Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

SALVAGUARDA DE LA CLAVE PRIVADA EN LA SOLICITUD DE UN CERTIFICADO DE COMPONENTE

	NOMBRE	FECHA
Elaborado por:	Soporte Técnico	17/05/2010
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	17/05/2010	Creación del documento	Soporte Técnico

Referencia:

Documento clasificado como: *Público/ Distribución limitada*

1. INTRODUCCIÓN

El presente documento muestra describe un método de salvaguarda de la clave privada de un certificado de componente para evitar cualquier problema que pueda surgir en la descarga del mismo.

El proceso consta de tres pasos que se detallan a continuación. Al final del documento se explica el proceso de instalación del certificado.

Este procedimiento sólo es válido para cuando hacemos la salvaguarda de la clave.

El documento sólo es útil para la solicitud de claves desde Internet Explorer. Se describe el proceso de solicitud desde nuestra página.

2. SALVAGUARDA DE LA CLAVE

2.1. SOLICITUD DEL CERTIFICADO

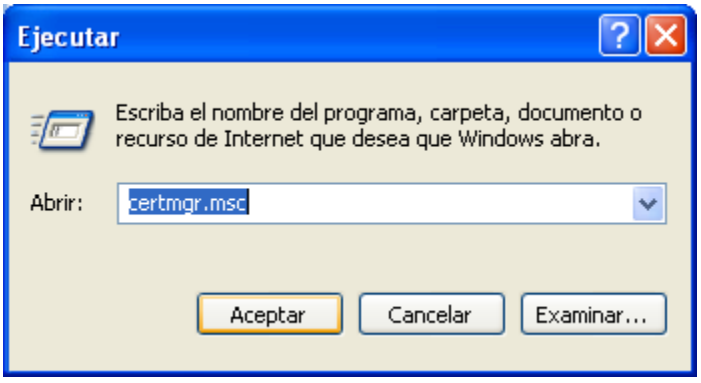
Para hacer la solicitud del certificado deberá acceder a una de las siguientes páginas:

- Clase 2: https://apus.cert.fnmt.es/PrerregistroSolicitudesComponentes/index.html
- APE: https://ape.cert.fnmt.es/PrerregistroSolicitudesComponentesAPE/index.html

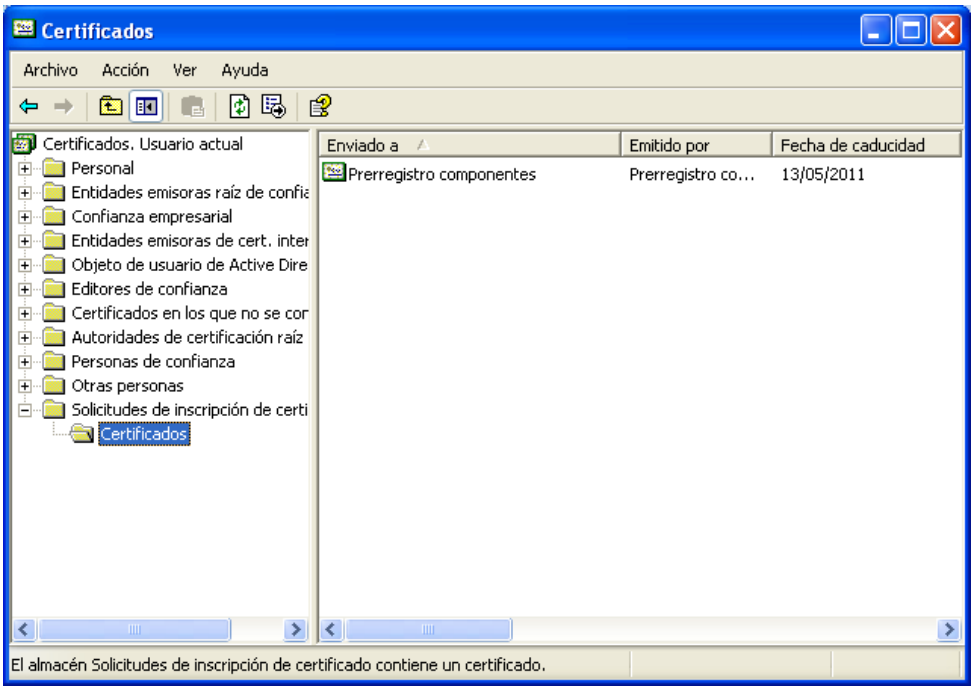
Una vez en la página haremos la solicitud desde la opción de la izquierda que nos permite generar una clave. Ahora puede, o bien guardar el pkcs#10 generado en un fichero de texto para luego pegarlo en la solicitud y hacer los pasos indicados en el manual, o bien puede realizar la solicitud del certificado y al finalizar seguir las indicaciones aquí marcadas, queda a elección del lector.

