Software Criptográfico
FNMT-RCM

ÍNDICE

1. Descarga e instalación del Software

La Fábrica nacional de Moneda y Timbre, dentro de su departamento CERES, ha desarrollado un software criptográfico destinado a operar con tarjetas inteligentes y una utilidad para desbloquear la tarjeta, en caso de que se bloquee, y para cambiar su PIN.

Este software es válido para su utilización en **Windows XP (32 bits) y Windows Vista (32 y 64 bits).**

Se puede descargar desde el siguiente enlace:

http://www.cert.fnmt.es/content/pages_std/software/insmodcriptc2v1001.exe

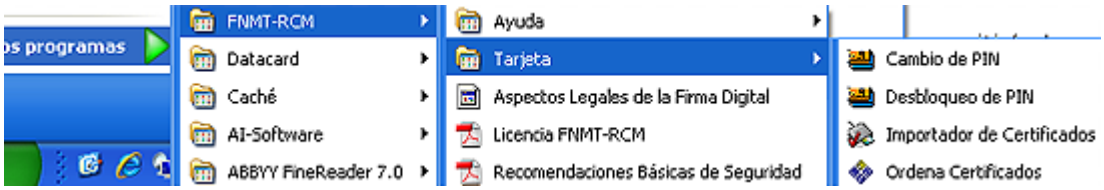
Una vez descargado para instalarlo simplemente debemos ejecutar la aplicación "insmodcripc2v810.exe". Esta aplicación lanzará un asistente que realizará automáticamente el proceso completo.

Una vez que ha sido preparado el asistente, comenzará automáticamente la instalación del software. El usuario no tiene que indicarle nada al asistente, ya que por defecto se utilizará para la instalación la ruta "C:\FNMT-RCM". En esa carpeta quedarán instalados todos los programas necesarios, mientras que las librerías se guardarán en el directorio Windows/System o Windows/System32, según el sistema operativo que tengamos instalado en el equipo.

Tras completarse la instalación del software, el asistente nos solicitará que reiniciemos la máquina para que los cambios tengan efecto.

Software Criptográfico FNMT-RCM

Una vez instalado todo el software criptográfico, en el menú Programas aparecerá una nueva entrada con los enlaces al nuevo software instalado.



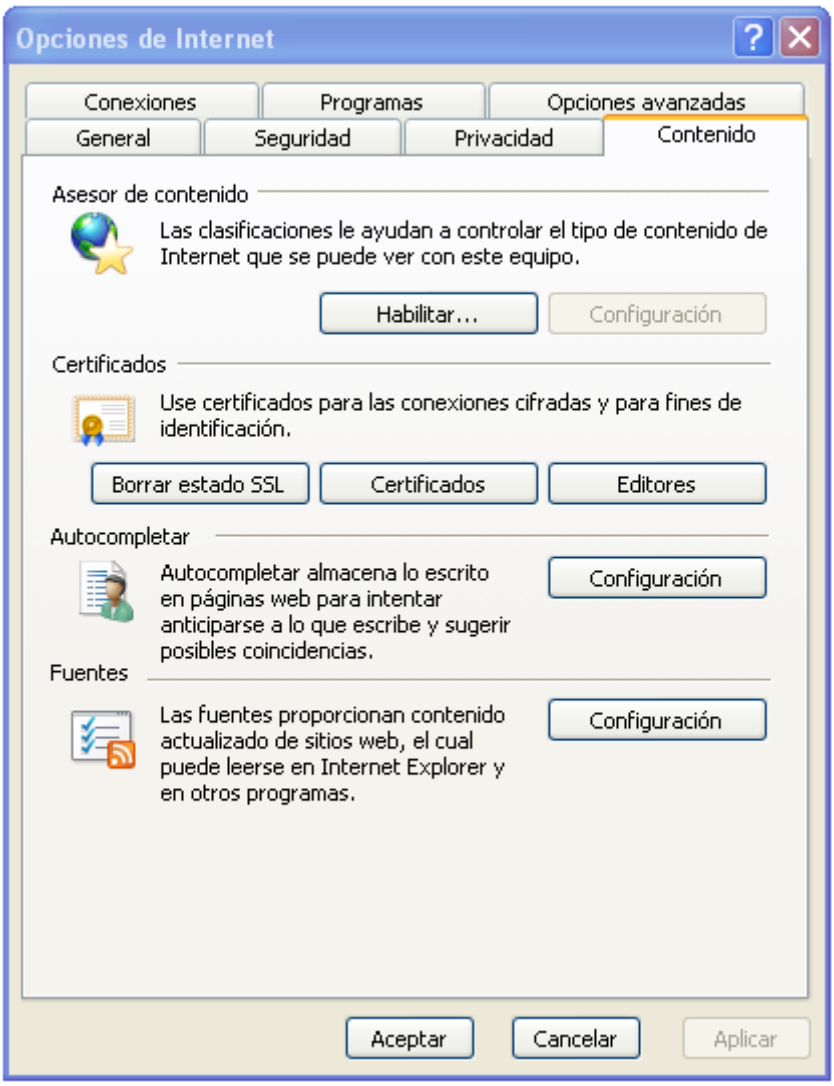
La tarjeta FNMT-RCM requiere para su uso un número de identificación personal (PIN), (que se incluye en el sobre de entrega de la misma junto al código de desbloqueo) que debe ser conocido sólo por su poseedor y permite acceder a las funciones de firma, descifrado, etc. Este mecanismo de seguridad permite evitar que alguien pueda utilizar nuestra tarjeta para realizar operaciones en nuestro nombre.

