Consejería de Hacienda y Administración Pública

Guía de uso del cliente

Sevilla, noviembre de 2010

Hoja de control		
Fecha	**Autor**	**Descripción**
18/11/2010	RPV	Adaptación guía de uso del cliente MPR

1 Introducción

El Cliente de Firma es una herramienta 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 (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 contiene las interfaces y componentes web necesarios para la realización de los siguientes procesos (además de otros auxiliares como cálculos de hash, lectura de ficheros, etc…):

- Firma de formularios Web.
- Firma de datos y ficheros.
- Multifirma masiva de datos y ficheros.
- Cofirma (CoSignature) → Multifirma al mismo nivel.
- Contrafirma (CounterSignature) → Multifirma en cascada.

Como complemento al cliente de firma, se encuentra un cliente de cifrado que nos permite realizar las funciones de encriptación y desencriptación de datos atendiendo a diferentes algoritmos y configuraciones. Además permite la generación de sobres digitales.

2 Objetivos

El objetivo del presente documento es detallar un posible uso típico del Cliente @firma dentro de una aplicación Web, tanto desde un punto de vista del entorno de ejecución como desde el directo por parte del usuario.

3 Instalación

3.1 Requisitos mínimos

Sistema operativo:

- Windows 2000, XP, Vista, 7, Server 2003, Server2008
- Linux (Guadalinex, Ubuntu)
- MacOS X 10.5
- Sun Solaris / OpenSolaris 10

Navegador web:

- Firefox 2.0.20 o superior
- Internet Explorer 5.5 o superior
- Chrome 3.0 o superior
- Apple Safari 10 o superior

JRE 1.5 update22 o superior (instalada en el navegador)

Certificado digital de usuario instalado en el navegador o disponible a través de un módulo PKCS#11 instalado en el navegador (caso del DNI-e)

Las siguientes matrices muestran las posibles combinaciones a ese efecto:

Windows 32 Bits (2000, XP, Vista, 7, Server 2003, Server 2008)					
MS Internet Explorer	Mozilla Firefox		Google Chrome	Apple Safari	Opera
6 y superiores	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
JSE 5u22 y superiores (32 Bits)	JSE 5u22 y superiores (32 Bits)	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	NO SOPORTADO

Windows 64 Bits (XP, Vista, 7, Server 2003, Server 2008)					
MS Internet Explorer	Mozilla Firefox		Google Chrome	Apple Safari	Opera
6 y superiores	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	NO SOPORTADO

Mac OS X x86 (10.5 y superiores)					
MS Internet Explorer	Mozilla Firefox (KeyStore de Mac OS X)		Google Chrome	Apple Safari	Opera
5.5	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
NO SOPORTADO	JSE 1.6.0_07 y superiores	JSE 1.6.0_07 y superiores	JSE 1.6.0_07 y superiores	JSE 1.6.0_07 y superiores	NO SOPORTADO

Linux 2.6 x86 (32 Bits)					
MS Internet Explorer	Mozilla Firefox		Google Chrome	Apple Safari	Opera
	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
	JSE 5u22 y superiores (32 Bits)	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	NO SOPORTADO

Sun Solaris / OpenSolaris (10 y superiores, x86, x64 y SPARC)					
MS Internet Explorer	Mozilla Firefox		Google Chrome	Apple Safari	Opera
5,5	Desde 2.0.0.20 hasta 3.5	3.6 y superiores	3.0.195 y superiores	4.0 y superiores	10.10 y superiores
NO SOPORTADO	JSE 5u22 y superiores (32 Bits)	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	JSE 6u18 32 Bits y superiores	NO SOPORTADO

NOTAS Importantes:
En Linux y Solaris el navegador Web (incluyendo las bibliotecas NSS), el núcleo del sistema operativo y el entorno de ejecución de Java deben ser exactamente de la misma arquitectura
En el sistema operativo Mac OS X siempre se utilizará el almacén de certificados (KeyStore) propio del sistema operativo, incluso con el navegador Mozilla Firefox

4 Guía de uso

4.1 Introducción

El componente de firma es una aplicación cliente de Firma Electrónica que se ejecuta en el PC del usuario. Está basado en Applets Java, por lo que es necesario tener instalada la máquina virtual de Java, que será el entorno donde se ejecutará dicha aplicación.

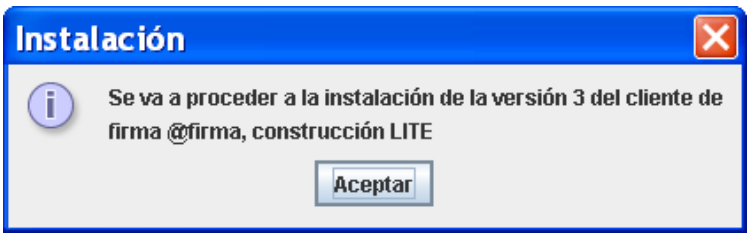
Básicamente, el componente recibe datos y los devuelve firmados, utilizando para ello los certificados instalados en el almacén de certificados (keystore) del navegador donde se esté ejecutando en ese momento.

La razón por la que se ejecuta en el cliente es porque la codificación de la firma electrónica se efectúa en el ordenador del usuario, utilizando la clave privada del certificado seleccionado, que reside en su PC. Si su certificado reside en una tarjeta inteligente (DNIe) o tokenUSB, estos son cargados automáticamente en el almacén de certificados a través de los controladores (drivers) de los dispositivos, por lo que serán accesibles desde el cliente de firma.

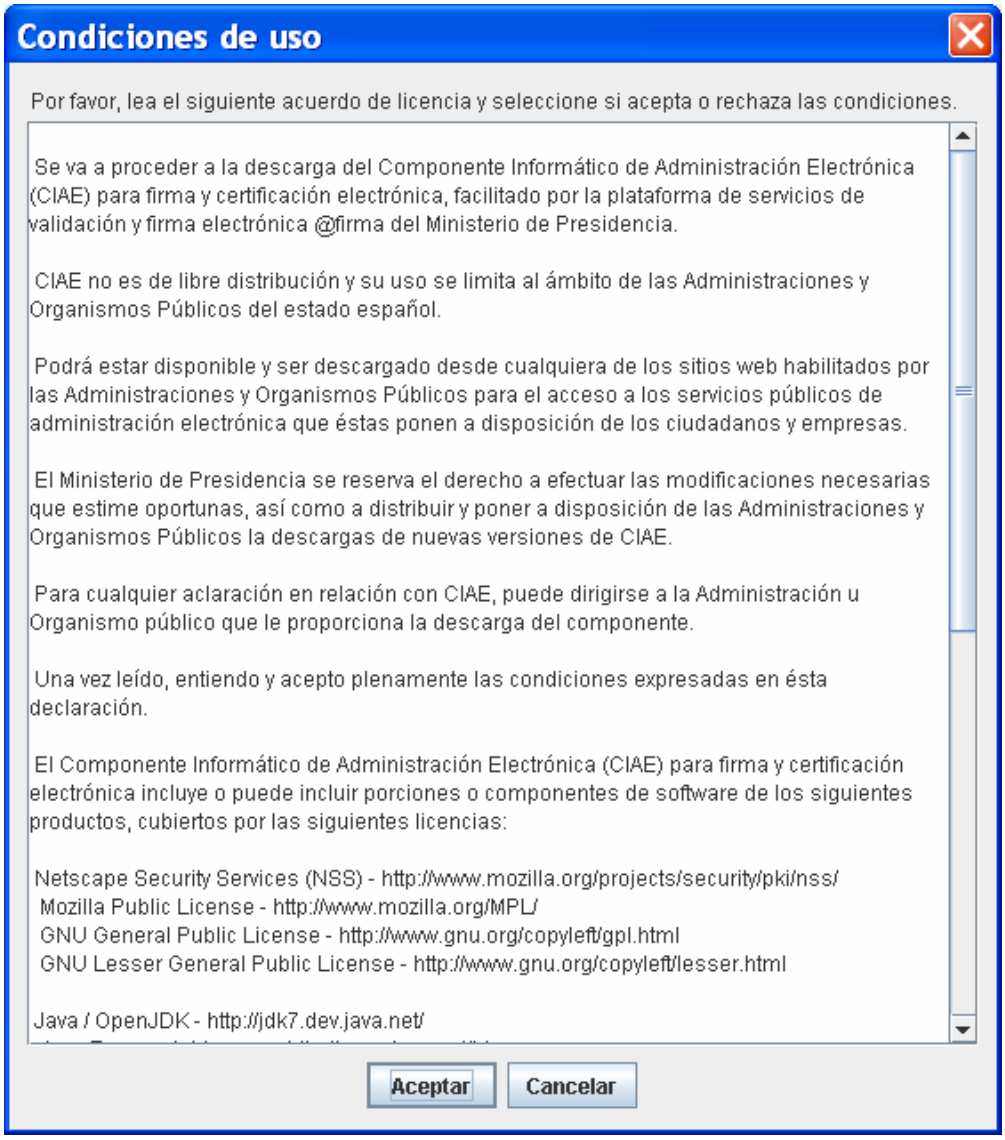
4.2 Instalación

Tras la invocación de la función cargarAppletFirma(build) se ejecutará automáticamente el proceso de instalación del componente de firma:

