Guía de Incidencias del

Índice

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 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 enumerar las dificultades típicas que pueden encontrar los integradores o sus usuarios durante la instalación, despliegue, integración o uso del Cliente @firma, así como las vías de resolución o paliación de estas.

3 Incidencias conocidas del núcleo del cliente @firma

3.1 Incidencias generales

El navegador no carga correctamente los Applets de Java pese a tener Java instalado

Los navegadores actuales, por motivos de seguridad, requieren acciones adicionales de configuración para habilitar los Applets de Java.

Siga las instrucciones del fabricante de su navegador Web y sistema operativo para habilitar los Applets de Java en su navegador, y compruebe adicionalmente que ha cumplido los requisitos que se detallan en la página de Oracle Java:

- http://java.com/en/download/help/enable_browser.xml

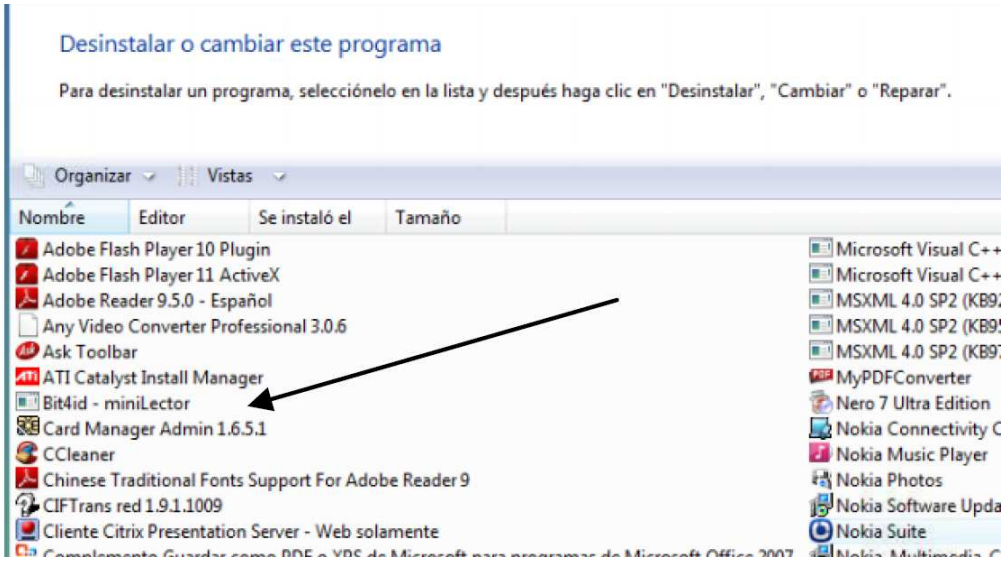
Es igualmente conveniente comprobar, antes de intentar cargar el Cliente @firma, que el Applet de prueba de Oracle Java se carga adecuadamente, para distinguir problemas de configuración con problemas propios del Applet o MiniApplet Cliente @firma:

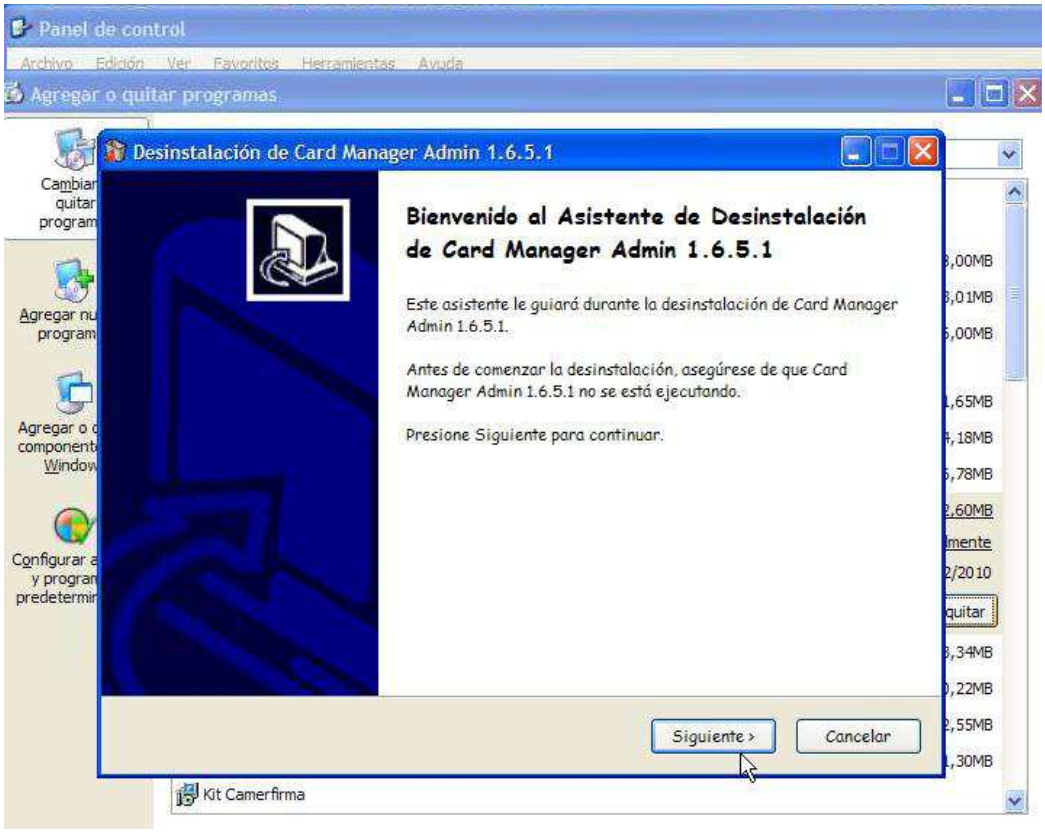
- https://www.java.com/verify/

No es posible realizar firmas electrónicas con cierto hardware criptográfico (tarjetas inteligentes y dispositivos USB) de CamerFirma. El proceso siempre termina en error

Algunas versiones antiguas de controladores CSP y PKCS#11 para hardware de CamerFirma contienen errores que provocan errores al realizar firmas electrónicas. Para corregirlo es necesario actualizar los controladores por la última versión, siguiendo el proceso descrito a continuación (para sistemas Windows, consulte con su suministrador de hardware y software criptográfico para otros sistemas operativos):

1) Desinstale el programa “CARD MANAGER ADMIN 1.6.xxx“ desde “Agregar o quitar programas“ o “programas y características“. Tras la desinstalación, reinicie el equipo. En caso de no tener el instalado el programa “CARD MANAGER“ pase directamente al paso 3.





2) Descargue los controladores más actuales, para ello acceda a la página Web de CamerFirma (http://www.camerfirma.es), entre en el Área de Usuario / Área de Descargas y ahí seleccione el Kit De Descargas. Pulse en “Descargar”, seleccionando entonces el “Kit De CamerFirma” correspondiente a su modelo “Bit4Id” y ejecute el programa de instalación descargado. Una vez finalizada la instalación, reinicie el equipo.


Camerfirma
Certificado Digital
BUSCAR Buscar en la web...
902 36 12 07
>> inicio
CAMERFIRMA
CERTIFICADOS
PRODUCTOS
SERVICIOS
ÁREA DE USUARIO
AYUDA
Camerfirma / AC Camerfirma SA
Business Wear
by camerfirma
Portátil....Seguro....Sin Controlador...Independiente...Personalizable
ÚLTIMAS NOTICIAS
02/01/12 02/01/2012CA/BROWSER FORUM PUBLÍCA "REQUISITOS BÁSICOS PARA LA EMISIÓN DE CERTIFICADOS SSL/TLS".
19/10/11 LA CÁMARA DE COMERCIO DE BADAJOZ Y EL COLEGIO DE INGENIEROS INDUSTRIALES DE EXTREMADURA HAN FIRMADO HOY UN CONTRATO DE PRESTACIÓN DE SERVICIOS PARA FACILITAR, MEDIANTE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN, LA EMISIÓN Y LA ENTREGA DE CERTIFICADOS DIGITALES.
¿Que Certificado NECESITO?
SOLICITA tu Certificado
DESCARGA tu Certificado
Notas Técnicas
Notificaciones electrónicas obligatorias
Agencia Tributaria
tienda
contacto
oficinas
catálogo
Certificados de FIRMA DE CÓDIGO
Reconocidos por Sun Microsystems
dni Solicitud certificado

Camerfirma / AC Camerfirma SA / Área de usuario / Área de Descargas

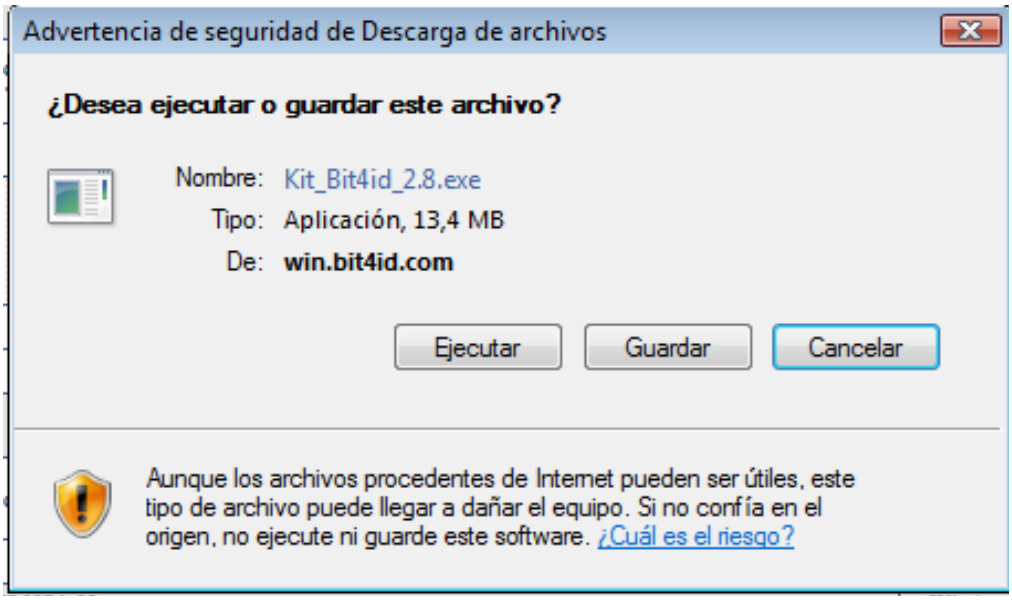
Descargas

►Kit Camerfirma y controladores para las tarjetas y lectores.