Puede ocurrir que cuando una aplicación nos solicite nuestro PIN, nos equivoquemos al introducirlo. En ese caso se nos dará un nuevo intento. Si fallásemos tres veces al insertar el PIN la tarjeta quedaría bloqueada, no permitiéndonos realizar ninguna operación. Para recuperar su funcionalidad será necesario desbloquear el PIN, utilizando para ello el código de desbloqueo de la tarjeta.

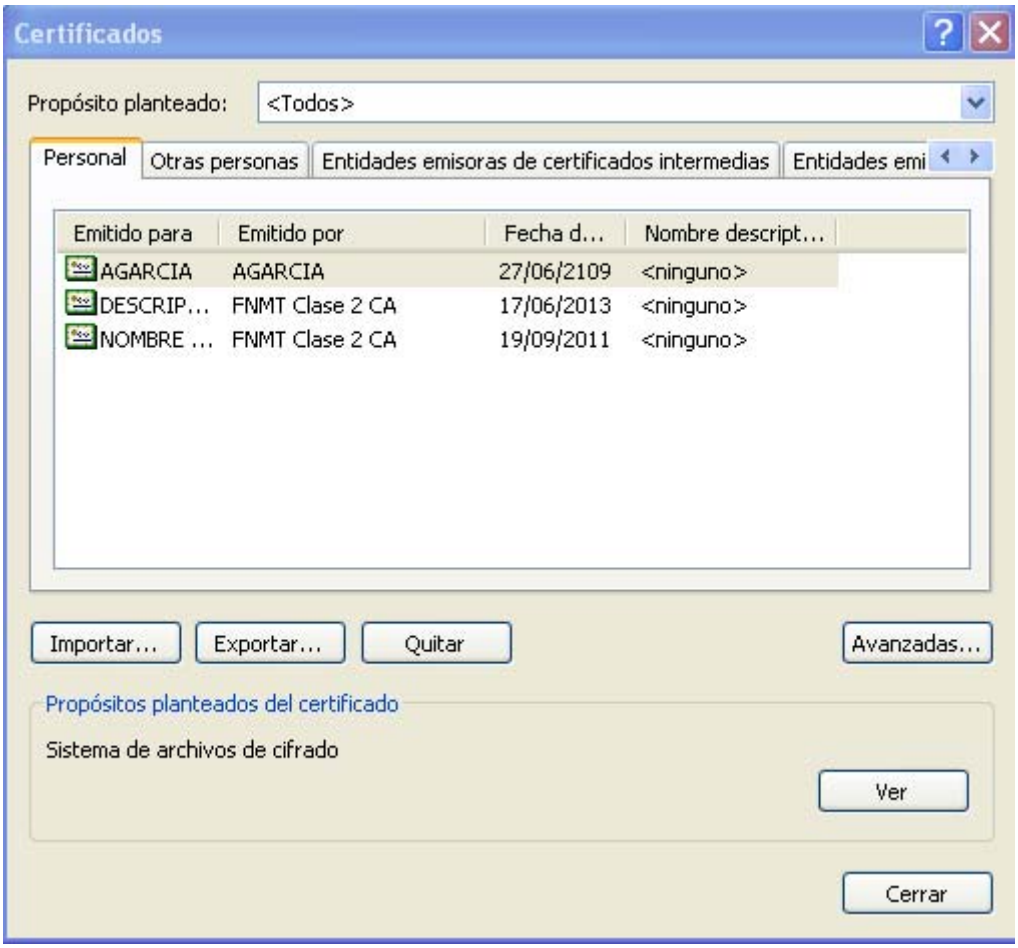
2. Exportación de certificados en Microsoft Internet Explorer.