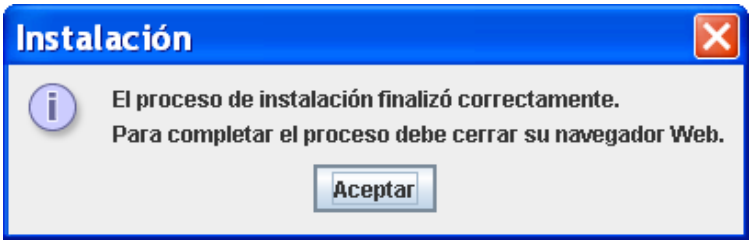
1 – Se informa del inicio de la instalación del Cliente de Firma de @firma.



2 – El proceso de instalación muestra el "Disclaimer", informando de las Condiciones de Uso del componente, las cuales deberán ser aceptadas para continuar con la instalación.

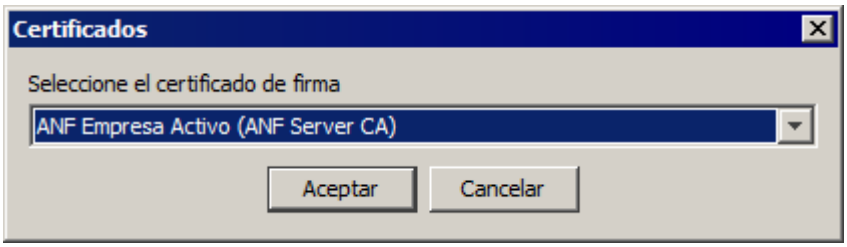


3 – Se notifica de la finalización de la instalación y se recomienda reiniciar los navegadores.



Una vez instalado, si usamos el DNI-e, el navegador nos mostrará la siguiente ventana:

En la cual deberemos introducir nuestro PIN y pulsar sobre el botón "Aceptar".



En la siguiente ventana, el navegador nos mostrará el listado de certificados instalados en el navegador, seleccionaremos el certificado con el que nos queramos identificar, en e caso del DNIe el listado como "**Apellidos, Nombre (AUTENTICACIÓN)**" y pulsaremos sobre el botón "**Aceptar**"

Es posible que el navegador nos vuelva a pedir introducir el PIN, una vez hecho pulsaremos **"Aceptar"** y tras el sistema realizar las comprobaciones pertinentes habremos accedido al aplicativo.

4.3 Desinstalación

Es posible desinstalar el Cliente @firma desde una página Web en habilitada para ello. Si no se le ha proporcionado la ruta a una Web para tal efecto, es posible desinstalar el Cliente @firma de forma manual.

4.3.1 Desinstalación manual

Para la desinstalación manual del Cliente @firma será necesario eliminar los ficheros que éste instala en disco. A continuación se listan los distintos ficheros que pueden copiarse en el sistema local durante la instalación del Cliente. Tenga en cuenta que si está ejecutando el Cliente @firma u otra aplicación Java es posible que no pueda eliminar alguno de estos ficheros:

- Todos los entornos:
  - [Directorio usuario]/afirma.5/ (Este es el directorio de instalación)

- Sólo en Java 6 de 64bits – Entornos Windows
  - [Directorio JRE]/lib/ext/sunmscapi.jar
  - [Directorio JRE]/bin/sunmscapi.dll

- Sólo en Java 5 – Entornos Windows
  - [Directorio JRE]/lib/endorsed/serializer.jar
  - [Directorio JRE]/lib/endorsed/xalan.jar
  - [Directorio JRE]/lib/endorsed/xercesImpl.jar
  - [Directorio JRE]/lib/endorsed/xml-apis.jar
  - [Directorio JRE]/lib/endorsed/afirma_5_java_5.jar
  - [Directorio JRE]/lib/ext/sunmscapi.jar
  - [Directorio JRE]/bin/sunmscapi.dll

- Java 5 - Resto de sistemas
  - [Directorio JRE]/lib/endorsed/serializer.jar
  - [Directorio JRE]/lib/endorsed/xalan.jar
  - [Directorio JRE]/lib/endorsed/xercesImpl.jar
  - [Directorio JRE]/lib/endorsed/xml-apis.jar
  - [Directorio JRE]/lib/endorsed/afirma_5_java_5.jar

Si anteriormente ha instalado el Cliente @firma v2.4.1 o anteriores, es posible que este instalase las bibliotecas de NSS en alguno de los directorios del sistema. En ese caso es posible que esta versión instalada de NSS interfiera en la ejecución del Cliente @firma v3 y superiores. Las bibliotecas son:

- libnspr4
- libplc4
- libplds4
- nss3
- nssckbi
- smime3
- softokn3
- ssl3

En Windows, por ejemplo, se pueden encontrar en "System32" con la extensión ".dll". En el resto de sistemas aparecerían con extensión ".so".

5 Instalación de certificados

Para el uso del componente de firma, es necesario disponer de un certificado electrónico, el cual puede encontrarse almacenado:

- **En el Navegador**. En el almacén de certificados del navegador dentro de la pestaña "personal" aparecen los que poseen clave privada y dentro de la pestaña "otras personas" aparecen los de clave pública.

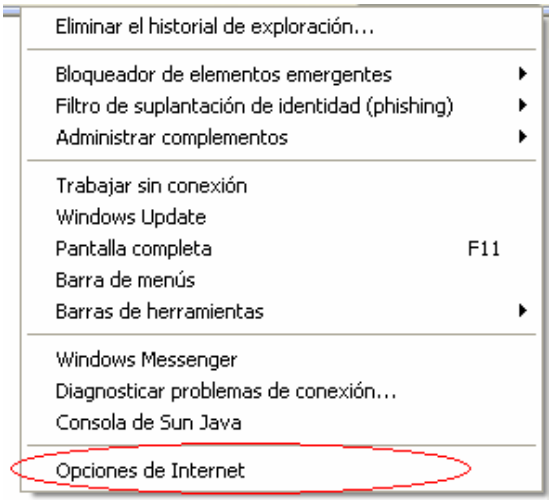
- **Tarjeta inteligente**. El DNI electrónico es un dispositivo seguro de creación de firma conforme a la norma CWA 14169. Esta norma está reconocida por la Unión Europea y se considera que la firma electrónica realizada con el DNI electrónico es equivalente a una firma manuscrita a efectos legales. Estas firmas son las más seguras porque la clave privada nunca sale de la tarjeta inteligente, por lo que no puede ser copiada por terceros.

Es importante recordar, que cuando se instala un certificado, el mismo queda instalado únicamente para el navegador en el que se realice dicha instalación, siendo necesario realizar la misma acción si se quisiera disponer del mismo certificado en otro navegador distinto.

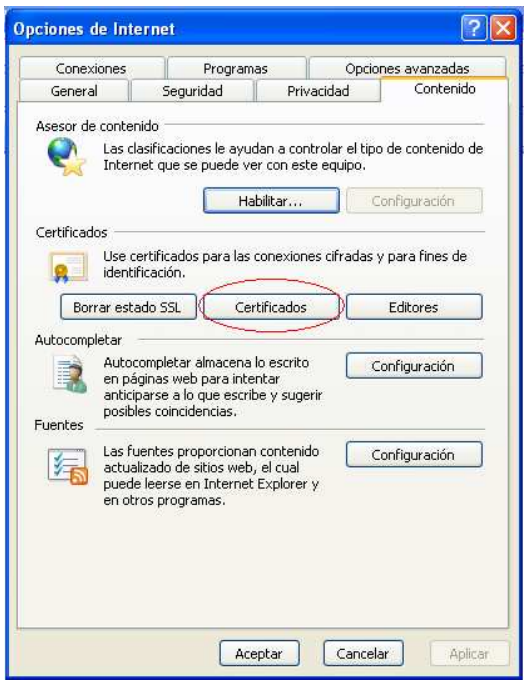
A continuación se detalla los diferentes pasos a seguir para la instalación del certificado según el lugar de almacenamiento de los mismos:

