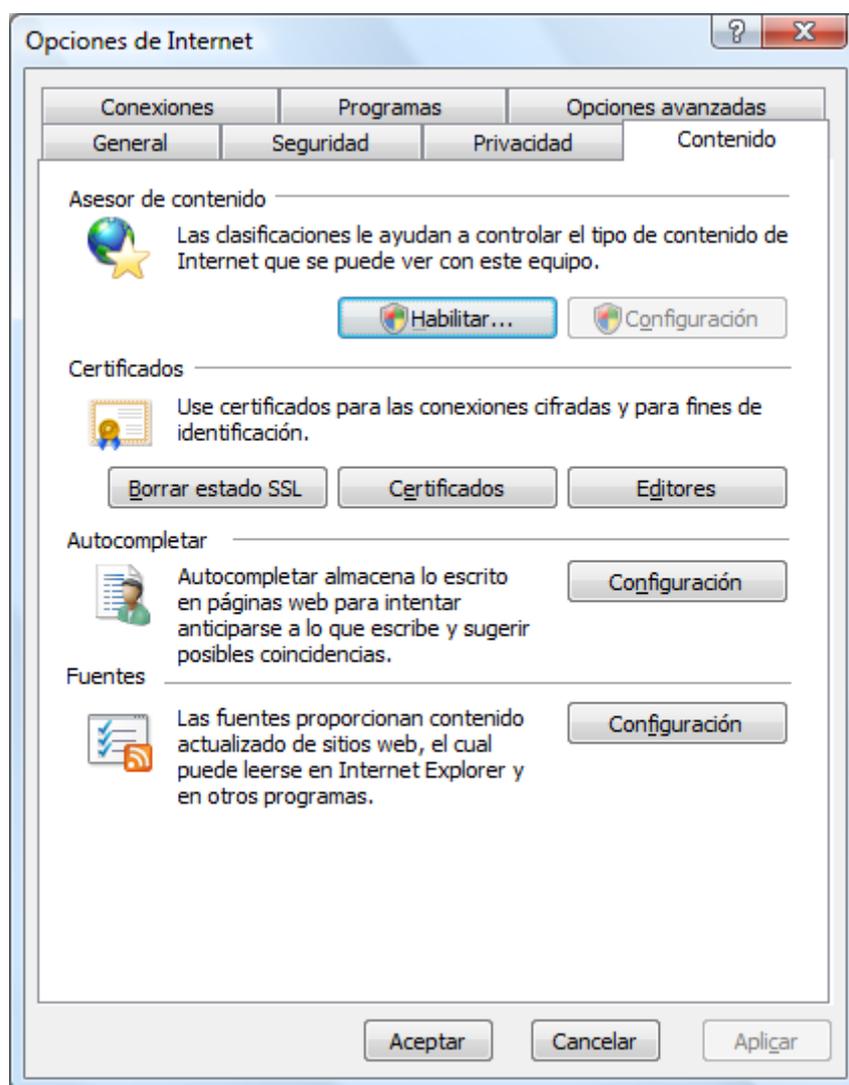


## Guía de exportación de datos de firma (certificado y clave privada) a un fichero de disco

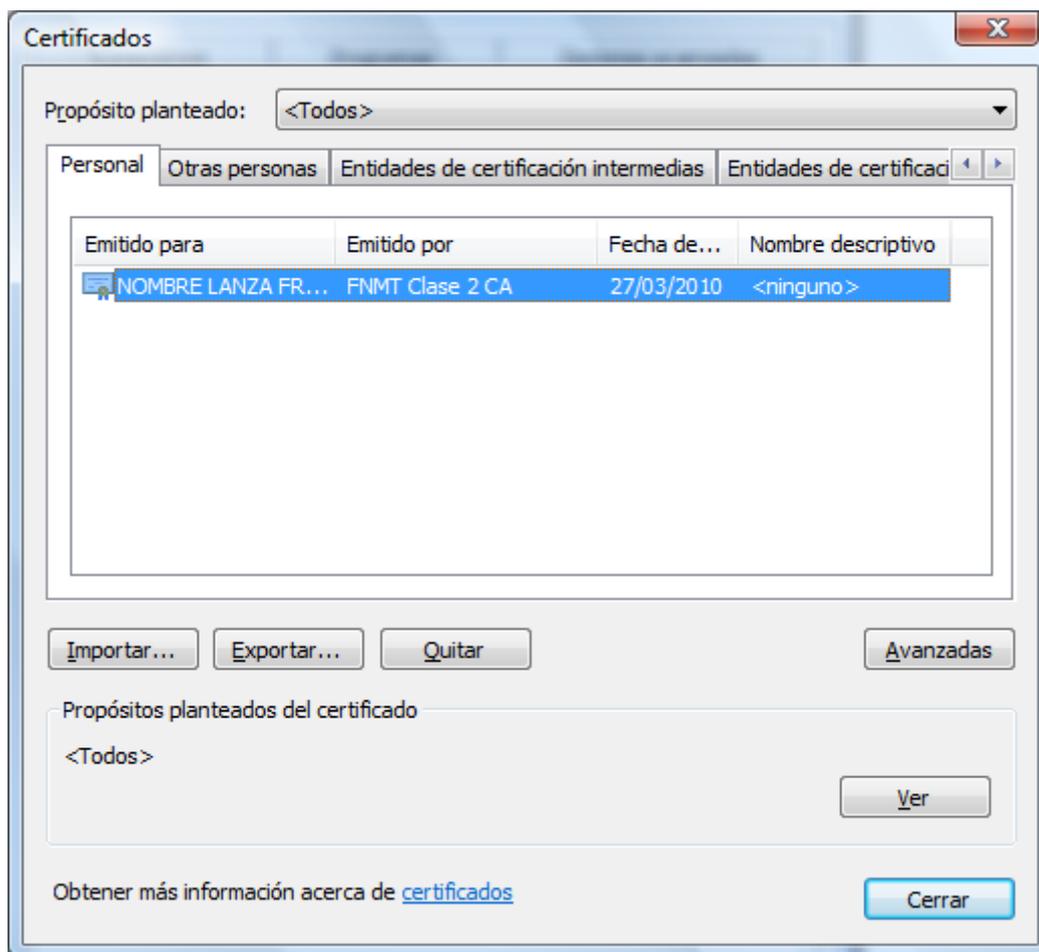
Esta guía explica, paso a paso, cómo exportar datos de firma desde un navegador de Internet<sup>1</sup>, que es donde suelen almacenarse normalmente, a un fichero de disco. Puede que ya tengas una copia de seguridad de tu certificado y clave privada en un fichero, en cuyo caso no te hará exportar de nuevo los datos. Si éste no fuera el caso, continúa leyendo...

Para empezar, abre el navegador (si no lo has hecho ya). Despliega el menú “Herramientas” (arriba a la derecha) y selecciona “Opciones de Internet”. Verás un cuadro de diálogo con varias pestañas. Selecciona la pestaña “Contenido”. Verás algo como esto:



<sup>1</sup> En este caso se ha usado el navegador Internet Explorer 7, de Microsoft. Para otros navegadores, como Firefox, u otras versiones de Internet Explorer, el proceso es muy parecido.

Pulsa el botón “Certificados”. Se mostrará un nuevo cuadro de diálogo con información de todos los certificados instalados en el navegador, como el siguiente:



Observa que, por defecto, aparece seleccionada la pestaña “Personal”, mostrándose el almacén de certificados personales (del usuario). El certificado a exportar debe encontrarse en este almacén (quizá haya más de uno). En el caso del ejemplo anterior solamente está mi certificado de clase 2CA, emitido por la FNMT<sup>2</sup>.