Para descargar el Kit Camerfirma y los controladores de los diferentes lectores y tarjetas, así como a los manuales de instalación, accedan al siguiente enlace: Descargar.

►Descarga de eSigna Viewer.

Visor gratuito de archivos firmados electrónicamente con los formatos estándar PKCS#7 y XMLDSig (Extensión XADES).
Descargar



3) Acceda a la carpeta `c:\Windows\System32` y, si existen, elimine estos tres ficheros (puede requerir permisos de administrador para completar este punto):

   a) `Sysgillo.cpl`

   b) `Sysgillocpsetup`

   c) `Sysgillocsp.dll`

   Una vez completados estos tres pasos tendrá en su equipo la última versión de los controladores, que están libres de errores y permiten realizar firmas electrónicas con @firma.

En ciertas instalaciones de versiones compatibles del Entorno de Ejecución de Java (JRE) el Cliente no funciona adecuadamente

Una de las posibles causas de que el Cliente no funcione en instalaciones del JRE (usando versiones y entornos declarados como compatibles) es que otra aplicación ejecutada previamente haya corrompido el entorno de ejecución de Java instalando incorrectamente bibliotecas como extensiones.

El Cliente @firma puede no funcionar cuando alguna de las bibliotecas que usa han sido instaladas como extensiones del JRE. Para restaurar el funcionamiento normal del JRE debe seguir los siguientes pasos:

1. Localizar el directorio de extensiones de su entorno de ejecución de Java
   - La opción más común es el directorio `lib/ext` dentro de la carpeta de instalación del JRE
   - Debe también revisar las carpetas de extensiones comunes:
     - `/usr/jdk/packages/lib/ext` en Sun Solaris y OpenSolaris
     - `/usr/java/packages/lib/ext` en Linux
     - `%SystemRoot%\Sun\Java\lib\ext` en Microsoft Windows
2. Eliminar las siguientes bibliotecas:
   - BouncyCastle
     - `bcprov*.jar`
     - `bcmail*.jar`
     - `bctsp*.jar`
     - `bcpq*.jar`
   - JXAdES
   - iText
     - `iText*.jar`
   - Apache Commons
   - Apache Oro
   - JMIMEMagic
3. Notificar al proveedor de la aplicación que instaló inapropiadamente bibliotecas como extensiones para que corrija este comportamiento en sus aplicativos.

Puede encontrar una pequeña guía sobre el uso e instalación de extensiones al entorno de ejecución de Java en: http://download.oracle.com/javase/tutorial/ext/basics/install.html

Cuando utilizo varias tarjetas inteligentes de firma electrónica y/o varios lectores de tarjetas inteligentes a veces no se muestran todos los certificados.

El Cliente @firma inicializa durante la primera operación criptográfica las tarjetas inteligentes encontradas en el sistema, y supone que no va a variar durante toda la ejecución del programa.

El insertar o extraer tarjetas durante la ejecución del programa puede ocasionar fallos ocasionales. No inserte o extraiga tarjetas mientras el Cliente @firma esté en ejecución.

Adicionalmente, es conveniente tener insertada únicamente la tarjeta que desea usar para realizar las operaciones de firma. Si dos tarjetas del mismo tipo (que usen el mismo controlador PKCS#11) están insertadas, el Cliente @firma utilizará únicamente la insertada en el primer lector encontrado en el sistema.

El conectar y desconectar lectores de tarjetas, o cambiarlos de puerto USB, puede ocasionar fallos ocasionales. No conecte o desconecte lectores de tarjetas inteligentes mientras el Cliente @firma esté en ejecución.

Si es absolutamente indispensable realizar inserciones o extracciones de tarjetas durante la ejecución del Cliente @firma, reintente la operación si esta fallase para permitir al Cliente @firma reconfigurarse.

Cuando se recuperan desde Java ficheros XML en formato Base64 como resultado de operaciones de firma la codificación de caracteres se corrompe.

Durante la creación de un *String* de Java a partir de un binario obtenido a su vez de la decodificación de un Base64 se pueden pervertir los caracteres especiales de los ficheros XML si se indica una codificación errónea en el constructor de la clase *String*. La solución más rápida es no indicar codificación y confiar en las capacidades de Java de auto-detección de formato de caracteres. Si esta auto-detección de Java sigue proporcionando resultados incorrectos siempre puede obtener los XML directamente como texto en vez de en Base64 usando el método `getSignatureText()` en vez de `getSignatureBase64Encoded()`.

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

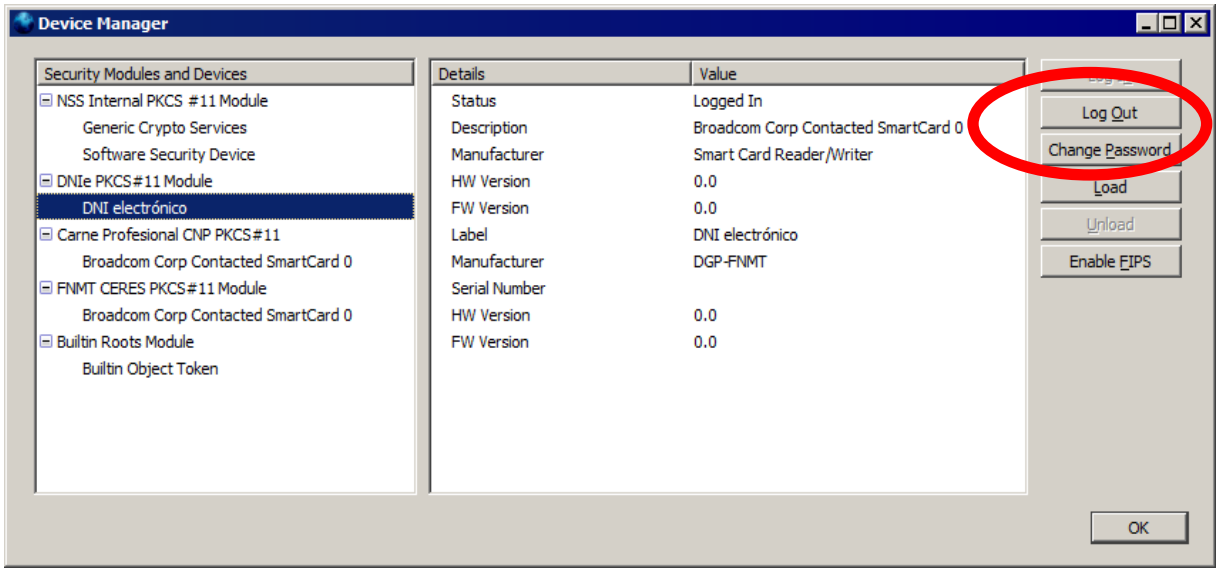
Ciertas versiones del controlador PKCS#11 del DNIe no admiten que se establezcan varias sesiones de forma simultánea, y si por cualquier razón (sesión SSL, etc.) el propio navegador Web Mozilla / Firefox tiene ya establecida una comunicación con el DNIe en el momento en el que el Cliente @firma también lo necesita, este último se queda bloqueado esperando a que en navegador Mozilla / Firefox cierre su sesión.

Para evitar estos problemas, instale la última versión de los controladores de DNIe OpenDNIe disponibles en http://opendnie.cenatic.es/, que corrigen en cierta medida estos problemas.

Si no desea o no puede actualizar los controladores, es necesario cerrar las sesiones activas contra el DNIe para que el Applet @firma pueda abrir una propia.

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).

En algunas ocasiones, se ha detectado que este cambio en la configuración de OpenSC afecta a la comunicación con la tarjeta inteligente, provocando que el PIN de la tarjeta llegue corrupto. Asegúrese de introducir correctamente el PIN de su tarjeta y, en caso de que vuelva a solicitarse, cancele la operación y deshaga el cambio en la configuración para evitar que repetidos intentos bloqueen su DNIe.