5.1 Instalación de certificados software en Internet Explorer

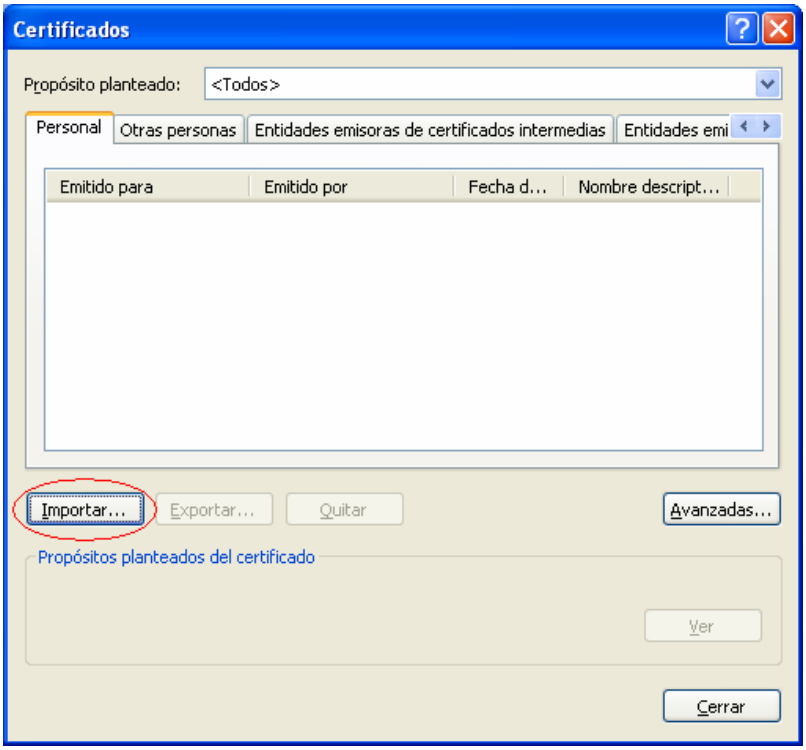
En primer lugar, en el menú superior del navegador, seleccionamos la opción "**Herramientas**" y a continuación hacemos clic sobre la opción "**Opciones de Internet**".



A continuación seleccionamos la opción "Certificados", dentro de la pestaña "**Contenido**"

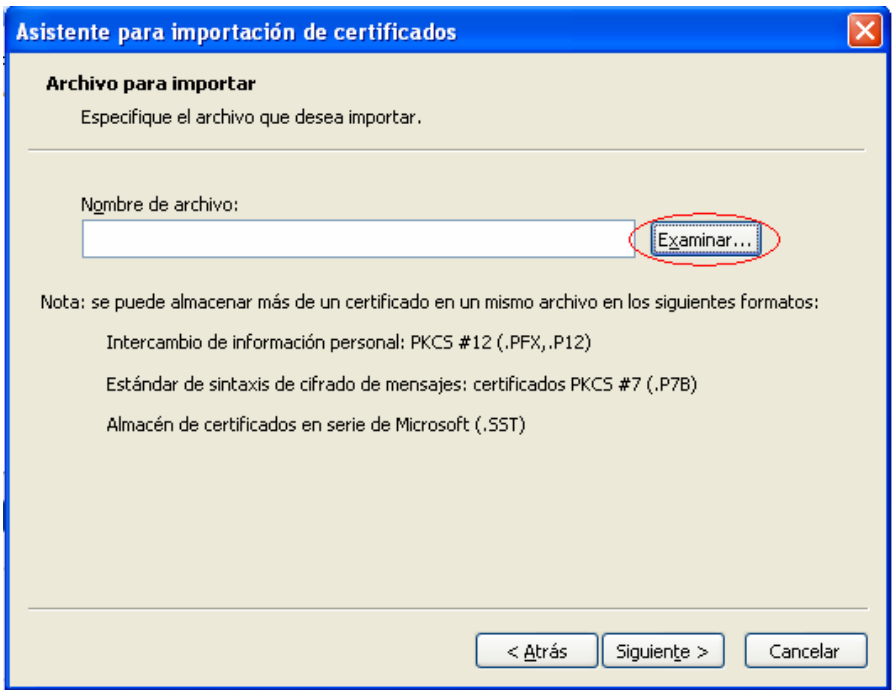


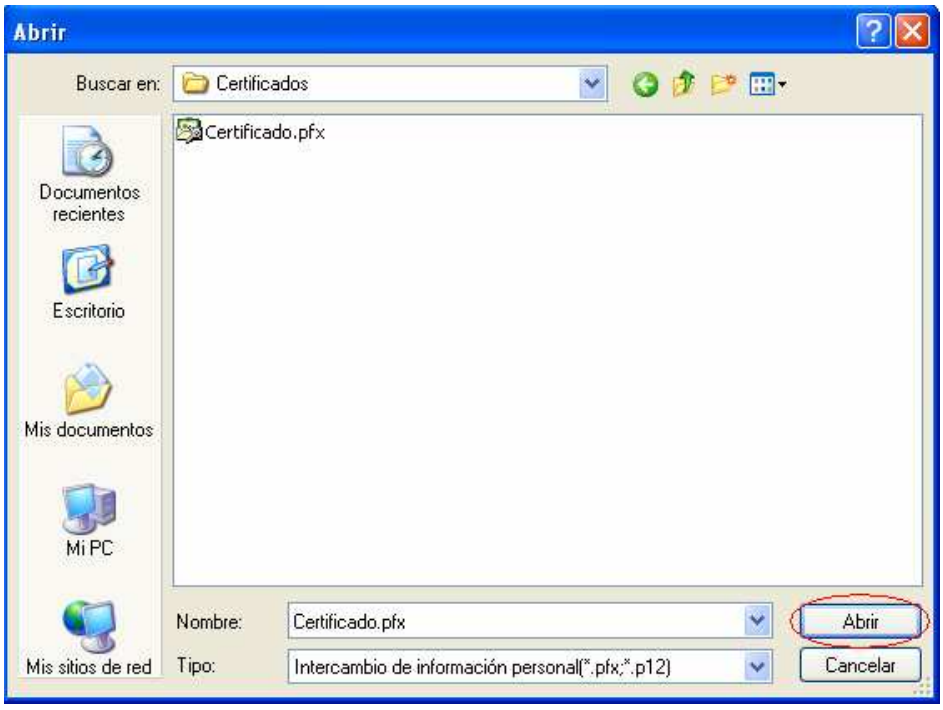
Continuamos seleccionando la opción "**Importar**", se nos abrirá el "**Asistente para importación de certificados**".



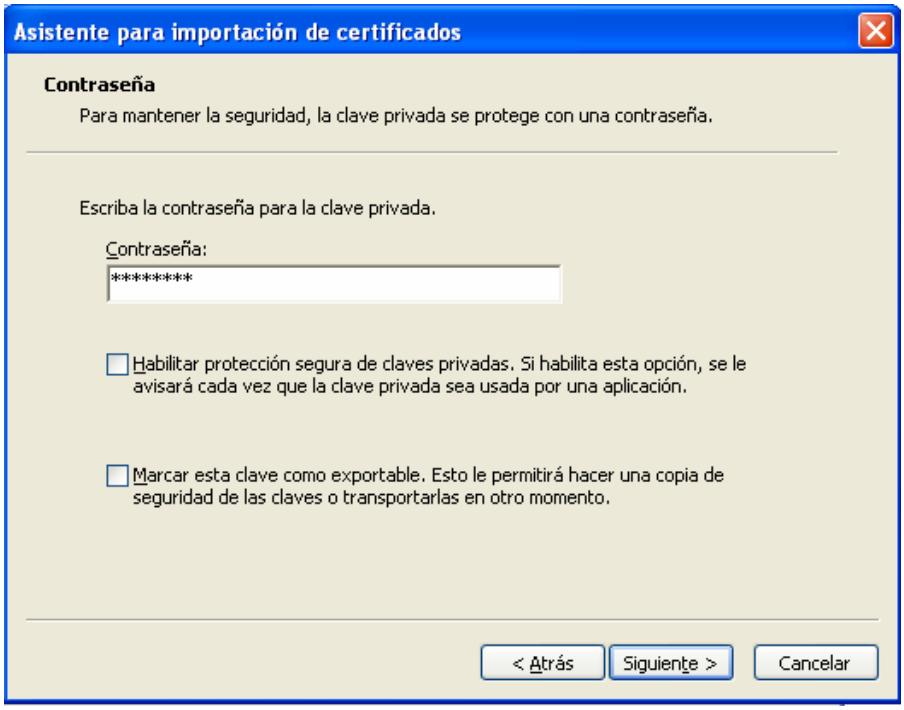
Pulsaremos "**Siguiente**" en la primera ventana del asistente, tras lo cual, nos pedirá que seleccionemos la ubicación del certificado que deseamos instalar, para lo cual, pulsaremos el botón "**Examinar...".**

Se nos abrirá una ventana en la cual tendremos que buscar el certificado que deseamos instalar, una vez encontrado, seleccionaremos el certificado y pulsaremos sobre el botón "**Abrir**".



