Problemas conocidos

Error al firmar ficheros mayores de 4 megabytes

El *plugin* de Java limita en cierta medida los datos que el cliente es capaz de procesar, lo que suele reducir el tamaño máximo de datos que el MiniApplet puede firmar. Esto se ve acompañado de las posibles limitaciones que surjan de la cantidad de memoria disponible en el equipo del usuario.

En la versión 1.2 del MiniApplet se ha paliado este problema de tal forma que el límite de tamaño pasa a depender más de los recursos del equipo del usuario y la configuración de la operación de firma. De forma segura, se pueden realizar firmas de datos de un tamaño mínimo de 8 megabytes.

Por parte del integrador, es posible evitar parcialmente esta limitación abandonando, siempre que sea posible, el uso de los métodos de carga de fichero getFileNameContentBase64 y getMultiFileNameContentBase64, en favor de la carga de datos realizada al llamar a las operaciones criptográficas sin indicar los datos a firmar/multifirma. Por ejemplo, en lugar de llamar al método getFileNameContentBase64 para cargar un fichero y luego pasarle los datos obtenidos al método sign, llamaremos al método sign sin datos para que sea el mismo el que permita cargar el fichero de datos.

No aparecen los certificados de las tarjetas CERES en el diálogo de selección de certificados desde Mozilla Firefox en Windows

La versión 4.0.0 del controlador para tarjetas criptográficas CERES trata de unificar el uso del DNIe y la tarjeta CERES por medio del mismo controlador. Sin embargo, errores en el diseño del controlador imposibilitan su uso desde Java para DNIe, lo que rompe la compatibilidad con esta tarjeta. Para solventarlo, el MiniApplet ignora este controlador, lo que imposibilita la carga de los certificados de las tarjetas CERES desde Mozilla Firefox. El DNIe puede seguir usándose normalmente, gracias al uso del controlador Java para DNIe que se incluye dentro del MiniApplet.

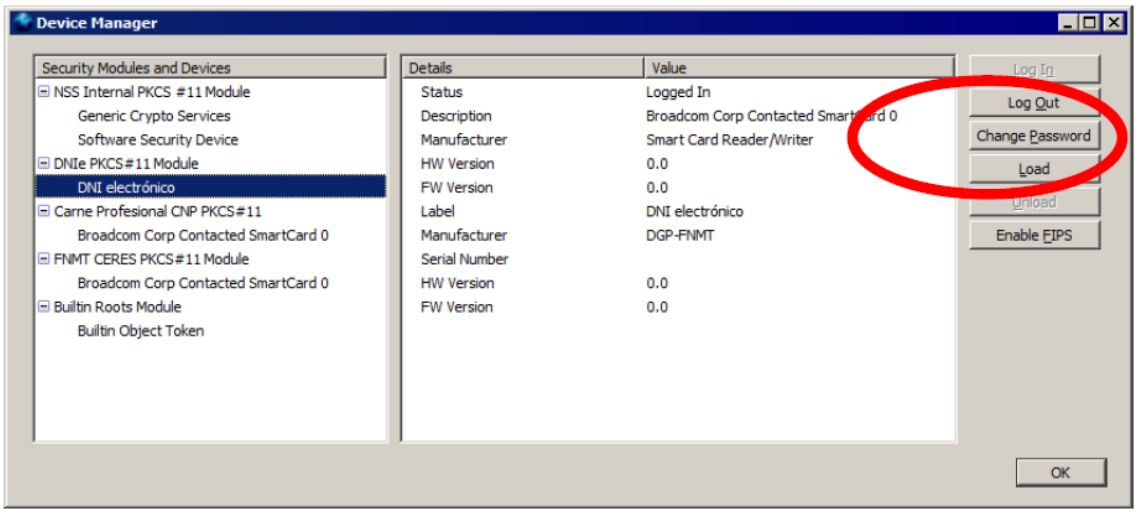
En el resto de navegadores funcionarán normalmente ambas tarjetas debido a que se utiliza el CSP de la tarjeta en lugar del PKCS#11 que se utiliza desde Mozilla Firefox.

Con el navegador Mozilla Firefox y DNIe (DNI Electrónico) el *applet* 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 oficial del DNIe (el usado desde Mozilla Firefox) 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. 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 surge principalmente en sistemas Linux/Solaris. Para estos sistemas se recomienda el uso del controlador OpenDNIe para DNI electrónico. Puede encontrar este controlador en:

https://forja.cenatic.es/projects/opendnie/

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

A veces puede ocurrir que el navegador no detecta la extracción o introducción del NIe (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.

El *applet* no detecta ningún certificado bajo Mozilla / Firefox

El Cliente @firma, cuando se ejecuta en Linux o Sun Solaris necesita que las bibliotecas NSS estén situadas en “/usr/lib”, “/lib” o al menos dentro de uno de los directorios incluidos en la variable de entorno LD_LIBRARY_PATH.

Si las bibliotecas NSS correspondientes a la versión de Mozilla Firefox instalada se encuentra en algún otro directorio, es posible hacérselo saber al Applet mediante el sistema indicado en el apartado Forzar ruta del almacén de Mozilla Firefox.

El MiniApplet no permite la firma de PDF con ciertos certificados

Las firmas de documentos PDF realizadas externamente (que es el método utilizado por el Cliente y el MiniApplet @firma) 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.