La Web donde está deplegado el Cliente solicita certificado cliente, y aunque este funciona correctamente en Internet Explorer y otros navegadores, no ocurre lo mismo con Mozilla / Firefox

Consulte el apartado “Despliegue del cliente en servidores Web que requieren identificación de los usuarios mediante certificado cliente” del manual del integrador para más información de cómo resolver este problema de configuración de Mozilla / Firefox.

El Cliente deja de funcionar tras ejecutar la Aplicación Web de firma de la Ventanilla Única de la Seguridad Social

El aplicativo de Ventanilla Única de la Seguridad Social hace uso de bibliotecas Java modificadas que son incompatibles con el Cliente @firma.

Problema en la codificación a Base64 de ficheros grandes

En determinados entornos de usuario, existe un problema en la codificación de ficheros a Base 64 que lleva al cierre abrupto de la máquina virtual de Java y el subsiguiente error en la ejecución del propio cliente. Este problema surge al utilizar los siguientes métodos del cliente para la conversión de ficheros grandes a base 64:

- `getFileBase64Encoded(boolean showProgress);`
- `getFileBase64Encoded(boolean showProgress, String strUri);`
- `getSignatureBase64Encoded();`

En la incidencia "No es posible realizar firmas de más de 4MB" podrá encontrar alternativas que pueden evitar que le surja este problema.

No es posible realizar firmas de más de 4MB

Al ejecutar el Cliente @firma en un entorno con Java 6u10 o superior y el plugin de nueva generación activado (configuración por defecto), nos encontramos con que no es posible convertir ficheros de datos mayores de 4MB a cadenas Base64. Esta operación es necesaria para posteriormente adjuntar los datos firmados (o la firma implícita generada) al formulario Web a través del cual se enviará la información al servidor. Esta limitación también puede afectar a la generación de firmas XML implícitas de ficheros mayores de 4MB.

Este problema no tiene solución actualmente pero es posible realizar algunas prácticas con las que es posible evitarlo en caso de que el propio fichero de datos no sea mayor de este tamaño.

1. Evalúe si es necesario que su sistema firme los ficheros adjuntos a una transacción o si basta con firmar la propia transacción. Esto podría hacerse mediante un XML en el que se almacenen los datos de la transacción (identificador, los datos proporcionados por el usuario, nombre de los ficheros adjuntos y su hash,…).
2. Si su sistema realiza firmas de ficheros seleccionados por el usuario y se van a admitir ficheros mayores de 4MB, evalúe el uso de firmas binarias (CAdES), que son de menor tamaño, en lugar de firmas XML (XAdES). El problema comentado puede afectar a la generación de firmas XML (XMLdSig / XAdES) de ficheros binarios mayores de 4MB.
3. Si es necesario el envío de ficheros mayores de 4MB al servidor, deberán enviarse mediante el componente File de los formularios HTML. Para esto, tendremos que firmar previamente los datos y obligar a que sea el propio usuario quien seleccione los ficheros de firma generados. Se propone el siguiente modelo de aplicación Web:
    a. Mostrar al usuario el formulario Web con la información que debe rellenar. Esto puede hacerse en una única página Web o en varias si la cantidad de datos lo requiere.
    b. En el punto que corresponda del formulario, se dará la opción al usuario de seleccionar los ficheros que desea adjuntar al mismo. Esto abrirá una nueva ventana en donde se cargará el Cliente @firma y, mediante el método descrito en el apartado 13.2 del Manual del Integrador, se dará al usuario la posibilidad de firmar los ficheros. En este caso, en lugar de adjuntar el resultado de la firma al formulario Web, se le permitirá almacenarla en disco, notificándole que esta es la firma electrónica generada que posteriormente se deberá adjuntar al formulario y que, si lo desea, puede conservar como parte del resguardo de la transacción. En este paso se pueden firmar tantos ficheros como se deseen. Consulte el apartado 9.1 del Manual del Integrador del Cliente @firma para conocer como almacenar las firmas en el sistema del usuario.
    c. De vuelta al formulario principal y al final del mismo se mostrará un botón Aceptar que redirigirá al usuario a una nueva página en la que se cargará el Cliente @firma y se mostrará el resumen de los datos del formulario para que confirme que son válidos. También en esta página se mostrarán los componentes necesarios de tipo File de HTML para que el usuario cargue los ficheros de firma generados en el paso anterior (y los documentos firmados en caso de firmas explícitas). En esta

ocasión no se utilizará el Cliente para cargar los ficheros de firma, únicamente el componente File

d. Tras revisar los datos y seleccionar los ficheros necesarios, el usuario podrá enviar el formulario para finalizar el trámite. Al pulsar el botón Enviar, se firmará la transacción con el Cliente @firma y seguidamente se enviará el formulario con esta firma.

    - El concepto de transacción deberá definirse para cada sistema. Puede ser, por ejemplo, un XML que contenga todos los datos del formulario y la relación de ficheros adjuntos (nombres y hashes).

NOTA: En sistemas con Java 6 y el Plugin de próxima generación desactivado la limitación se encuentra en torno a los 50MB. Sin embargo, no debe presuponerse que el usuario operará desde un entorno de este tipo ya que está obsoleto y no es la configuración por defecto.

No se detecta la inserción/extracción del DNIe en el lector (u otra tarjeta inteligente)

A veces puede ocurrir que el navegador no detecta la extracción o introducción del DNIe (u otra tarjeta inteligente) en el lector, por lo que si no hemos introducido la tarjeta previamente a que se arranque el cliente de firma, no se encontrará el certificado. Otro posible caso es que una vez cargado el cliente, se extraiga la tarjeta y, al realizar una operación de firma, el navegador muestre los certificados de la tarjeta (aunque ya no esté presente) fallando al intentar utilizarlo.

Este es un problema del navegador en la gestión de los dispositivos criptográficos (PKCS#11 para Mozilla y CSP para Internet Explorer), que no informa a la sesión abierta en el almacén de certificados de los cambios que se producen en el mismo.

La solución más rápida al problema es el insertar la tarjeta antes de que se produzca la carga del cliente de firma.

No se detecta el certificado del DNIe tras una autenticación infructuosa

Cuando se introduce mal el PIN del DNIe, ocurre que el navegador no detecta sus certificados, incluso aunque posteriormente el usuario sí lo introduzca correctamente.

El problema viene del CSP (Cryptographic Service Provider) del DNI electrónico y la mejor forma de solucionarlo es extraer e insertar el DNIe en el lector de tarjeta y volverse a autenticar.

3.2 Despliegue del Cliente

Cuando se despliega el Cliente en entornos donde las páginas HTML se generan dinámicamente no es posible cargar el Applet

Las páginas HTML provistas como ejemplo necesitan ciertos cambios cuando se quiere desplegar el Cliente en servidores donde las páginas se generan dinámicamente (como por ejemplo, Portlets en un Servidor de Portales):

- Las bibliotecas Java del cliente (JAR) deben situarse en una dirección estática dentro del servidor Web, como por ejemplo: *http://dirección/directorio_clases*
- El JavaScript (las bibliotecas JS) debe incluirse dentro de la página que invoca al Applet y puede generarse dinámicamente, pero debe editarse el fichero *constantes.js* para indicar su localización mediante una URL absoluta:

```
/*************************************************************************
 * Ruta a los instalables.                                               *
 * Si no se establece, supone que estan en el mismo directorio (que el HTML). *
 *************************************************************************/
var baseDownloadURL = http://direccion/directorio_clases;

/*************************************************************************
 * Ruta al instalador.                                                   *
 * Si no se establece, supone que estan en el mismo directorio (que el HTML).  *
 *************************************************************************/
var base = http://direccion/directorio_clases;
```

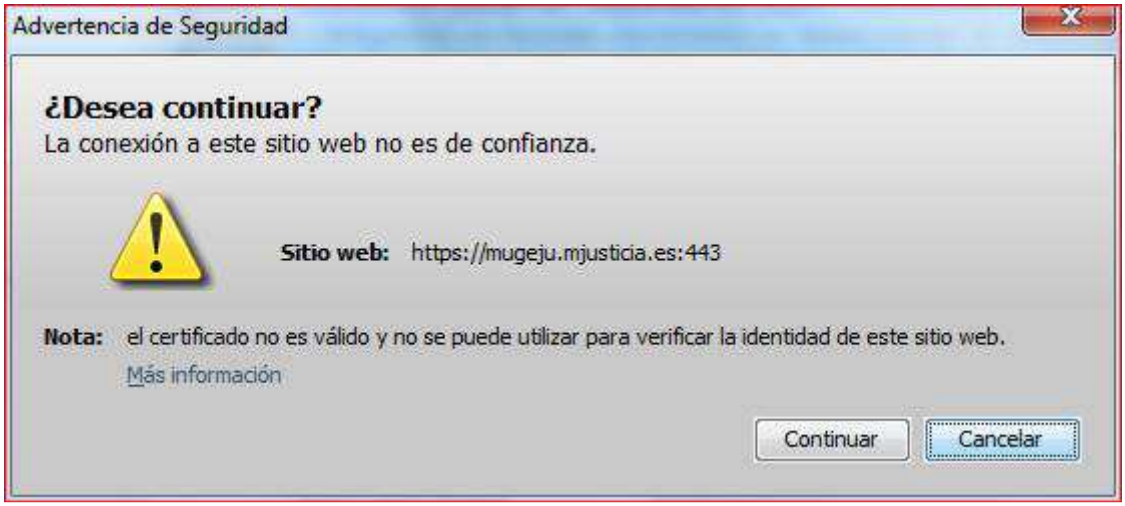
Se producen errores en la carga del Cliente con Java 7u65

Java 7u65 introduce un error que impide la ejecución de Applet cuando se le proporcionan comandos a la máquina virtual, como es el caso del Cliente @firma que indica la memoria mínima a reservar. Actualice a la última versión de Java 7 disponible para solventar el problema.