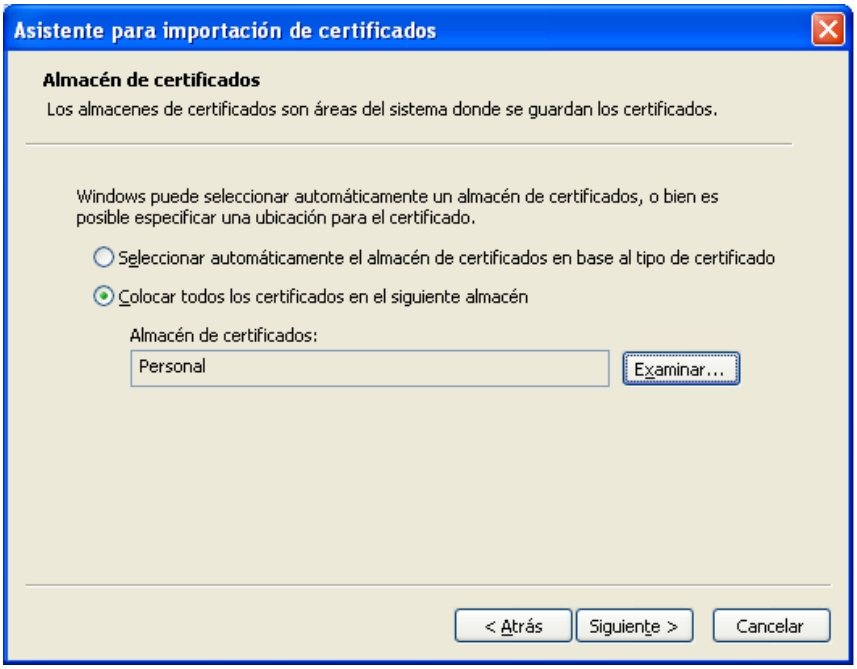


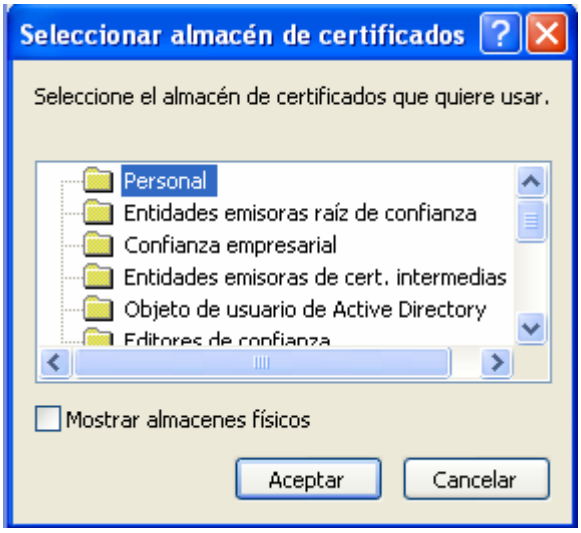
Tras seleccionar el botón "**Siguiente**", en la siguiente ventana el asistente nos pedirá que introduzcamos la contraseña usada en el cifrado del certificado, introducimos la clave y pulsamos sobre el botón "**Siguiente**"



En la siguiente ventana, el asistente nos pedirá que seleccionemos el almacén en el cual se guardará el certificado, seleccionaremos la opción "Colocar todos los certificados en el siguiente almacén".

Pulsaremos sobre el botón "**Examinar**", seleccionaremos la carpeta "**Personal**" y pulsaremos el botón "**Siguiente**".

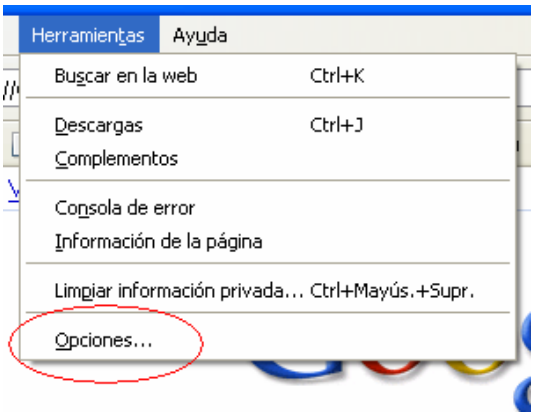




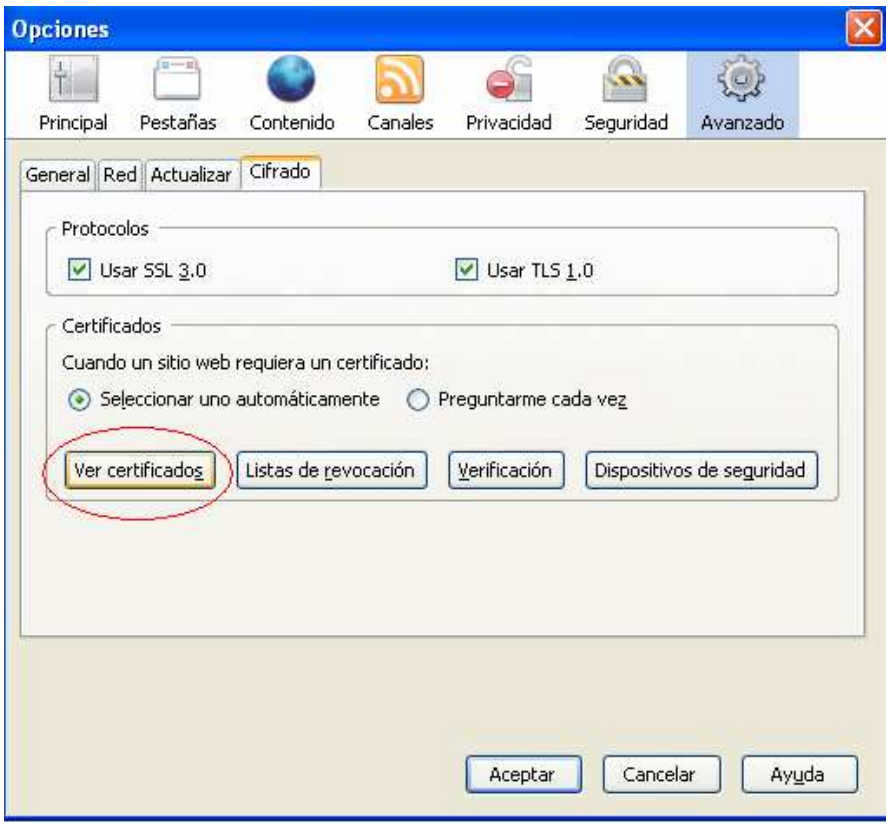
Tras este paso, el asistente nos informará de que el certificado ha quedado importado correctamente.

5.2 Instalación de certificados software en Mozilla Firefox

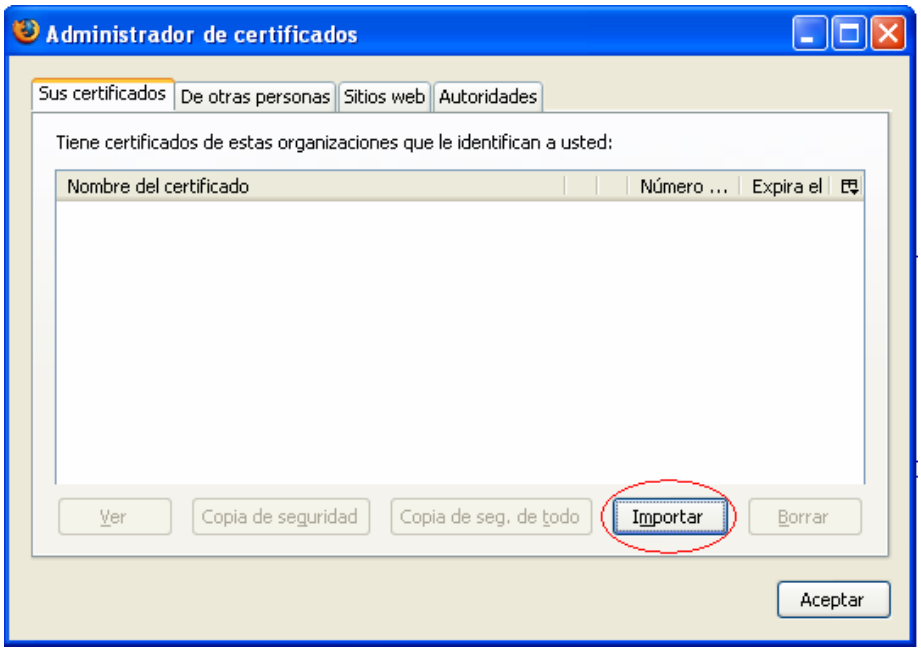
En primer lugar, en el menú superior del navegador, seleccionamos la opción "**Herramientas**" y a continuación hacemos clic sobre la opción "**Opciones**".