Si no dispones de un certificado personal, puedes obtenerlo, de forma gratuita, a través del sitio web del proyecto CERES, de la FNMT. Tienes más información sobre cómo hacerlo en el portal del empleado, <http://intranet.colmenarviejo.es/empleado/como-obtener-un-certificado-digital-de-la-fnmt>

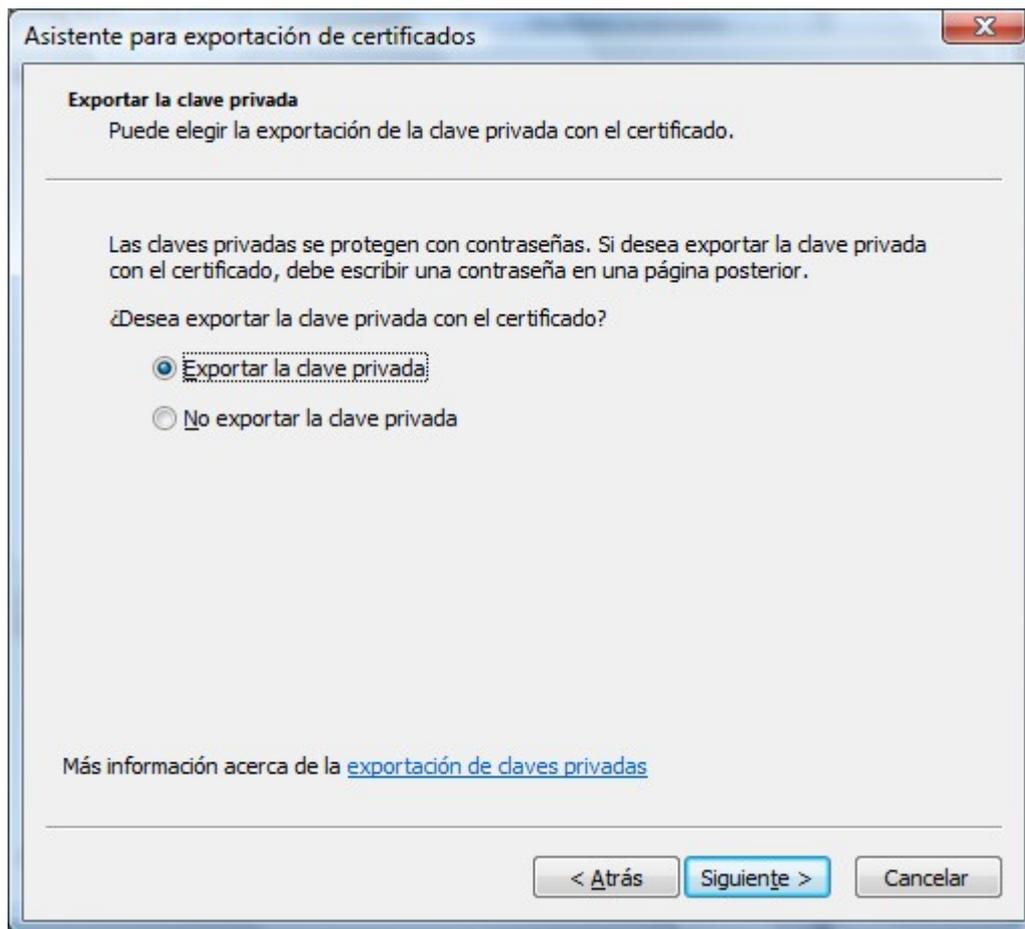
Selecciona el certificado en el que estás interesado y pulsa el botón “Exportar”.

<sup>2</sup> Fábrica Nacional de Moneda y Timbre, <http://www.fnmt.es/>

Aparecerá el asistente para la exportación de certificados:

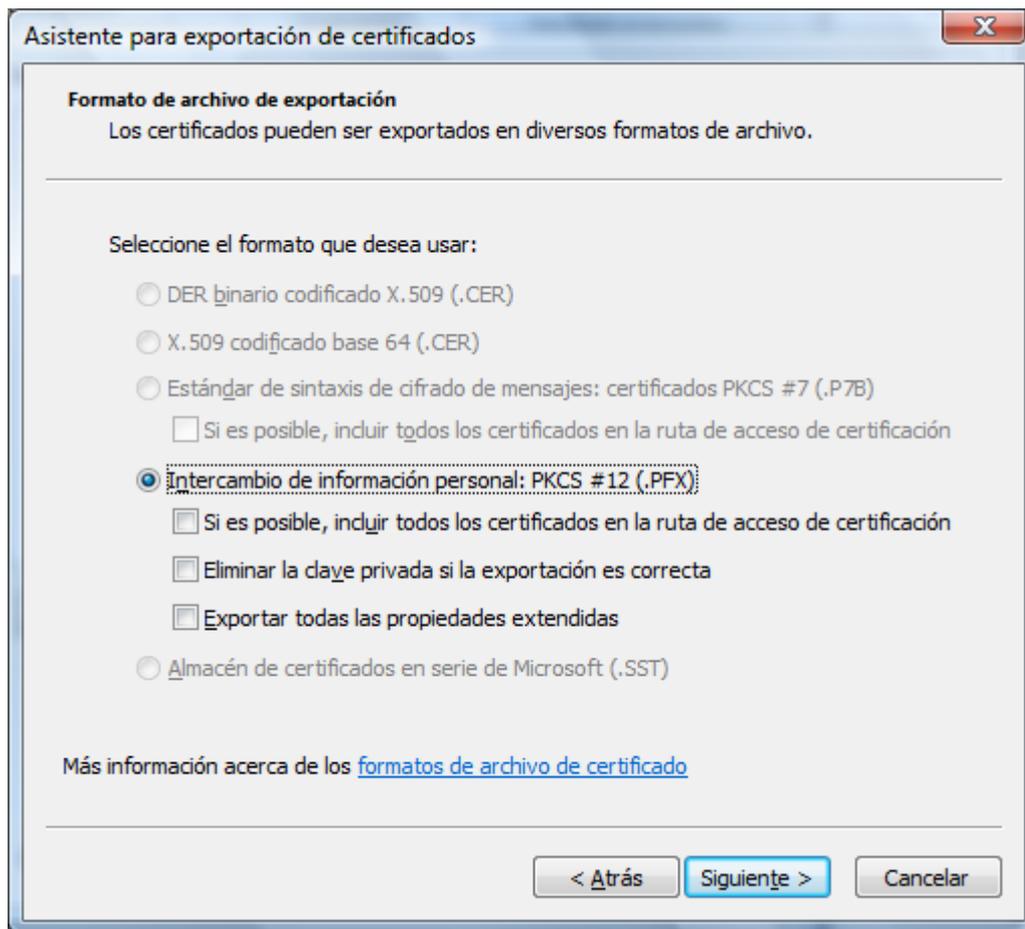


Pulsa el botón “Siguiente”. Verás el siguiente cuadro de diálogo:



Selecciona la opción “Exportar la clave privada” y pulsa el botón “Siguiente”.

Verás un nuevo cuadro de diálogo:



Selecciona la opción “Intercambio de información personal: PKCS #12” y pulsa el botón “Siguiente”.

Verás un nuevo cuadro de diálogo:

Asistente para exportación de certificados

**Contraseña**  
Para mantener la seguridad, debe proteger la clave privada por medio de una contraseña.

Escriba y confirme una contraseña.

Contraseña:

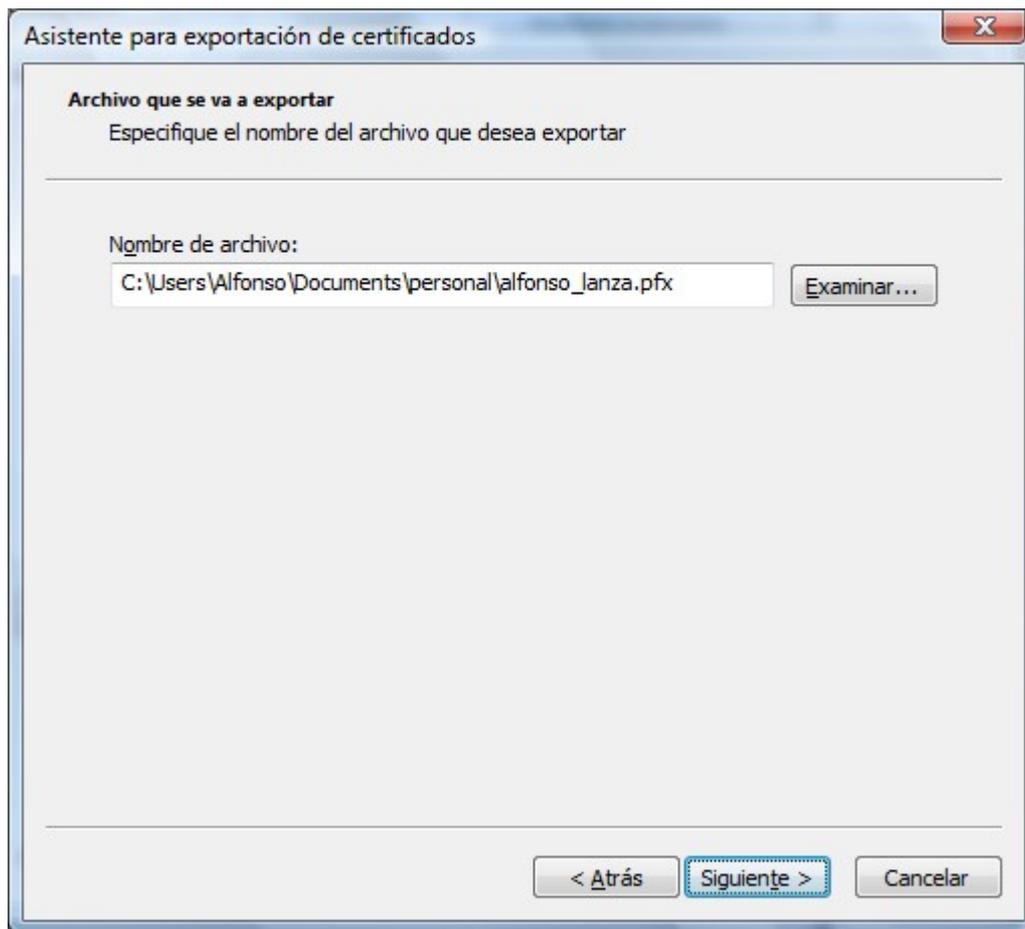
Escribir y confirmar contraseña (obligatorio):

< Atrás    Siguiente >    Cancelar

Se van a exportar tu certificado y tu clave privada. Ambos dos permiten que puedas firmar y que se pueda verificar tu firma. Tu certificado es público, mientras que tu clave privada es, como su nombre indica, privada. Es la clave privada la que permite firmar, por lo que es necesario protegerla de forma adecuada. Lo que se hace es cifrar la clave privada usando una contraseña, de manera que para usar la clave privada es preciso descifrarla antes, mediante esa contraseña. Sin conocer la contraseña no se puede descifrar la clave privada y, por tanto, no se puede usar la misma para firmar. Por seguridad, debes elegir esa contraseña en este punto.