Google Chrome muestra diálogos de advertencia de seguridad a los usuarios cuando el MiniApplet se publica bajo SSL

Para la ejecución de Applets de Java, Chrome cruza la verificación del certificado del servidor SSL no solo contra la lista de raíces de confianza del sistema operativo, sino también contra la lista equivalente del entorno de ejecución de Java.

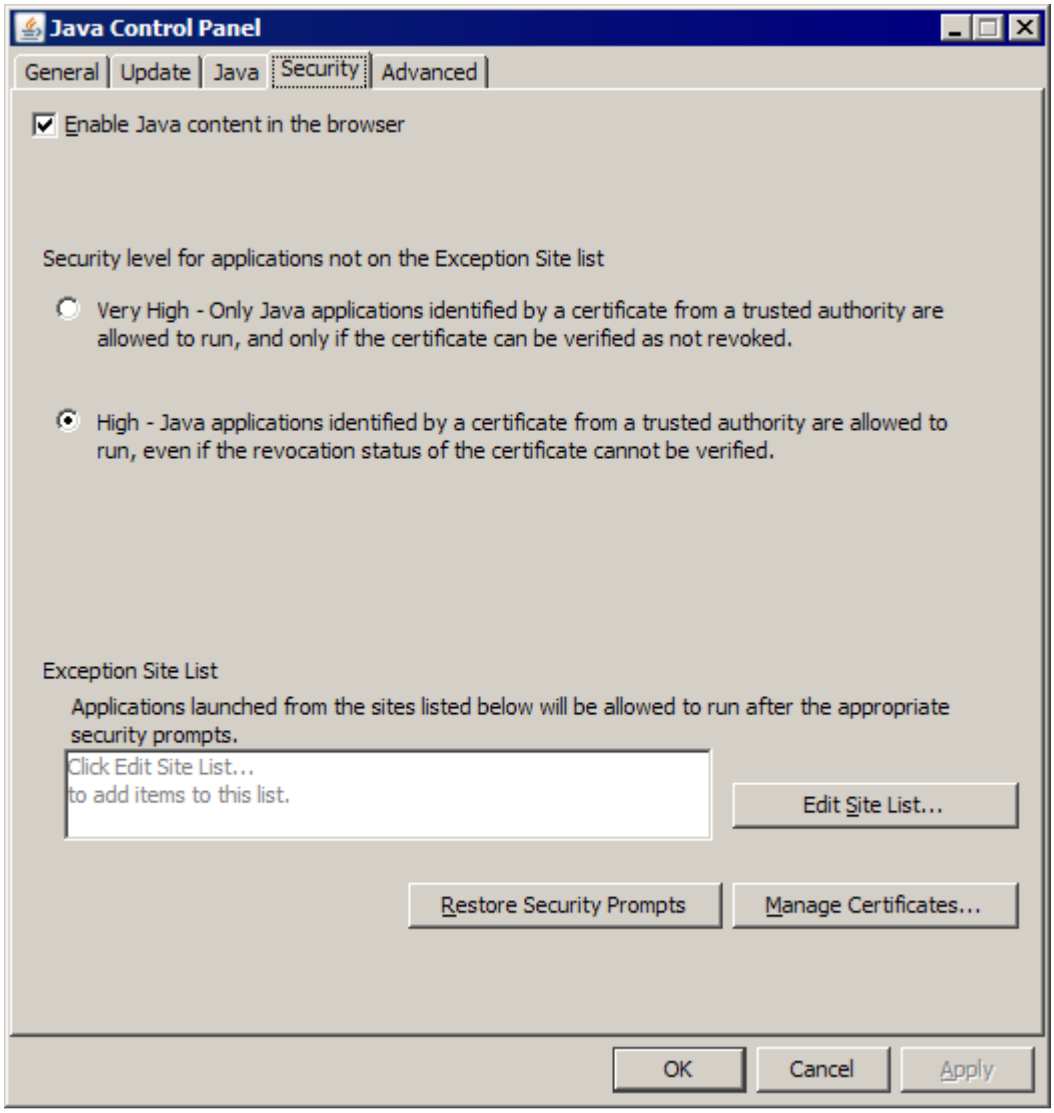
Así, cuando se carga un Applet desde un sitio SSL cuyo certificado no sea de confianza por Java, aunque sí lo sea para el sistema operativo, se muestra un diálogo al usuario como el siguiente:



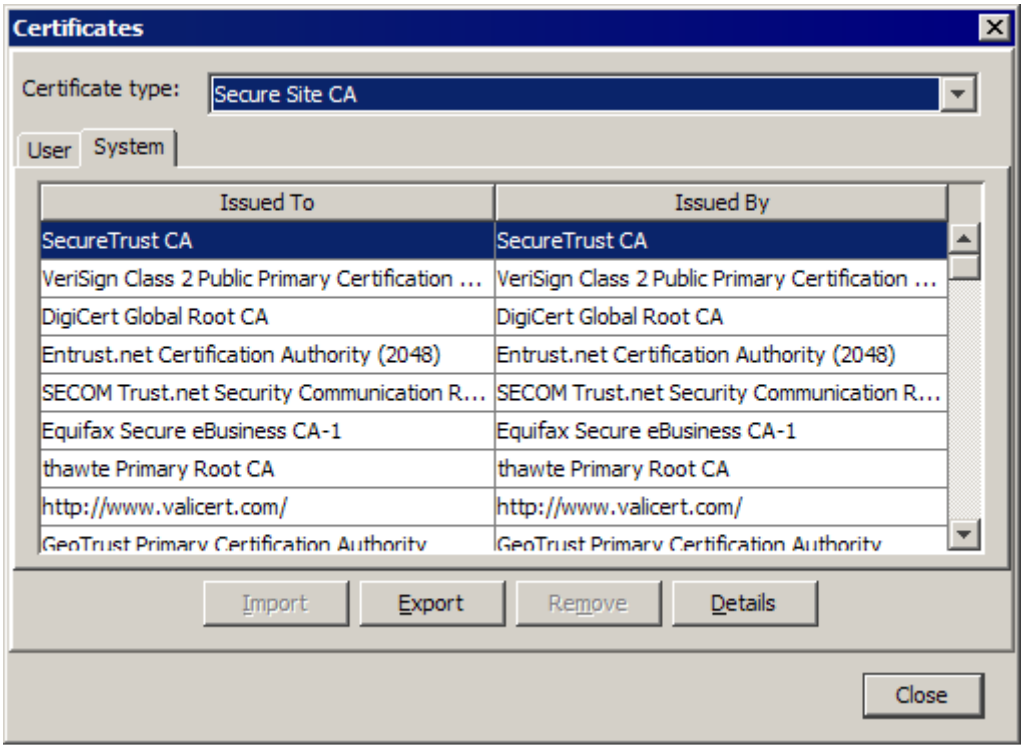
Esta situación es muy común en servidores Web con certificados de FNMT-RCM-CERES.

La forma directa de evitar estos diálogos es reemplazar los certificados de servidor de FNMT-RCM-CERES por otros emitidos por una Autoridad de Certificación reconocida universalmente (por Windows, Mozilla, Java, etc.).

Si no fuese posible este reemplazo, la única forma de evitarlo es que el usuario instale los certificados raíz de su sitio Web en el repositorio de proveedores de confianza de Java, para lo cual debe abrir el Panel de Control de Java y seleccionar “Gestionar Certificados”:


Java Control Panel
General
Update
Java
Security
Advanced
Enable Java content in the browser
Security level for applications not on the Exception Site list
Very High - Only Java applications identified by a certificate from a trusted authority are allowed to run, and only if the certificate can be verified as not revoked.
High - Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocation status of the certificate cannot be verified.
Exception Site List
Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.
Click Edit Site List...
to add items to this list.
Edit Site List...
Restore Security Prompts
Manage Certificates...
OK
Cancel
Apply

Y a continuación importar directamente los certificados raíz como “Autoridad de Certificación de Sitio Seguro”, preferentemente en el almacén de sistema:



En caso de duda, consulte con el emisor de los certificados de su sitio Web SSL para obtener los certificados raíz y ampliar estas instrucciones de instalación.

3.3 Firmas Generales

Alguno de los formatos de firma generados con el Cliente @firma no validan adecuadamente en otras plataformas

Compruebe siempre las matrices de compatibilidad del cliente para verificar que los formatos no están sujetos a problemas de adecuación con normativas/estándares (cuando esto ocurra estará así indicado) y cuáles de los que no presentan estos problemas están soportados por su plataforma validadora.