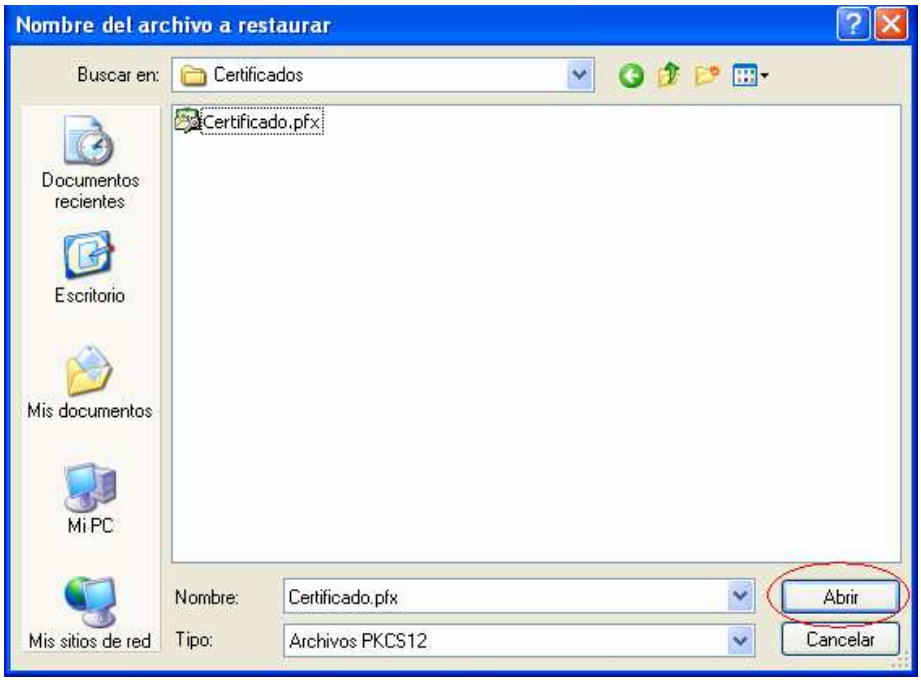
A continuación seleccionamos la pestaña "**Avanzado**" del menú superior de la nueva ventana, tras lo cual, seleccionamos la subpestaña "**Cifrado**", en la que seleccionaremos la opción "**Ver certificados**"



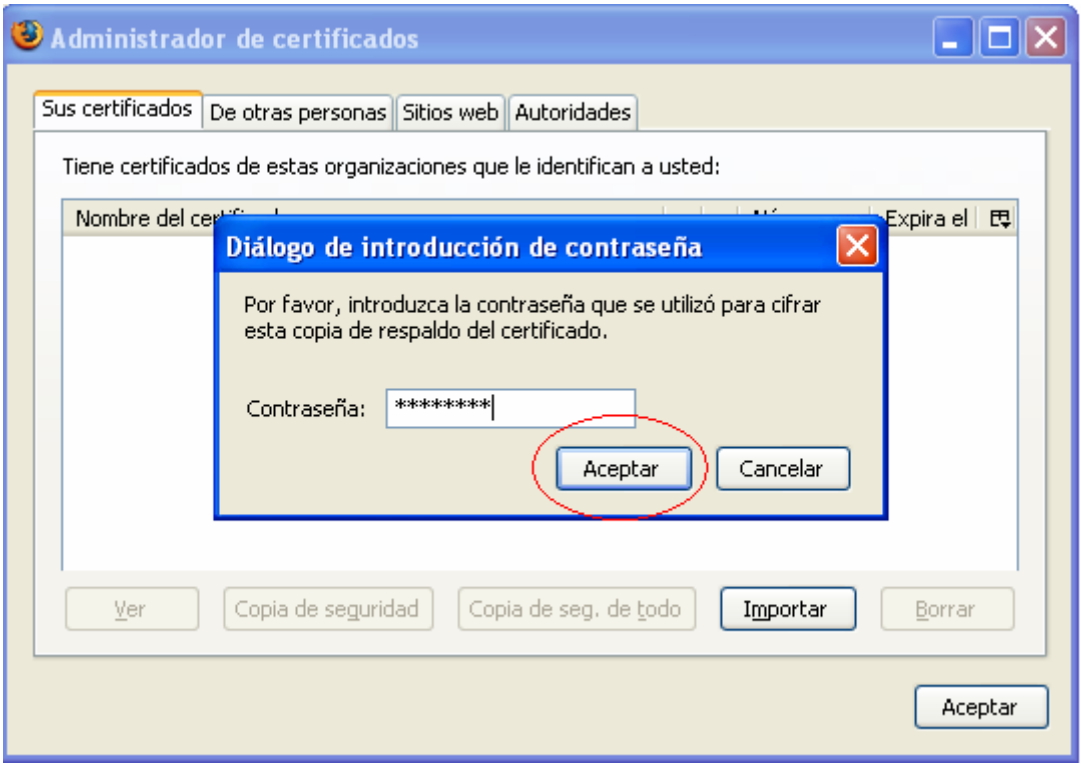
Continuamos seleccionando la opción "**Importar**", se nos abrirá una ventana en la cual tendremos que buscar el certificado que deseamos instalar, una vez encontrado, seleccionaremos el certificado y pulsaremos sobre el botón "**Abrir**".



El navegador nos pedirá que introduzcamos la contraseña usada en el cifrado del certificado, introducimos la clave y pulsamos sobre el botón "**Aceptar**".



El navegador nos pedirá que introduzcamos la contraseña usada en el cifrado del certificado, introducimos la clave y pulsamos sobre el botón "**Aceptar**".



Una vez realizado este paso, el sistema nos informará con un mensaje que el certificado ha quedado instalado de forma satisfactoria.

5.3 Instalación de certificados software en Google Chrome y Apple Safari

Los navegadores Web Google Chrome y Apple Safari no disponen de un almacén de certificados propio, en su lugar utilizan el almacén de certificados del sistema operativo que utilice el usuario. Esto es:

- En **Microsoft Windows**: El almacén de certificados que Internet Explorer.
- En **Linux**: El almacén de certificados de Mozilla Firefox.
- En **Solaris** / **OpenSolaris**: El almacén de certificados de Mozilla Firefox.
- En **Mac OS X**: El almacén de certificados del sistema operativo.

Si nuestro sistema operativo es Microsoft Windows deberemos seguir los pasos descritos en el apartado "Instalación de certificados software en Internet Explorer".

Si nuestro sistema operativo es Linux o Solaris se importarán los certificados a través de Mozilla Firefox tal como se describe en el apartado "Instalación de certificados software en Mozilla Firefox".

Si nuestro sistema operativo es Mac OS X sólo deberemos hacer doble clic sobre el certificado para solicitar su instalación y seleccionar el almacén de certificados del sistema.

Seguidamente, insertaremos la contraseña de usuario del sistema para finalizar la importación.

Aunque este proceso de instalación de certificados es el común en Mac OS X, pueden existir cambios entre cada una de sus versiones. Para conocer los detalles de cada versión acuda a la página Web de soporte de su sistema operativo. Para Mac OS X 10.6 es:

http://docs.info.apple.com/article.html?path=Mac/10.6/es/9082.html

5.4 Uso de certificados desde tarjetas inteligentes

5.4.1 DNIe (DNI electrónico)

Para la utilización del DNI electrónico es necesario contar determinados elementos hardware y software que nos van a permitir el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

a) Elementos hardware

El DNI electrónico requiere el siguiente equipamiento físico:

- Un Ordenador personal (Intel -a partir de Pentium III- o tecnología similar).
- Un lector de tarjetas inteligentes **que cumpla el estándar ISO 7816**. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados vía USB) o bien a través de una interfaz PCMCIA.