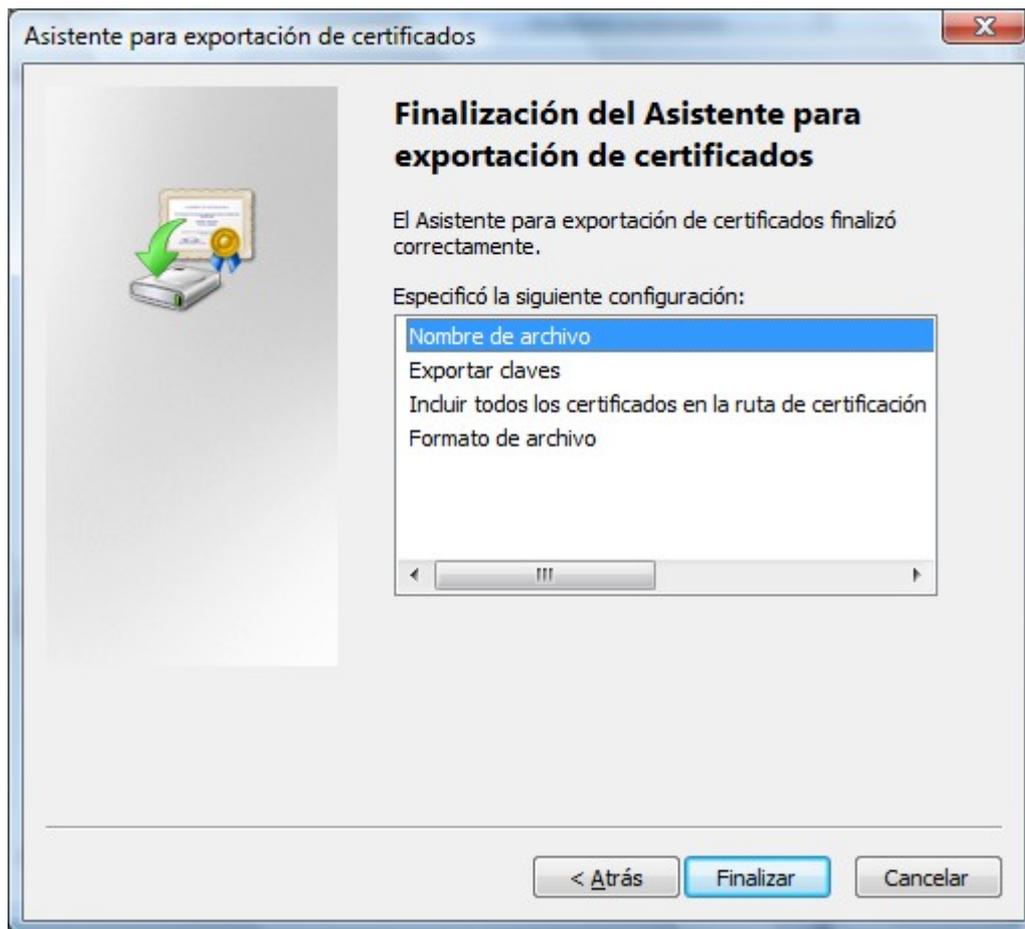
Escribe (y confirma) una contraseña para cifrar tu clave privada y pulsa el botón “Siguiente”.

Verás un nuevo cuadro de diálogo:



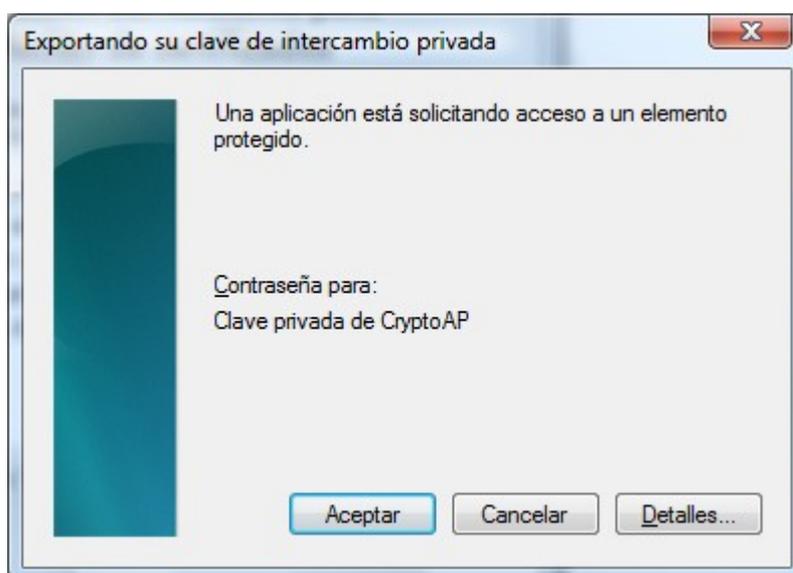
Certificado y clave privada se exportarán a un fichero. Debes especificar el nombre de fichero y su ubicación en el disco. Elige un nombre de fichero, ayudándote del botón “Examinar”. Nota que la extensión del fichero será “.pfx”. Pulsa el botón “Siguiente”.

Verás la siguiente pantalla de confirmación:



Pulsa el botón “Finalizar”.

Puede que veas el siguiente cuadro de diálogo:



Pulsa el botón “Aceptar”.

Verás la siguiente pantalla de confirmación:



Pulsa el botón “Aceptar”.

Has terminado. Comprueba que el fichero con tus datos de firma se encuentra en la ubicación que elegiste. Ahora podrás usar este fichero para cargar tus datos de firma en el sistema de notificaciones telemáticas. Podrás hacerlo a través del panel de control.