Algunos dispositivos de creación de firma no funcionan con las funcionalidades de firma multi-fase del Cliente

Estas limitaciones son impuestas por los fabricantes de los dispositivos de creación de firmas y no es posible sortearlas. Consulte con el fabricante de su dispositivo de creación de firmas para comprobar que funcionalidades pueden estar restringidas.

La configuración de filtros de certificados produce un error cuando se establece un filtro de gran tamaño.

Este error ocurre al usar un filtro de certificados mediante el método deprecado "`setCertFilter(String)`" o "`setMandatoryCertificateCondition(String)`". Al concatenar/anidar múltiples expresiones de este tipo se produce un error en la JVM que obliga a desactivar el filtro. Debe evitarse el uso de filtros con múltiples expresiones.

Es recomendable migrar las aplicaciones al nuevo sistema de filtros basado en la RFC 2254. Pueden establecerse filtros de este tipo mediante el método "`setCertFilterRFC2254(String, String, boolean)`".

Mensajes de confirmación durante el proceso de firma masiva

A partir del Cliente @firma v3.3, cualquier acceso a disco como leer y guardar datos requiere del consentimiento expreso del usuario. Este procedimiento no afecta a la mecánica de las aplicaciones que integran el Cliente, por lo que no requerirán ningún tipo de modificación, salvo en casos concretos de firma masiva de datos.

El proceso de firma masiva programática dispone de un método para la firma de ficheros, asegúrese de utilizar este método (`massiveSignatureFile()`) y no el de firma de datos (`massiveSignatureData()`) si va a firmar ficheros en disco.

Por otra parte, el proceso de firma masiva programática no dispone de un método propio para el guardado de las firmas en disco. En anteriores versiones del Cliente era posible utilizar los métodos comunes de guardado para almacenar las firmas pero a partir de la versión 3.3 esto supone que se pida confirmación para el guardado de cada firma individual. Por motivos de seguridad, este comportamiento no puede evitarse.

Si se desea firmar ficheros y almacenar el resultado en disco, consulte la información del proceso de firma de directorios del manual del integrador del Cliente. Este mecanismo permitiría firmar y almacenar todos los ficheros sin necesidad de que el usuario lo apruebe individualmente.

3.4 Incidencias específicas de la plataforma Windows

Error "el conjunto de claves no existe" al firmar con el almacén de claves de Windows

En ciertas ocasiones, y especialmente cuando se usan tarjetas de FNMT-RCM (CERES, DNIe, APE, etc.), al firmar en un entorno operativo Windows, la operación finaliza con error y se muestra en consola el mensaje "`El conjunto de claves no existe`" (o "`Keyset does not exist`" si se tiene un Windows en inglés).

Este problema, que si bien puede darse en cualquier versión de Windows es más común en Windows XP, no tiene solución, y se debe a una incompatibilidad de Java con los controladores CAPI de Windows instalados en el sistema del usuario (por ejemplo, los controladores de FNMT-RCM).

Pruebe a actualizar tanto en entorno de ejecución de Java como los posibles controladores de tarjetas que tenga instalados a la última versión disponible.

Si el problema se da únicamente al intentar firmar con una tarjeta inteligente o un almacén de claves distinto del central de Windows, abra una incidencia contra el proveedor de este hardware/software de almacén de claves.

En versiones antiguas de Internet Explorer no es posible tener simultáneamente abiertas dos o más páginas que contengan diferentes instancias del Cliente @firma

Es posible que en versiones 7 y anteriores de Internet Explorer abrir una segunda página que contenga el Cliente @firma teniendo otra ya abierta ocasione fallos de carga en la segunda o un malfuncionamiento general en ambas.

Actualice a la última versión de Internet Explorer disponible para su sistema operativo Windows y a al menos la versión 6u30 del entorno de ejecución de Java (JRE) para sortear estos problemas. Si por cualquier motivo no puede actualizar Internet Explorer pruebe a usar otro navegador Web, como Google Chrome.

El Cliente no Funciona Correctamente en Windows sobre arquitectura IA64 (Intel Itanium)

La arquitectura IA64 en Windows no está soportada por el Cliente y no lo estará en un futuro próximo.

El Cliente no permite acceder a los almacenes de certificados con Java 6 (64 bits)

El entorno de ejecución de Java 6 de 64 bits no incorpora las bibliotecas necesarias para el acceso a los almacenes de Windows y Mozilla. Estas bibliotecas tratan de instalarse durante el proceso de carga del Cliente pero, en sistemas con permisos restringidos, no será posible.

Si su navegador web es de 64 bits y no puede acceder al almacén de su sistema, actualice a Java 7 (64 bits).

El Cliente deja de funcionar por completo cuando estoy utilizándolo a la vez que una aplicación nativa Windows que hace uso de una tarjeta inteligente

Algunas aplicaciones nativas de Windows que hacen uso de tarjetas inteligentes como el DNIe (aplicación de escritorio, controles ActiveX en páginas Web de Internet Explorer…) interfieren en el funcionamiento de las bibliotecas SunMSCAPI de Java para el uso de los certificados del sistema operativo. Esta interferencia provoca que cualquier intento de una aplicación Java de acceder al almacén de certificados de Windows cuando se tiene insertada la tarjeta inteligente en el lector mientras la otra aplicación esté también ejecutándose, genere un error interno en la máquina virtual de Java que cierra instantáneamente la aplicación afectada.

Este es un problema generado por aplicaciones nativas Windows que acceden a CAPI por medios no recomendados y por defectos de la biblioteca SunMSCAPI, encargada del acceso al almacén de certificados de Windows, que no puede ser tratado, que impiden operar cuando se realizan estos accesos no recomendados.

En general, debe intentar evitarse la situación en donde una aplicación utilice una tarjeta inteligente a la vez que se usa el cliente de firma. Para hacerlo, conviene separar el uso de las dos aplicaciones que acceden a la tarjeta mediante la extracción y reinserción de la misma en el lector o simplemente cerrando el resto de las aplicaciones mientras se usa una de ellas.

Si llegase a producirse este error, es posible que necesite cerrar la aplicación Windows que produce la incompatibilidad y reiniciar la aplicación (página Web) que integra el cliente @firma.

No es posible acceder al almacén de Firefox en sistemas Windows con Java 6u32 o superior y Java 7u4 o superior

La JRE de Oracle para Windows utiliza a partir de las versiones u32 de Java 6 y u4 de Java 7 el entorno de ejecución de Visual C++ 2010. El Cliente @firma no podrá acceder al almacén de Firefox si no cuenta con este entorno de ejecución instalado en su sistema. Puede descargarlo desde:

http://www.microsoft.com/download/en/details.aspx?id=5555

No es posible cargar el Cliente @firma o acceder al almacén de certificados con Apple Safari y Java 6

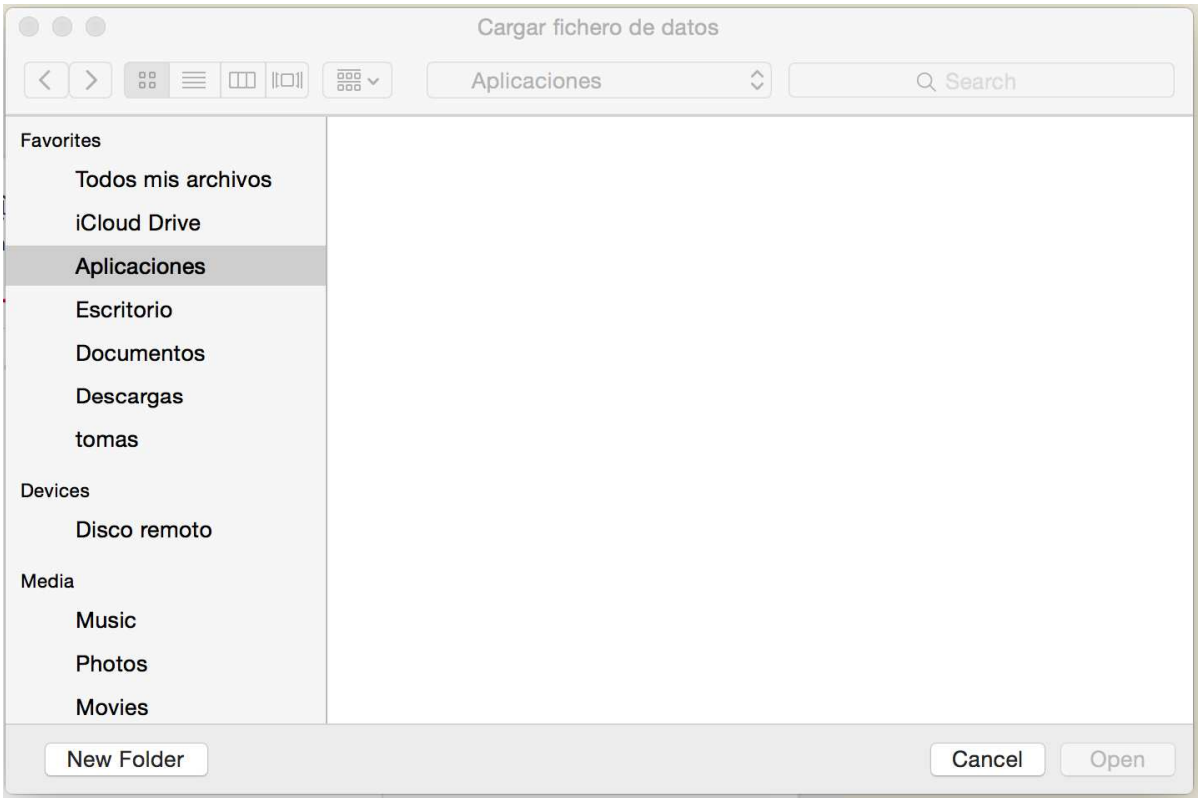
Java 6 no está certificado para su uso con Apple Safari sobre Windows en ninguna plataforma. En sistemas Windows Vista y Windows 7 actualice a la última versión de Java 7. Por otra parte, las últimas versiones de Java no son compatibles con Safari sobre Windows XP, por lo que será necesario utilizar otro navegador web.