Para elegir un lector que sean compatible con el DNI electrónico verifique que, al menos,

- Cumpla el estándar ISO 7816 (1, 2 y 3).
- Soporta tarjetas asíncronas basadas en protocolos **T=0 (y T=1).**
- Soporta velocidades de comunicación mínimas de 9.600 bps.
- Soporta los estándares:
  - API PC/SC (Personal Computer/Smart Card)
  - CSP (Cryptographic Service Provider, Microsoft)

- API PKCS#11

b) Elementos software

Sistemas operativos

El DNI electrónico puede operar en diversos entornos:

- Microsoft Windows
- Linux
- Unix (Solaris)
- Mac OS X

Navegadores

El DNI electrónico es compatible con todos los navegadores:

- Microsoft Internet Explorer (versión 6.0 o superior)
- Mozilla Firefox (versión 1.5)
- Netscape (versión 4.78 o superior)

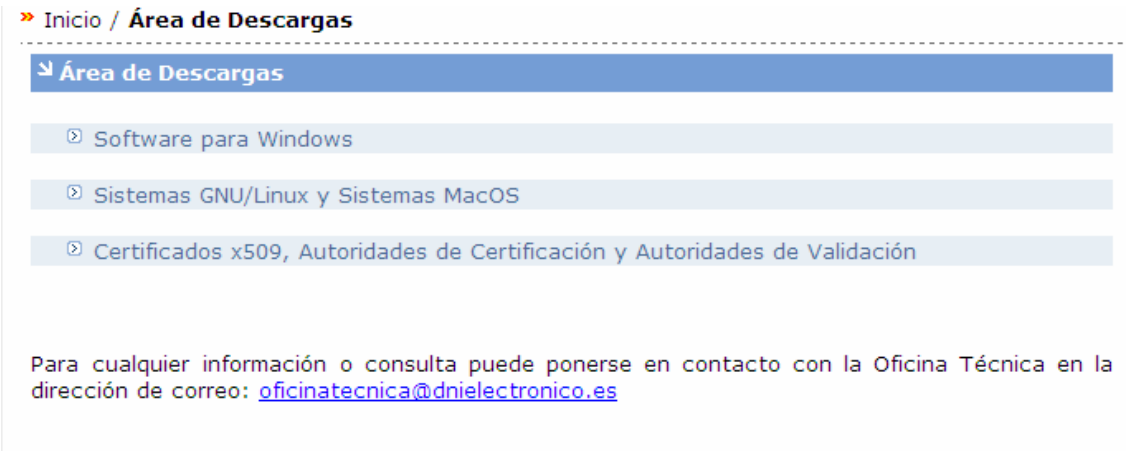
Controladores / Módulos criptográficos

Para poder interaccionar adecuadamente con las tarjetas criptográficas en general y con el DNI electrónico en particular, el equipo ha de tener instalados unas "piezas" de software denominadas módulos criptográficos.

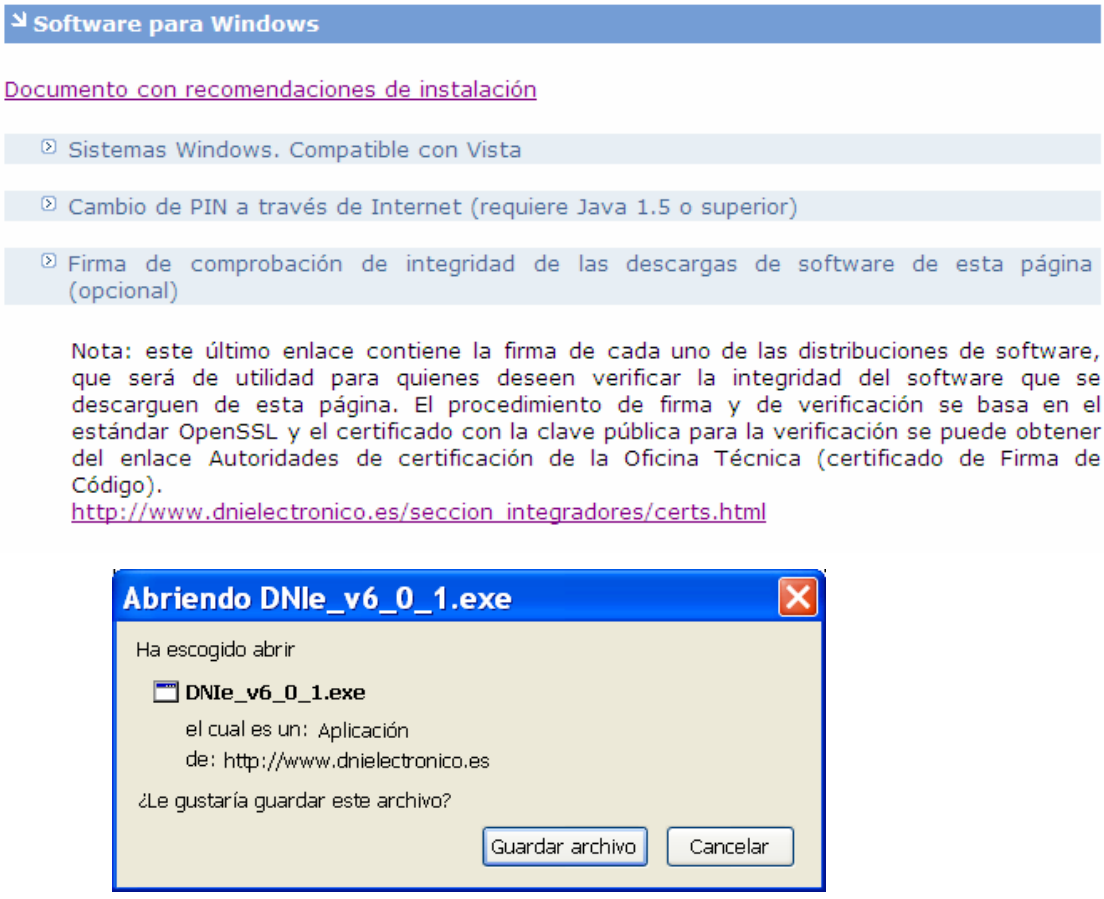
- En un entorno **Microsoft Windows**, el equipo debe tener instalado un servicio que se denomina "Cryptographic Service Provider" **(CSP).**
- En los entornos **UNIX / Linux o MAC** podemos utilizar el DNI electrónico a través de un módulo criptográfico denominado **PKCS#11.**

Tanto el **CSP** como el **PKCS#11** específico para el DNI electrónico podrán obtenerse en el Área de Descargas de la web del DNI-e, accediendo a la siguiente URL: http://www.dnielectronico.es/descargas/index.html

En esta página deberemos seleccionar la primera opción si tenemos un Sistema Operativo Windows o la segunda en caso de tener otro Sistema Operativo.



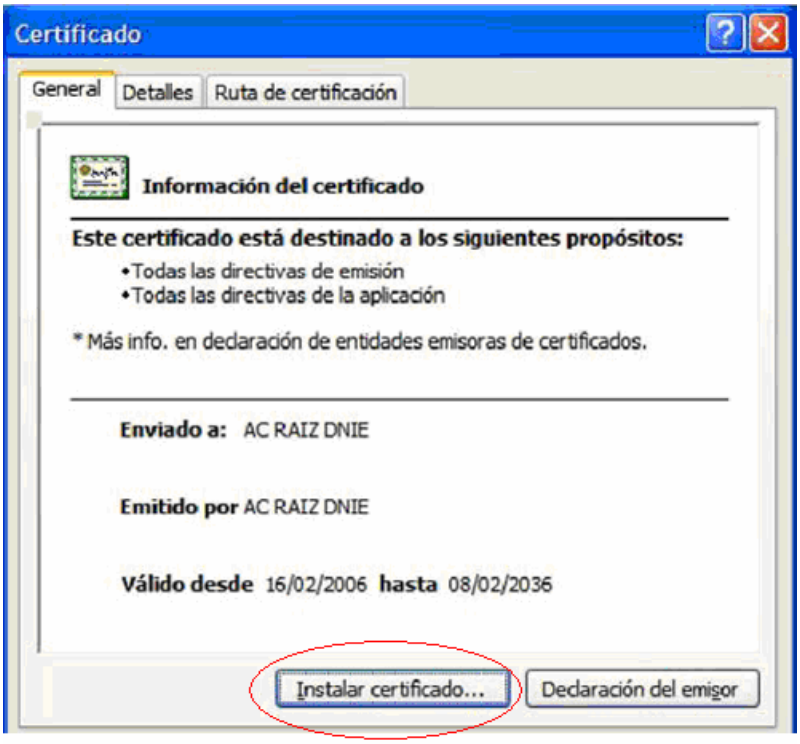
En la siguiente pantalla seleccionaremos la opción "**Sistemas Windows. Compatible con Vista",** tras lo cual se nos descargara el software. Seleccionaremos "**Guardar**" y elegiremos la carpeta deseada donde queremos que sea descargado.