Las tarjetas inteligentes proporcionan un mecanismo idóneo para la portabilidad de perfiles digitales y la seguridad en operaciones criptográficas. Pero puede ocurrir que inicialmente ya tuviésemos nuestro perfil en software (fichero electrónico) y queramos introducirlo en una tarjeta inteligente. Para poder hacerlo deberemos exportar el certificado desde el sistema inicial a un a un soporte hardware (tarjetas inteligentes, por ejemplo).

En Microsoft Internet Explorer todas las operaciones relacionadas con la gestión de certificados (perfiles) se encuentran en la solapa Contenido de la pantalla de Herramientas/Opciones de Internet. Desde aquí podremos ejecutar el apartado de Certificados, donde se realizan las operaciones de importar, exportar, eliminar certificados, ver sus características, fechas de validez, etc.



Dentro del apartado de certificados encontramos una pantalla en la que se nos muestran los certificados instalados en el sistema, y una serie de botones que nos permiten realizar las operaciones comunes: importar, exportar, eliminar, ver detalles, etc.



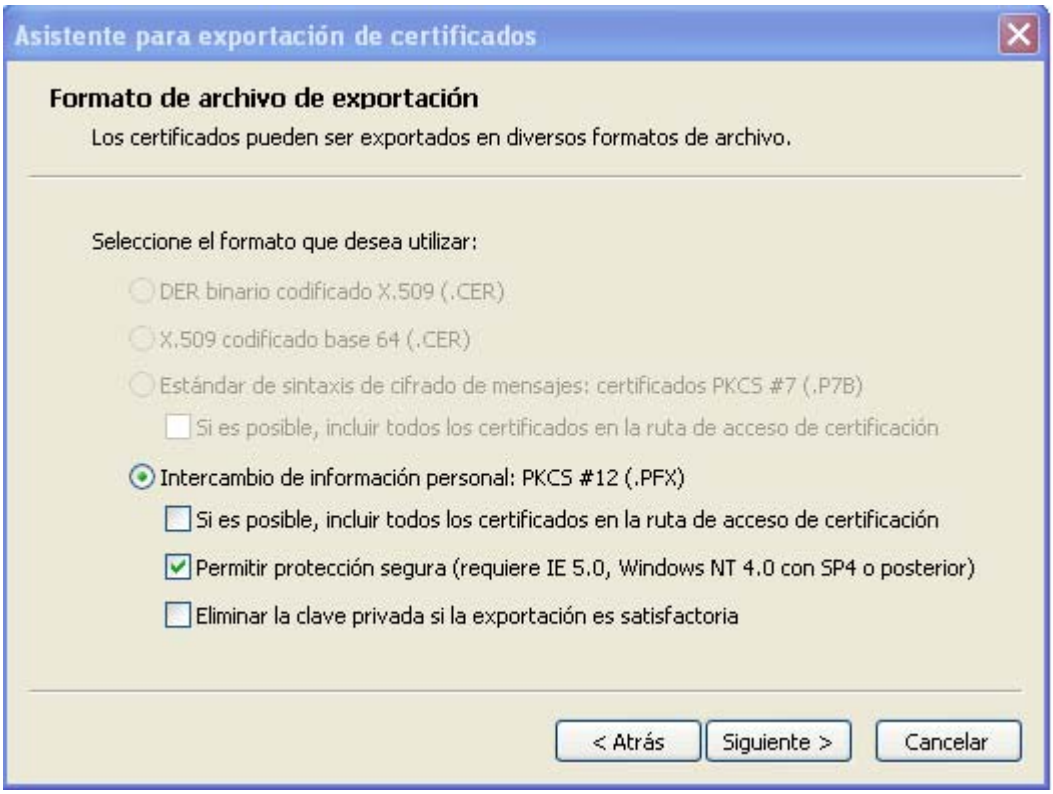
Deberemos seleccionar aquel certificado que queremos exportar del sistema. Para ver los detalles de cualquiera de ellos simplemente debemos pulsar sobre él dos veces el botón izquierdo del ratón. Aparecerá una ventana con la fecha de emisión, la caducidad, la Autoridad de Certificación (CA) que lo ha expedido, etc.