3.5 Incidencias específicas de la plataforma Apple OS X

Al intentar abrir un fichero en Safari el diálogo de selección se abre, pero no muestra ningún fichero para seleccionar

Los Applets de Java en OS X con Safari tienen restringido por defecto el acceso al sistema de ficheros, lo cual puede causar cierta confusión con los Applets Cliente @firma en OS X, porque da la impresión de funcionar apropiadamente, pero cuando se solicita abrir o guardar un fichero, no es posible.

En particular, lo que el usuario aprecia al intentar abrir un fichero es que el diálogo de selección se abre, pero no muestra ningún archivo:



Para conseguir que el MiniApplet tenga acceso no restringido al sistema de ficheros del usuario es necesario que este configure Safari para habilitar el “Modo Inseguro” para el sitio Web en concreto que publique el MiniApplet.

Para ello, siga las indicaciones de Apple, que puede encontrar aquí:

http://support.apple.com/kb/HT5954

Al cargar el Cliente @firma aparece el componente instalador solicitando la introducción de la contraseña de usuario privilegiado, pero o no deseo introducirla por motivos de seguridad o aunque la introduzca el proceso termina en error.

Para el uso del repositorio de Mozilla Firefox en Mac OS X es necesario que las bibliotecas NSS estén situadas dentro de una ruta de carga de bibliotecas, pero Firefox al instalarse en Mac OS X las instala en su propio directorio, sin añadir este a la lista de rutas de carga de bibliotecas.

Para sortear esta dificultad, el Cliente @firma, mediante su componente instalador (BootLoader), intenta crear enlaces simbólicos de estas bibliotecas desde el directorio de Firefox a `/usr/lib`, carpeta dentro de la lista de directorios de carga de bibliotecas. Para realizar esta copia, se necesitan ciertos privilegios, y es por esta razón por la que se solicita la contraseña de usuario privilegiado.

Si prefiere no introducir su contraseña de usuario privilegiado o simplemente el proceso automático del BootLoader no funciona en su entorno específico, siempre puede realizar la copia de ficheros de forma manual desde una ventana de terminal.

Los ficheros a enlazar simbólicamente son (si alguno de estos ficheros no existe en su instalación de Firefox en Mac OS X):

- `libnspr4.dylib`
- `libplds4.dylib`
- `libplc4.dylib`
- `libmozsqlite3.dylib`
- `libnssutil3.dylib`
- `libmozutils.dylib`

Es necesario enlazarlos desde su directorio de origen (el de instalación de Mozilla Firefox, normalmente `/Applications/Firefox.app/Contents/MacOS`) a `/usr/lib`.

Si tiene instalado Mozilla Firefox y no encuentra las bibliotecas indicadas en `/Applications/Firefox.app/Contents/MacOS` puede intentar localizaras mediante el siguiente comando:

```
#find / -name “libnspr4.dylib”
```

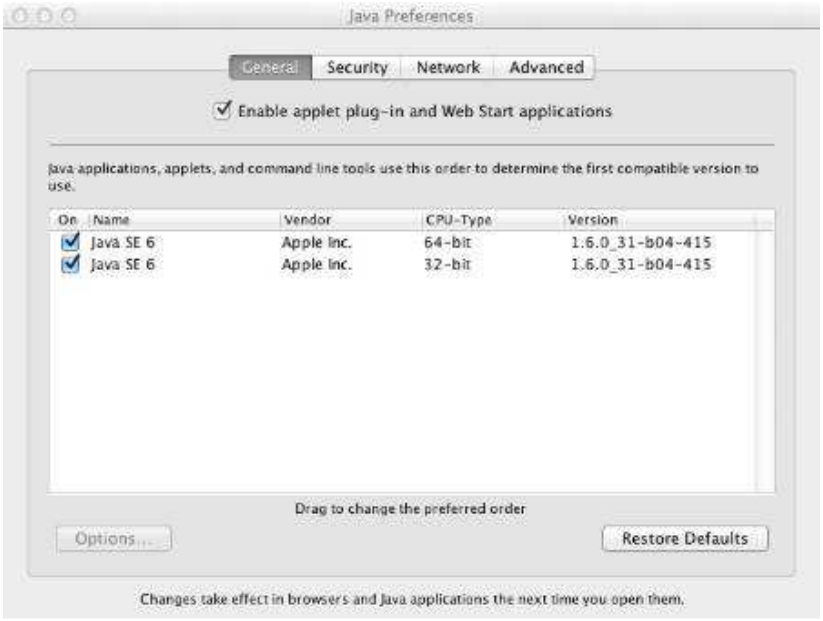
Para enlazar simbólicamente las bibliotecas es recomendable usar el comando `ln`. Consulte la documentación de Mac OS X o use el comando `man` para más información sobre el comando `ln`. De igual forma, es probable que necesite hacer uso del comando `sudo` (o `su`) para obtener privilegios elevados desde un terminal de comandos en Mac OS X.

Error en la ejecución del Cliente @firma en Mac OS X 10.7.4 o superior

Se ha detectado que los cambios de seguridad incorporados por Apple a la actualización 10.7.4 de Mac OS X Lion pueden causar problemas aleatorios en la obtención de privilegios de los Applets Java firmados. Si experimenta problemas ejecutando el Applet Cliente @firma en Mac OS X 10.7.4 puede actualizar su entorno de ejecución de Java a la versión 7 usando la versión de Oracle, disponible para libre descarga desde:

http://www.oracle.com/technetwork/java/javase/downloads/index.html

Adicionalmente, aunque Java esté correctamente instalado, puede ser necesaria la activación del soporte específico de Applets de Java y aplicaciones Java WebStart. Esta activación puede realizarse desde “Preferencias de Java”, en el menú “Utilidades” de Mac OS X:



3.6 Incidencias específicas de las firmas PDF

El Cliente no permite la firma de PDF con ciertos certificados

Las firmas de documentos PDF realizadas externamente (que es el método utilizado por el Cliente) tienen un tamaño máximo de octetos que pueden ocupar dentro del PDF.

Como la firma incluye la cadena de certificación completa, si esta es muy extensa puede llegar a agotarse este espacio y resultar en una firma inválida o corrupta. Si esto le ocurre, por favor, póngase en contacto con el servicio de atención a los usuarios del Cliente @firma enviando una copia de su certificado de firma y la cadena de confianza completa. **Tenga siempre mucho cuidado de no enviar jamás las partes privadas de los certificados**.

3.7 Incidencias específicas de las firmas XML

El Cliente no firma las hojas de estilo de los ficheros XML

Dado que las hojas de estilo de un XML pueden declararse de distintas formas, el cliente adopta distintas estrategias para cada forma de declaración y según la variante de firma.

Las formas de declarar una hoja de estilo y la forma de firmar el XML en ese caso por el Cliente son las siguientes:

- La hoja de estilo está empotrada dentro del XML, y se declara con una referencia local (el valor del atributo `href` de la declaración del XSL es un nombre de identificador de nodo XML precedido por "#").
  - En este caso no es necesaria ninguna estrategia adicional, pues al ser parte la hoja de estilo del XML, siempre que se firma uno, se firma también el otro. Esto aplica a la totalidad de las firmas XML.
- La hoja de estilo está accesible remotamente por protocolo HTTP o HTTPS (el valor del atributo `href` es una URL válida con esquema `http` ó `https`).
  - En este caso se añade una referencia a la firma que apunta a la hoja de estilo mediante la misma URL (una referencia Externally Detached). Esto aplica a la totalidad de las firmas XML).
- Se referencia a la hoja de estilo mediante una referencia relativa local.
  - En este caso, dado que las referencias relativas locales se pierden al firmar (el Applet no sabe en qué directorio o carpeta estaba el XML para localizar el XSL, y no puede asumir dónde se guardará la firma generada), las hojas de estilo no se firman.

Compruebe que el XML que desea firmar declara las hojas de estilo mediante alguno de los modos soportado.

Las firmas XMLDSig generadas no son compatibles con SOAP

Esta funcionalidad está en estudio para ser incluida en futuras versiones del Cliente.

Ciertos validadores no aceptan algunas de las firmas generadas por el Cliente @firma

El Cliente @firma permite generar un amplio abanico de formatos de firmas, algunos de los cuales no están soportados por todos los validadores de firma actuales. Por ejemplo, firmas ODF, PDF, firmas XML explícitas (en donde se firma el hash de un fichero)….