Una vez descargado el fichero con la nomenclatura "DNIe_vx_j_y.zip" lo descomprimiremos y accederemos al fichero "DNIe_vx_j_y.exe".

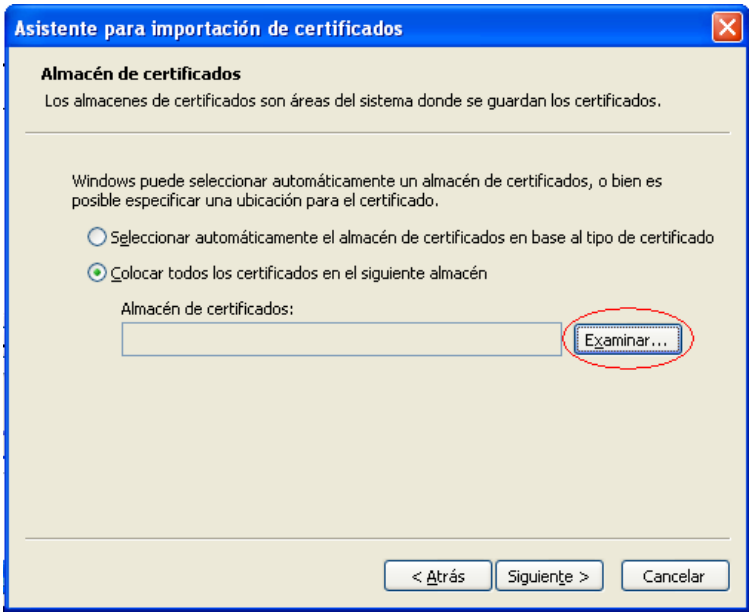
El software se instalará automáticamente y se le pedirá reiniciar el equipo.

Es posible, dependiendo de la configuración de su navegador, que nos aparezca la siguiente ventana:

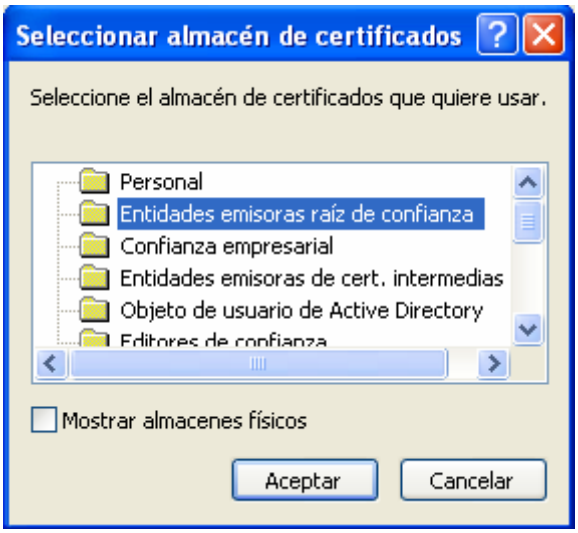


Se nos solicitará, por tanto que instalemos en el certificado raíz del DNIe, para ello deberemos seleccionar sobre "**Instalar certificado...**"

Pulsaremos sobre el botón "**Siguiente**"



Seleccionamos la opción "Colocar todos los certificados en el siguiente almacén" y pulsamos sobre el botón "**Examinar...**"



Seleccionaremos el almacén de certificados **"Entidades Emisoras Raíz de Confianza"**

En la siguiente ventana seleccionaremos la opción **"Finalizar"**

Si nos aparece la siguiente advertencia, seleccionaremos "Si" para permitir que la autoridad raíz del DNIe, se instale en el navegador y se pueda así establecer la cadena de confianza de certificación.

Tras lo cual, el software quedará instalado y listo para su uso.

Adicionalmente, para operar con un lector de tarjetas inteligentes, será necesario instalar un **driver** que, normalmente, se distribuye con el propio lector.

Nota: Para hacer uso del software de cambio de PIN virtual, deberá tener instalado en el equipo la versión **JAVA 1.5 o superior**.

Para más información puede acudir a la página http://www.dnielectronico.es o contactar con el Servicio de Atención al Ciudadano en el teléfono 900 364 463 o en el correo sac@dnielectronico.es

5.4.2 Otros certificados

En el caso de hacer uso de otro certificado desde una tarjeta inteligente deberá consultar con la entidad emisora del mismo para que le indique su forma de uso.

6 Resolución de problemas

Para la resolución de problemas relacionados con el uso del Cliente @firma, consulte la Guía de Incidencias de este o a la sección 8 de este mismo documento.

7 Glosario de términos

Firma electrónica

Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

XML Digital Signature (XMLDSig)

Es una recomendación del W3C que define una sintaxis XML para la firma digital

XML Advanced Signature (XAdES)

Es un conjunto de extensiones a las recomendaciones XML-DSig haciéndolas adecuadas para la firma electrónica avanzada.

RSA

Es un sistema criptográfico de clave pública desarrollado en 1977. En la actualidad, RSA es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

XML

Es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). Es una simplificación y adaptación del SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML). Por lo tanto XML no es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades. Algunos de estos lenguajes que usan XML para su definición son XHTML, SVG, MathML.

Office Open XML (OOXML)

Es un formato de archivo abierto y estándar cuyas extensiones más comunes son .docx, .xlsx y .pptx. Se le utiliza para representar y almacenar hojas de cálculo, diagramas, presentaciones y documentos de texto. Un archivo Office Open XML contiene principalmente datos basados en el lenguaje de marcado XML, comprimidos en un contenedor .zip específico.

Open Document Format (ODF)

Es un formato de fichero estándar para el almacenamiento de documentos ofimáticos tales como hojas de cálculo, memorandos, gráficas y presentaciones. Aunque las especificaciones fueron inicialmente elaboradas por Sun, el estándar fue desarrollado por el comité técnico para Open Office XML de la organización OASIS y está basado en un esquema XML inicialmente creado e implementado por la suite ofimática OpenOffice.org (ver OpenOffice.org XML).

ZIP

Es un formato de almacenamiento sin pérdida, muy utilizado para la compresión de datos como imágenes, programas o documentos.

PDF

Es un formato de almacenamiento de documentos, desarrollado por la empresa Adobe Systems. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto).

SHA

Es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (llamándose SHA-2 a todos ellos).

PKCS

Se refiere a un grupo de estándares de criptografía de clave pública concebidos y publicados por los laboratorios de RSA en California. A RSA Security se le asignaron los derechos de licenciamiento para la patente de algoritmo de clave asimétrica RSA y adquirió los derechos de licenciamiento para muchas otras patentes de claves.

W3C

Es un consorcio internacional que produce recomendaciones para la World Wide Web. Está dirigida por Tim Berners-Lee, el creador original de URL (Uniform Resource Locator, Localizador Uniforme de Recursos), HTTP (HyperText Transfer Protocol, Protocolo de Transferencia de HiperTexto) y HTML (Lenguaje de Marcado de HiperTexto) que son las principales tecnologías sobre las que se basa la Web.

OpenOffice.org

Es una suite ofimática libre (código abierto y distribución gratuita) que incluye herramientas como procesador de textos, hoja de cálculo, presentaciones, herramientas para el dibujo vectorial y base de datos. Está disponible para varias plataformas, tales como Microsoft Windows, GNU/Linux, BSD, Solaris y Mac OS X. Soporta numerosos formatos de archivo, incluyendo como predeterminado el formato

estándar ISO/IEC OpenDocument (ODF), entre otros formatos comunes. A febrero de 2010, OpenOffice soporta más de 110 idiomas.

Base64

Es un sistema de numeración posicional que usa 64 como base. Es la mayor potencia de dos que puede ser representada usando únicamente los caracteres imprimibles de ASCII. Esto ha propiciado su uso para codificación de correos electrónicos, PGP y otras aplicaciones. Todas las variantes famosas que se conocen con el nombre de Base64 usan el rango de caracteres A-Z, a-z y 0-9 en este orden para los primeros 62 dígitos, pero los símbolos escogidos para los últimos dos dígitos varían considerablemente de unas a otras. Otros métodos de codificación como UUEncode y las últimas versiones de binhex usan un conjunto diferente de 64 caracteres para representar 6 dígitos binarios, pero éstos nunca son llamados Base64.

ASN.1

Es una norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas. Es un protocolo de nivel de presentación en el modelo OSI.

Autoridad de Certificación (CA)

Es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.

Certificado Digital

Es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Infraestructura de Clave Pública (PKI)

Es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

8 FAQ

8.1 ¿Qué información posee un certificado digital?

