado de la TSA de la ACCV caducará el 18 de Noviembre de 2016, lo que implica que a partir de esa fecha las firmas PAdES-LTV realizadas con la TSA de la ACCV dejarán de ser válidas. Con el objeto de alargar la vida de una firma longeva será necesario realizar un resellado de la misma cuando se cambie el certificado de la TSA.