También existe la posibilidad de que un validador sólo admita versiones específicas de estos formatos.

El sistema de validación de firmas VALIDe soporta todas las firmas generadas con el Cliente @firma, a excepción de las firmas OOXML que se incorporarán en una próxima versión.

El Cliente no genera firmas XML usando huellas digitales SHA-2

El error de Java 6845600 (http://bugs.sun.com/view_bug.do?bug_id=6845600) afecta a la generación de firmas XML con SHA-256 y SHA-512, y los errores de Java 6753664 y 6946836 (http://bugs.sun.com/view_bug.do?bug_id=6753664 y http://bugs.sun.com/view_bug.do?bug_id=6946836) impiden usar estos algoritmos de huella digital sobre Internet Explorer.

Para sortear estos problemas debe usar Java 6u30 o Java 7u2 y superiores.

El Cliente produce un error de derreferenciación al generar firmas XAdES: javax.xml.crypto.URIReferenceException:

Errores en las primeras versiones de Java 7 producen problemas internos de derreferenciación al generar firmas XAdES cuando se configura la propiedad “contentTypeOid”. Esta propiedad, que es la encargada de indicar el tipo de dato firmado a través de un OID se representa internamente como una URI de tipo URN que Java es incapaz de derreferenciar.

El problema surge también durante las operaciones de firma masiva XAdES ya que internamente utilizan esta propiedad.

Este error aparece por regla general en sistemas con sistema operativo Windows 7 aunque no se descarta que surja en otros entornos como Windows XP u otros sistemas operativos.

Estos errores de Java quedan solucionados en versiones posteriores de Java 7. Actualice a la última versión para solventar el problema.

Los errores comentados están reconocidos y publicados por Oracle con los identificadores 7094155 y 2219607 (http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7094155 y http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=2219607).

4 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.

Creative Commons

Reconocimiento-NoComercial-CompartirIgual 3.0 Unported

Usted es libre de:

Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra

hacer obras derivadas

Bajo las condiciones siguientes:

Atribución — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).

NoComercial — No puede utilizar esta obra para fines comerciales.

Compartir bajo la Misma Licencia — Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

Entendiendo que:

Renuncia — Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Dominio Público — Cuando la obra o alguno de sus elementos se hallen en el dominio público según la ley vigente aplicable, esta situación no quedará afectada por la licencia.

Otros derechos — Los derechos siguientes no quedan afectados por la licencia de ninguna manera:

- Los derechos derivados de usos legítimos u otras limitaciones reconocidas por ley no se ven afectados por lo anterior.
- Los derechos morales del auto;
- Derechos que pueden ostentar otras personas sobre la propia obra o su uso, como por ejemplo derechos de imagen o de privacidad.

Aviso — Al reutilizar o distribuir la obra, tiene que dejar muy en claro los términos de la licencia de esta obra. La mejor forma de hacerlo es enlazar a esta página.

Licencia

LA OBRA O LA PRESTACIÓN (SEGÚN SE DEFINEN MÁS ADELANTE) SE PROPORCIONA BAJO LOS TÉRMINOS DE ESTA LICENCIA PÚBLICA DE CREATIVE COMMONS (CCPL O LICENCIA). LA OBRA O LA PRESTACIÓN SE ENCUENTRA PROTEGIDA POR LA LEY ESPAÑOLA DE PROPIEDAD INTELECTUAL Y/O CUALESQUIERA OTRAS NORMAS QUE RESULTEN DE APLICACIÓN. QUEDA PROHIBIDO CUALQUIER USO DE LA OBRA O PRESTACIÓN DIFERENTE A LO AUTORIZADO BAJO ESTA LICENCIA O LO DISPUESTO EN LA LEY DE PROPIEDAD INTELECTUAL.

MEDIANTE EL EJERCICIO DE CUALQUIER DERECHO SOBRE LA OBRA O LA PRESTACIÓN, USTED ACEPTA Y CONSIENTE LAS LIMITACIONES Y OBLIGACIONES DE ESTA LICENCIA, SIN PERJUICIO DE LA NECESIDAD DE CONSENTIMIENTO EXPRESO EN CASO DE VIOLACIÓN PREVIA DE LOS TÉRMINOS DE LA MISMA. EL LICENCIADOR LE CONCEDE LOS DERECHOS CONTENIDOS EN ESTA LICENCIA, SIEMPRE QUE USTED ACEPTE LOS PRESENTES TÉRMINOS Y CONDICIONES.

1. Definiciones

a. La **obra** es la creación literaria, artística o científica ofrecida bajo los términos de esta licencia.

b. En esta licencia se considera una **prestación** cualquier interpretación, ejecución, fonograma, grabación audiovisual, emisión o transmisión, mera fotografía u otros objetos protegidos por la legislación de propiedad intelectual vigente aplicable.

c. La aplicación de esta licencia a una **colección** (definida más adelante) afectará únicamente a su estructura en cuanto forma de expresión de la selección o disposición de sus contenidos, no siendo extensiva a éstos. En este caso la colección tendrá la consideración de obra a efectos de esta licencia.

d. El **titular originario** es:

   a. En el caso de una obra literaria, artística o científica, la persona natural o grupo de personas que creó la obra.

   b. En el caso de una obra colectiva, la persona que la edite y divulgue bajo su nombre, salvo pacto contrario.

   c. En el caso de una interpretación o ejecución, el actor, cantante, músico, o cualquier otra persona que represente, cante, lea, recite, interprete o ejecute en cualquier forma una obra.

   d. En el caso de un fonograma, el productor fonográfico, es decir, la persona natural o jurídica bajo cuya iniciativa y responsabilidad se realiza por primera vez una fijación exclusivamente sonora de la ejecución de una obra o de otros sonidos.

   e. En el caso de una grabación audiovisual, el productor de la grabación, es decir, la persona natural o jurídica que tenga la iniciativa y asuma la responsabilidad de las fijaciones de un plano o secuencia de imágenes, con o sin sonido.

   f. En el caso de una emisión o una transmisión, la entidad de radiodifusión.

   g. En el caso de una mera fotografía, aquella persona que la haya realizado.

h. En el caso de otros objetos protegidos por la legislación de propiedad intelectual vigente, la persona que ésta señale.

e. Se considerarán **obras derivadas** aquellas obras creadas a partir de la licenciada, como por ejemplo: las traducciones y adaptaciones; las revisiones, actualizaciones y anotaciones; los compendios, resúmenes y extractos; los arreglos musicales y, en general, cualesquiera transformaciones de una obra literaria, artística o científica. Para evitar la duda, si la obra consiste en una composición musical o grabación de sonidos, la sincronización temporal de la obra con una imagen en movimiento (synching) será considerada como una obra derivada a efectos de esta licencia.

f. Tendrán la consideración de **colecciones** la recopilación de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales. La mera incorporación de una obra en una colección no dará lugar a una derivada a efectos de esta licencia.

g. El **licenciador** es la persona o la entidad que ofrece la obra o prestación bajo los términos de esta licencia y le concede los derechos de explotación de la misma conforme a lo dispuesto en ella.

h. **Usted** es la persona o la entidad que ejercita los derechos concedidos mediante esta licencia y que no ha violado previamente los términos de la misma con respecto a la obra o la prestación, o que ha recibido el permiso expreso del licenciador de ejercitar los derechos concedidos mediante esta licencia a pesar de una violación anterior.

i. La **transformación** de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente. La creación resultante de la transformación de una obra tendrá la consideración de obra derivada.

j. Se entiende por **reproducción** la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o la prestación o de parte de ella, que permita su comunicación o la obtención de copias.

k. Se entiende por **distribución** la puesta a disposición del público del original o de las copias de la obra o la prestación, en un soporte tangible, mediante su venta, alquiler, préstamo o de cualquier otra forma.

l. Se entiende por **comunicación pública** todo acto por el cual una pluralidad de personas, que no pertenezcan al ámbito doméstico de quien la lleva a cabo, pueda tener acceso a la obra o la prestación sin previa distribución de ejemplares a cada una de ellas. Se considera comunicación pública la puesta a disposición del público de obras o prestaciones por procedimientos alámbricos o inalámbricos, de tal forma que cualquier persona pueda acceder a ellas desde el lugar y en el momento que elija.

m. La **explotación** de la obra o la prestación comprende la reproducción, la distribución, la comunicación pública y, en su caso, la transformación.

2. Límites de los derechos. Nada en esta licencia pretende reducir o restringir cualesquiera límites legales de los derechos exclusivos del titular de los derechos de propiedad intelectual de acuerdo con la Ley de propiedad intelectual o cualesquiera otras leyes aplicables, ya sean derivados de usos legítimos, tales como la copia privada o la cita, u otras limitaciones como la resultante de la primera venta de ejemplares (agotamiento).