Un certificado digital es, en realidad, una clave pública, con cierta información adjunta, como el nombre del propietario, el periodo de validez de la clave, etc, permitiendo:

- La autenticación del usuario.
- La confidencialidad del mensaje.
- La integridad del documento.
- El no repudio.

Los certificados digitales sólo son útiles si existe alguna Autoridad Certificadora (*Certification Authority* o CA) que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia.

El formato de certificados X.509 es un estándar del ITU-T (*International Telecommunication Union-Telecommunication Standarization Sector*) y el ISO/IEC (*International Standards Organization* / *International Electrotechnical Commission*).

Los elementos del formato de un certificado X.509 v3 son:

- Versión. El campo de versión contiene el número de versión del certificado codificado.
- Número de serie del certificado. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- Identificador del algoritmo de firmado. Este campo identifica el algoritmo empleado para firmar el certificado.
- Nombre del emisor. Este campo identifica la CA que ha firmado y emitido el certificado.
- Periodo de validez. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo.
- Nombre del sujeto. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada,

aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.

- Información de clave pública del sujeto. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.

8.2 El Cliente de Firma, cuando se ejecuta sobre Java5 actualiza algunas bibliotecas del propio entorno de ejecución. ¿Por qué? ¿Puede tener alguna repercusión sobre otras aplicaciones Java?

El cliente actualiza los API Apache Xalan y Apache Xerces de Java 5 por las últimas versiones disponibles a fecha de publicación de este. Estas versiones son completamente compatibles con las anteriores incluidas con Java 5, por lo que no introducen ningún problema de compatibilidad.

Adicionalmente, si se detecta la versión 5 de JRE se instala el proveedor de seguridad SunMSCAPI en su versión 6, ya que Java 5 originalmente no lo incluye. Esta instalación no cambia ni actualiza ninguna funcionalidad, sino que añade posibilidades completamente nuevas, por lo que no es posible que suponga problema de compatibilidad alguno.

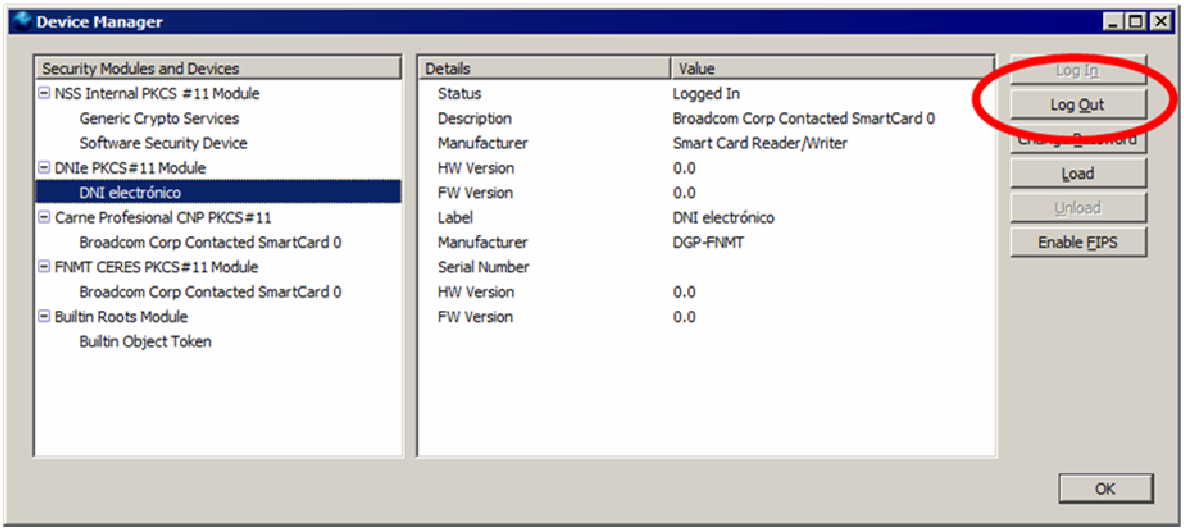
8.3 En ciertas ocasiones, usando el Cliente de Firma en Mozilla/Firefox con DNIe (DNI electrónico) éste se queda bloqueado y no muestra el diálogo de selección de certificados, desbloqueándose si retiro el DNIe del lector.

El controlador PKCS#11 del DNIe no admite que se establezcan varias sesiones de forma simultánea, y si por cualquier razón (sesión SSL, etc.) el propio navegador Web Mozilla / Firefox tiene ya establecida una comunicación con el DNIe en el momento en el que el Cliente @firma también lo necesita, este último se queda bloqueado esperando a que en navegador Mozilla / Firefox cierre su sesión. El cierre de la sesión contra el DNIe por parte de Mozilla / Firefox puede tardar varios **minutos** si el usuario no interviene, por lo que conviene forzar manualmente este cierre:

- Extraer el DNIe del lector y volverlo a insertar justo en el momento en el que se solicita la contraseña del Repositorio Central de certificados de Mozilla Firefox (antes de introducirla).

Es posible que Mozilla / Firefox reabra la sesión en la reinserción (adelantándose al Cliente @firma), por lo que quizás necesite repetir la operación.

- Podemos indicar a Mozilla / Firefox que cierre la sesión pulsando el botón "Log out" teniendo el dispositivo "DNIe PKCS#11 Module" seleccionado en la ventana "Dispositivos de Seguridad" del menú Opciones de Mozilla Firefox. Al igual que en el método anterior, a veces es necesario repetir la operación varias veces, ya que Mozilla / Firefox reabre automáticamente la comunicación con el DNIe sin dar tiempo al Cliente @firma a utilizarlo. En otras ocasiones, el botón aparece deshabilitado aunque Mozilla / Firefox tenga una sesión abierta contra el dispositivo, con lo que no es posible aplicar este método.



Este problema se da predominantemente en Linux, Solaris y Mac OS X. No se ha detectado en ningún caso en ninguna versión de Windows.

Una solución alternativa en sistemas basados en UNIX (Linux, Solaris, Mac OS X) es modificar la configuración de OpenSC (producto en el que se basa el controlador PKCS#11 del DNIe en estas plataformas indicando que nunca se debe bloquear el acceso a las tarjetas inteligentes.

Para realizar esta indicación debe modificar el archivo de configuración de OpenSC, normalmente situado en `/etc/opensc/opensc.conf` y asegurarse de que contiene una línea descomentada con la opción **lock_login=false;** :

```
# By default, the OpenSC PKCS#11 module will lock your card
# once you authenticate to the card via C_Login.
# This is to prevent other users or other applications
# from connecting to the card and perform crypto operations
```

```
# (which may be possible because you have already authenticated
# with the card). Thus this setting is very secure.
#
# This behavior is a known violation of PKCS#11 specification,
# and is forced due to limitation of the OpenSC framework.
#
# However now once one application has started using your
# card with C_Login, no other application can use it, until
# the first is done and calls C_Logout or C_Finalize.
# In the case of many PKCS#11 application this does not happen
# until you exit the application.
#
# Thus it is impossible to use several smart card aware
# applications at the same time, e.g. you cannot run both
# Firefox and Thunderbird at the same time, if both are
# configured to use your smart card.
#
# Default: true
lock_login = false;
```

Dado que este cambio puede tener implicaciones de seguridad con otras tarjetas inteligentes (la seguridad del DNIe no se ve comprometida por él, dado que implementa medidas adicionales de protección, como la implementación de la normativa CWA-14890), realice únicamente estas modificaciones si está completamente seguro de sus implicaciones.

En ciertas distribuciones de Linux (como Guadalinex v6) el cambio no tienen ningún efecto sobre los bloqueos con DNIe, por lo que no solucionará el problema).

8.4 Pérdida de foco en ventanas

En ocasiones, las ventanas del cliente pierden el foco, haciendo imposible la interacción del usuario. Este error se debe a un error reconocido por Sun Microsystems a partir del JRE 1.5.0 que bloquea ciertas ventanas Java en Internet Explorer y Mozilla, perdiendo el foco y haciendo imposible la interacción con el usuario.

En muchos casos este error se solventa al cambiar el foco a otras ventanas, o minimizar/maximizar el navegador, para intentar que recupere el foco, aunque no siempre resulta efectivo, por lo que se deberá reiniciar el navegador y reintentar la operación. En caso de problemas graves con alguna aplicación Web concreta, es recomendable el uso de Internet Explorer, en donde el problema aparece en menor medida.

9 Información de contacto

Soporte a la Administración Electrónica

Consejería de Hacienda y Administración Pública

Dirección General de Tecnologías para Hacienda y la Administración Electrónica

soporte.admonelectronica@juntadeandalucia.es