Cuando hayamos seleccionado el certificado que queremos exportar del sistema, pulsaremos el botón correspondiente para que el asistente de exportación nos indique los pasos que debemos seguir. Dicho asistente nos solicitará información sobre el tipo de exportación, el formato de salida que queremos que tenga el fichero, la ruta de salida, la contraseña para las claves, etc.

En la primera ventana se nos pregunta si queremos exportar la clave privada junto con el certificado. Sin esa clave el certificado servirá para que aquel que esté en posesión del mismo cifre correos con nuestra clave pública y pueda verificar nuestra firma digital. Esto es útil sobre todo para aplicaciones de correo en las que queramos utilizar criptografía. Si no exportamos la clave privada, lo que no se podrá hacer con el certificado son operaciones de firma ni descifrado.
Si queremos exportar el certificado con todas sus funcionalidades debemos hacerlo exportando también su clave privada. El fichero así obtenido contendrá el certificado completo, pudiendo realizar así todo tipo de operaciones criptográficas. Con el fin de evitar que ese fichero pudiese caer en manos no deseadas y alguien usase nuestro certificado en nuestro nombre, el fichero quedará protegido por una contraseña que indique el usuario.

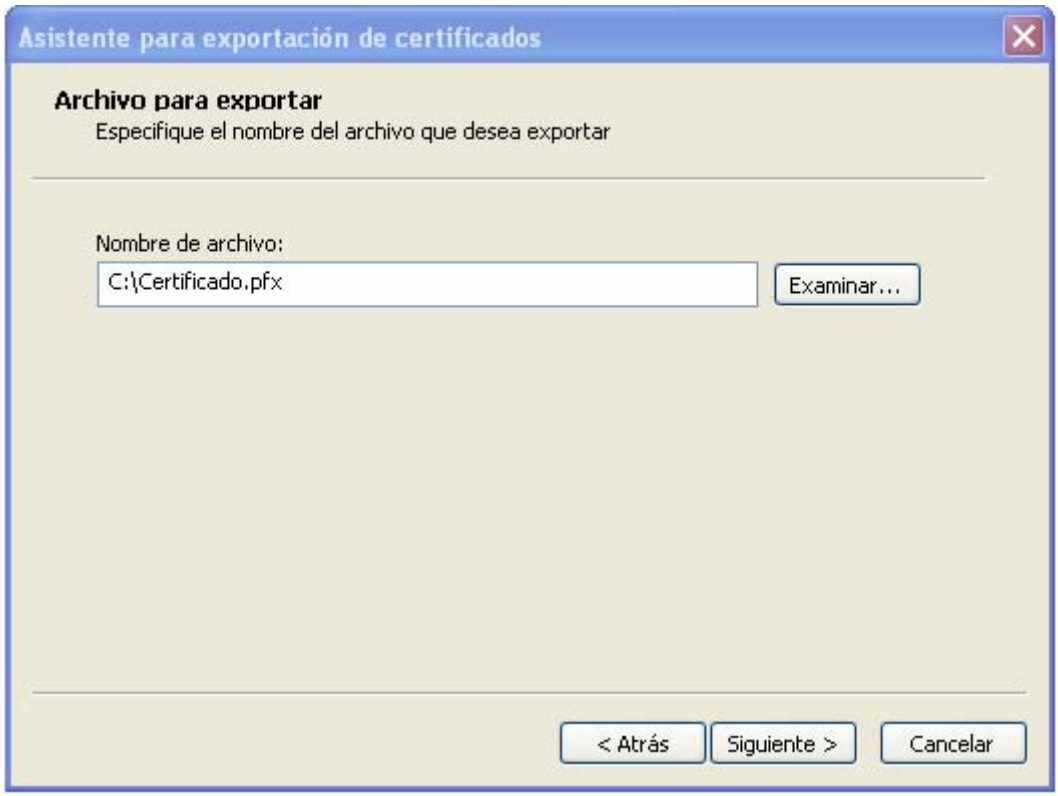
Al elegir exportar la clave privada, en la siguiente pantalla nos preguntará la contraseña con que queremos protegerla. Es importante recordar dicha contraseña ya que sin ella no será posible reinstalar el certificado.