3. Concesión de licencia. Conforme a los términos y a las condiciones de esta licencia, el licenciador concede, por el plazo de protección de los derechos de propiedad intelectual y a título gratuito, una licencia de ámbito mundial no exclusiva que incluye los derechos siguientes:

a. Derecho de reproducción, distribución y comunicación pública de la obra o la prestación.

b. Derecho a incorporar la obra o la prestación en una o más colecciones.

c. Derecho de reproducción, distribución y comunicación pública de la obra o la prestación lícitamente incorporada en una colección.

d. Derecho de transformación de la obra para crear una obra derivada siempre y cuando se incluya en ésta una indicación de la transformación o modificación efectuada.

e. Derecho de reproducción, distribución y comunicación pública de obras derivadas creadas a partir de la obra licenciada.

f. Derecho a extraer y reutilizar la obra o la prestación de una base de datos.

g. Para evitar cualquier duda, el titular originario:

   i. Conserva el derecho a percibir las remuneraciones o compensaciones previstas por actos de explotación de la obra o prestación, calificadas por la ley como irrenunciables e inalienables y sujetas a gestión colectiva obligatoria.

   ii. Renuncia al derecho exclusivo a percibir, tanto individualmente como mediante una entidad de gestión colectiva de derechos, cualquier remuneración derivada de actos de explotación de la obra o prestación que usted realice.

Estos derechos se pueden ejercitar en todos los medios y formatos, tangibles o intangibles, conocidos en el momento de la concesión de esta licencia. Los derechos mencionados incluyen el derecho a efectuar las modificaciones que sean precisas técnicamente para el ejercicio de los derechos en otros medios y formatos. Todos los derechos no concedidos expresamente por el licenciador quedan reservados, incluyendo, a título enunciativo pero no limitativo, los derechos morales irrenunciables reconocidos por la ley aplicable. En la medida en que el licenciador ostente derechos exclusivos previstos por la ley nacional vigente que implementa la directiva europea en materia de derecho sui generis sobre bases de datos, renuncia expresamente a dichos derechos exclusivos.

4. Restricciones. La concesión de derechos que supone esta licencia se encuentra sujeta y limitada a las restricciones siguientes:

a. Usted puede reproducir, distribuir o comunicar públicamente la obra o prestación solamente bajo los términos de esta licencia y debe incluir una copia de la misma, o su Identificador Uniforme de Recurso (URI). Usted no puede ofrecer o imponer ninguna condición sobre la obra o prestación que altere o restrinja los términos de esta licencia o el ejercicio de sus derechos por parte de los concesionarios de la misma. Usted no puede sublicenciar la obra o prestación. Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías. Usted no puede reproducir, distribuir o comunicar públicamente la obra o prestación con medidas tecnológicas que controlen el acceso o el uso de una manera contraria a los términos de esta licencia. Esta sección 4.a también afecta a la obra o prestación incorporada en una colección, pero ello no implica que ésta en su conjunto quede automáticamente o deba quedar sujeta a los términos de la misma. En el caso que le sea requerido, previa comunicación del licenciador, si usted incorpora la obra en una colección

y/o crea una obra derivada, deberá quitar cualquier crédito requerido en el apartado 4.b, en la medida de lo posible.

b. Si usted reproduce, distribuye o comunica públicamente la obra o la prestación, una colección que la incorpore o cualquier obra derivada, debe mantener intactos todos los avisos sobre la propiedad intelectual e indicar, de manera razonable conforme al medio o a los medios que usted esté utilizando:

   i. El nombre del autor original, o el seudónimo si es el caso, así como el del titular originario, si le es facilitado.

   ii. El nombre de aquellas partes (por ejemplo: institución, publicación, revista) que el titular originario y/o el licenciador designen para ser reconocidos en el aviso legal, las condiciones de uso, o de cualquier otra manera razonable.

   iii. El título de la obra o la prestación si le es facilitado.

   iv. El URI, si existe, que el licenciador especifique para ser vinculado a la obra o la prestación, a menos que tal URI no se refiera al aviso legal o a la información sobre la licencia de la obra o la prestación.

   v. En el caso de una obra derivada, un aviso que identifique la transformación de la obra en la obra derivada (p. ej., "traducción castellana de la obra de Autor Original," o "guión basado en obra original de Autor Original").

   Este reconocimiento debe hacerse de manera razonable. En el caso de una obra derivada o incorporación en una colección estos créditos deberán aparecer como mínimo en el mismo lugar donde se hallen los correspondientes a otros autores o titulares y de forma comparable a los mismos. Para evitar la duda, los créditos requeridos en esta sección sólo serán utilizados a efectos de atribución de la obra o la prestación en la manera especificada anteriormente. Sin un permiso previo por escrito, usted no puede afirmar ni dar a entender implícitamente ni explícitamente ninguna conexión, patrocinio o aprobación por parte del titular originario, el licenciador y/o las partes reconocidas hacia usted o hacia el uso que hace de la obra o la prestación.

c. Para evitar cualquier duda, debe hacerse notar que las restricciones anteriores (párrafos 4.a y 4.b) no son de aplicación a aquellas partes de la obra o la prestación objeto de esta licencia que únicamente puedan ser protegidas mediante el derecho sui generis sobre bases de datos recogido por la ley nacional vigente implementando la directiva europea de bases de datos

5. Exoneración de responsabilidad

A MENOS QUE SE ACUERDE MUTUAMENTE ENTRE LAS PARTES, EL LICENCIADOR OFRECE LA OBRA O LA PRESTACIÓN TAL CUAL (ON AN "AS-IS" BASIS) Y NO CONFIERE NINGUNA GARANTÍA DE CUALQUIER TIPO RESPECTO DE LA OBRA O LA PRESTACIÓN O DE LA PRESENCIA O AUSENCIA DE ERRORES QUE PUEDAN O NO SER DESCUBIERTOS. ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE TALES GARANTÍAS, POR LO QUE TAL EXCLUSIÓN PUEDE NO SER DE APLICACIÓN A USTED.

6. Limitación de responsabilidad. SALVO QUE LO DISPONGA EXPRESA E IMPERATIVAMENTE LA LEY APLICABLE, EN NINGÚN CASO EL LICENCIADOR SERÁ RESPONSABLE ANTE USTED POR CUALESQUIERA DAÑOS RESULTANTES, GENERALES O ESPECIALES (INCLUIDO EL DAÑO EMERGENTE Y EL LUCRO CESANTE), FORTUITOS O

CAUSALES, DIRECTOS O INDIRECTOS, PRODUCIDOS EN CONEXIÓN CON ESTA LICENCIA O EL USO DE LA OBRA O LA PRESTACIÓN, INCLUSO SI EL LICENCIADOR HUBIERA SIDO INFORMADO DE LA POSIBILIDAD DE TALES DAÑOS.

7. Finalización de la licencia

a. Esta licencia y la concesión de los derechos que contiene terminarán automáticamente en caso de cualquier incumplimiento de los términos de la misma. Las personas o entidades que hayan recibido de usted obras derivadas o colecciones bajo esta licencia, sin embargo, no verán sus licencias finalizadas, siempre que tales personas o entidades se mantengan en el cumplimiento íntegro de esta licencia. Las secciones 1, 2, 5, 6, 7 y 8 permanecerán vigentes pese a cualquier finalización de esta licencia.

b. Conforme a las condiciones y términos anteriores, la concesión de derechos de esta licencia es vigente por todo el plazo de protección de los derechos de propiedad intelectual según la ley aplicable. A pesar de lo anterior, el licenciador se reserva el derecho a divulgar o publicar la obra o la prestación en condiciones distintas a las presentes, o de retirar la obra o la prestación en cualquier momento. No obstante, ello no supondrá dar por concluida esta licencia (o cualquier otra licencia que haya sido concedida, o sea necesario ser concedida, bajo los términos de esta licencia), que continuará vigente y con efectos completos a no ser que haya finalizado conforme a lo establecido anteriormente, sin perjuicio del derecho moral de arrepentimiento en los términos reconocidos por la ley de propiedad intelectual aplicable.

8. Miscelánea

a. Cada vez que usted realice cualquier tipo de explotación de la obra o la prestación, o de una colección que la incorpore, el licenciador ofrece a los terceros y sucesivos licenciatarios la concesión de derechos sobre la obra o la prestación en las mismas condiciones y términos que la licencia concedida a usted.

b. Cada vez que usted realice cualquier tipo de explotación de una obra derivada, el licenciador ofrece a los terceros y sucesivos licenciatarios la concesión de derechos sobre la obra objeto de esta licencia en las mismas condiciones y términos que la licencia concedida a usted.

c. Si alguna disposición de esta licencia resulta inválida o inaplicable según la Ley vigente, ello no afectará la validez o aplicabilidad del resto de los términos de esta licencia y, sin ninguna acción adicional por cualquiera las partes de este acuerdo, tal disposición se entenderá reformada en lo estrictamente necesario para hacer que tal disposición sea válida y ejecutiva.

d. No se entenderá que existe renuncia respecto de algún término o disposición de esta licencia, ni que se consiente violación alguna de la misma, a menos que tal renuncia o consentimiento figure por escrito y lleve la firma de la parte que renuncie o consienta.

e. Esta licencia constituye el acuerdo pleno entre las partes con respecto a la obra o la prestación objeto de la licencia. No caben interpretaciones, acuerdos o condiciones con respecto a la obra o la prestación que no se encuentren expresamente especificados en la presente licencia. El licenciador no estará obligado por ninguna disposición complementaria que pueda aparecer en cualquier comunicación que le haga llegar usted. Esta licencia no se puede modificar sin el mutuo acuerdo por escrito entre el licenciador y usted.