En la pantalla siguiente el asistente nos preguntará acerca del formato que queremos que tenga el fichero de salida. Por defecto usaremos PKCS#12, que genera archivos .pfx.



Tras la selección del formato, deberemos introducir la contraseña para proteger la clave privada (en caso de que hayamos decidido exportarla).

El último paso antes de la exportación es indicar la ruta y el nombre de salida del fichero. El asistente nos mostrará una pantalla en la que podemos teclearlo completo, o pulsar el botón de "Examinar" y navegar hasta la carpeta de destino e indicar sólo el nombre que queremos darle al fichero.

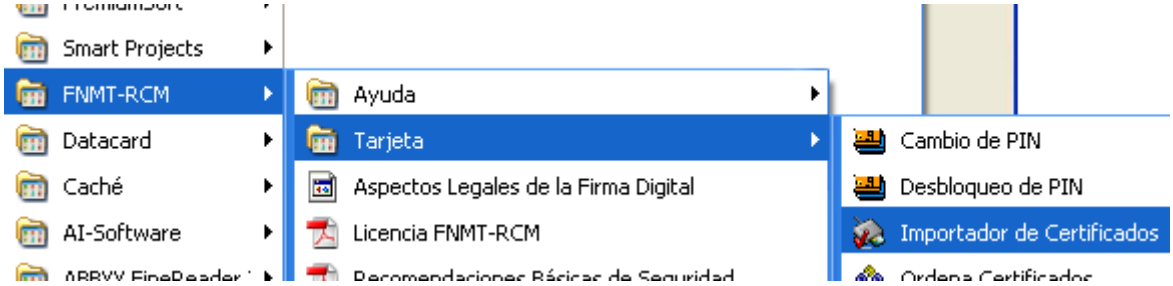


Al pulsar en "Siguiente" se mostrará una ventana con la información final del fichero.

Cuando pulsemos el botón de "Finalizar", el asistente realizará la exportación a fichero. En caso de que todo vaya correctamente se nos mostrará un mensaje de verificación. El fichero se habrá generado en la ruta indicada en pantallas anteriores y estará listo para ser importado a cualquier otro sistema

3. Importación del certificado a la tarjeta criptográfica.

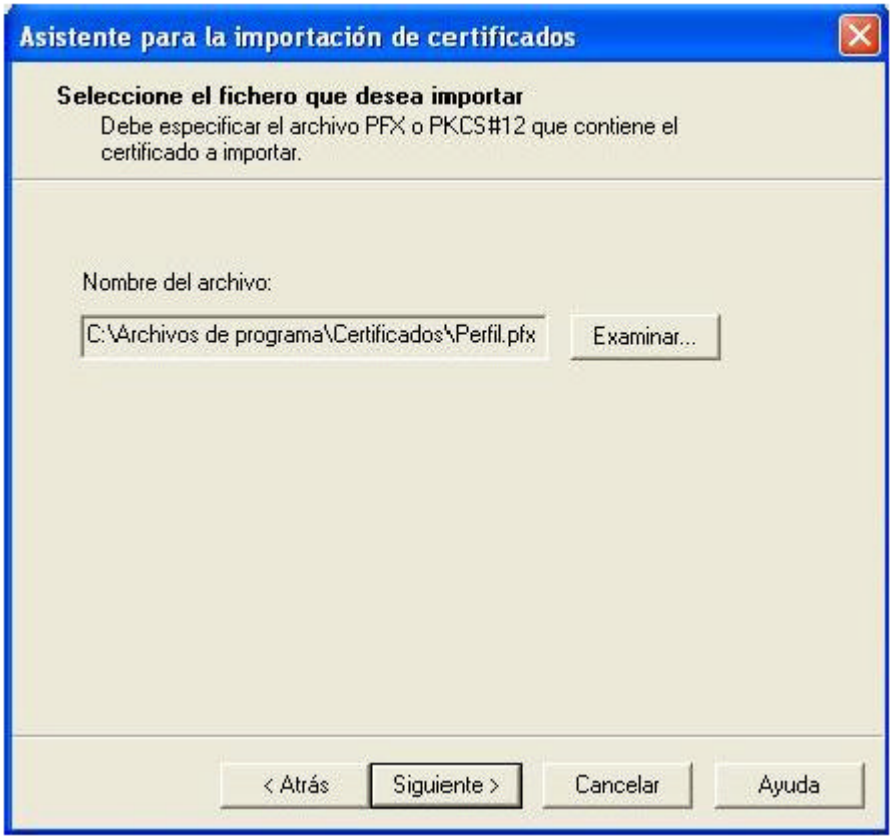
Introducimos la tarjeta en el lector, abrimos el programa y elegimos la opción "**Importador de certificados**"



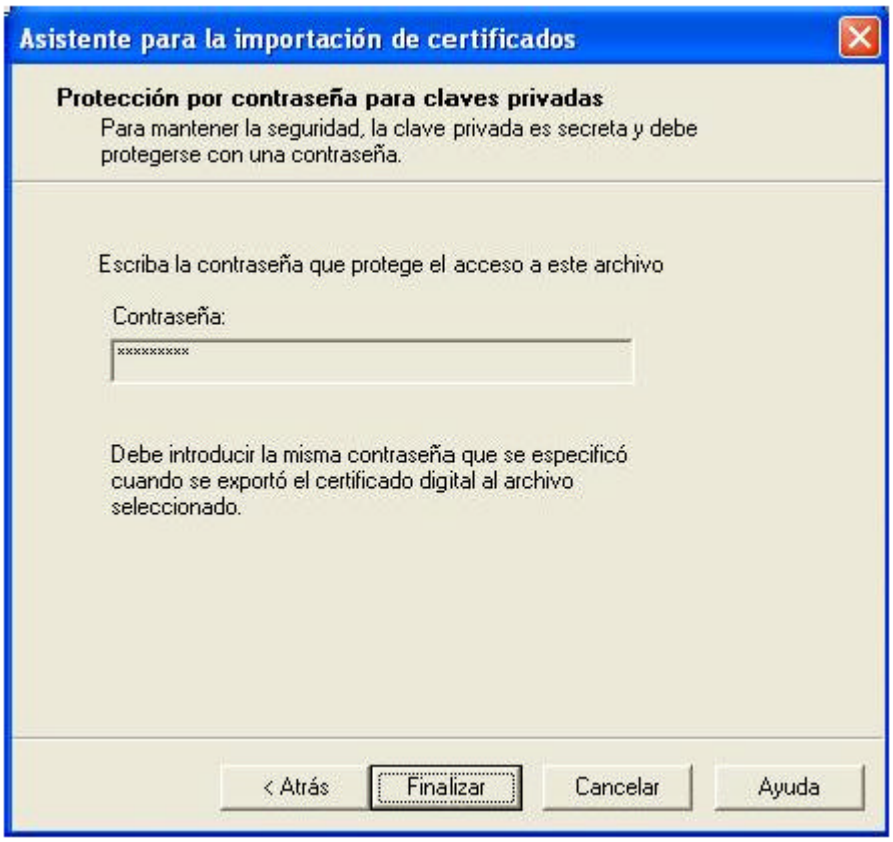
Inicialmente nos muestra una ventana con información sobre el proceso que vamos a seguir, además de información adicional sobre qué es un certificado digital, su utilidad y las ventajas de almacenarlo en tarjeta inteligente. Después nos indicará los pasos que debemos ir cumpliendo para realizar correctamente la importación.

La segunda pantalla del asistente nos va a solicitar la ruta en la que se encuentra el archivo pfx o p12 en el que está almacenado el certificado que queremos importar a la tarjeta. Dicho archivo se habrá generado mediante una operación previa de exportación, realizada desde el navegador Microsoft Internet Explorer.

La ventana de selección de fichero contiene un botón "Examinar" que nos permite navegar a través del explorador de archivos hasta encontrar la ruta adecuada. De esta manera evitaremos tener que escribir la ruta completa.



Una vez indicada la ruta al fichero, el asistente nos solicitará la contraseña para acceder al certificado. Dicha clave se la asigna el usuario al fichero en el momento de exportarlo desde el navegador hacia el archivo pfx. Sin ella será imposible realizar la importación a la tarjeta ya que no se tendrá acceso a las claves del certificado



Cuando tengamos la tarjeta introducida en el lector, comenzará la importación del certificado software. Para poder acceder a la tarjeta, el asistente nos solicitará que insertemos el PIN. De esta manera quedaremos autenticados contra ella y tendremos acceso a la creación de objetos.

Si todo ha ido correctamente, el certificado quedará almacenado en la tarjeta y será idéntico al software, pero con las ventajas añadidas de guardarlo en un soporte hardware.