2.2. SALVAR LA CLAVE PRIVADA

Diríjase a Inicio → Ejecutar y teclee certmgr.msc → Aceptar



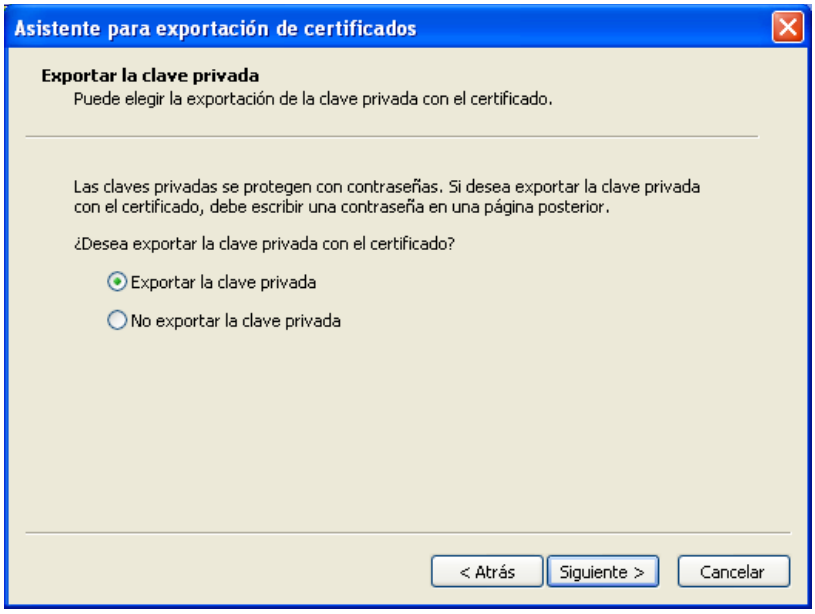
Esta acción abre el almacén de certificados de la cuenta en uso.



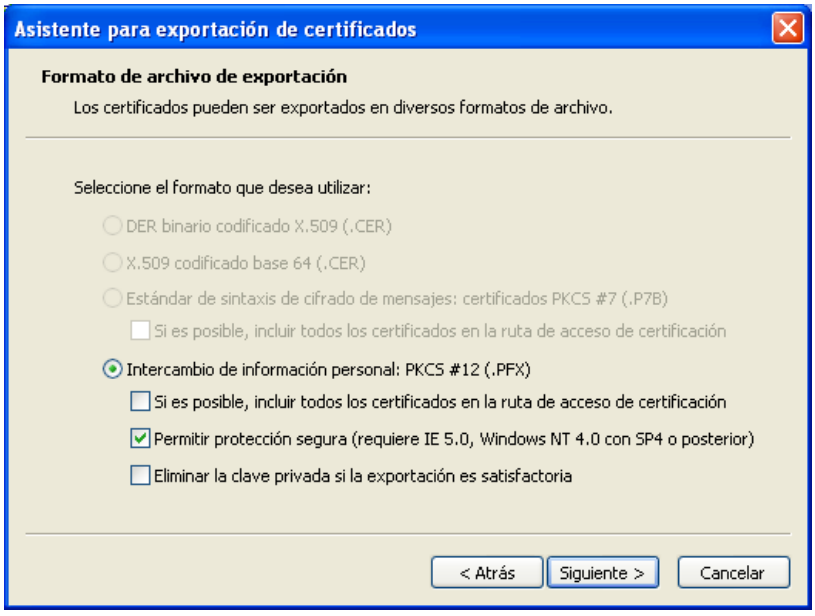
En esta ventana seleccionaremos la carpeta “Solicitud de inscripción de Certificados” y dentro de esta certificados. Deberá aparecer en la parte de la derecha un certificado con el nombre “Prerregistro componentes” con fecha una año posterior al día de la solicitud.

Posicione el ratón sobre este elemento y pulse el botón derecho, del menú contextual seleccione la opción **Todas las Tareas → Exportar**, esto inicia el asistente de exportación de certificados.

Pulsamos en **Siguiente** para iniciar el asistente, en la siguiente pantalla, seleccionamos la opción de **Exportar la Clave Privada.**

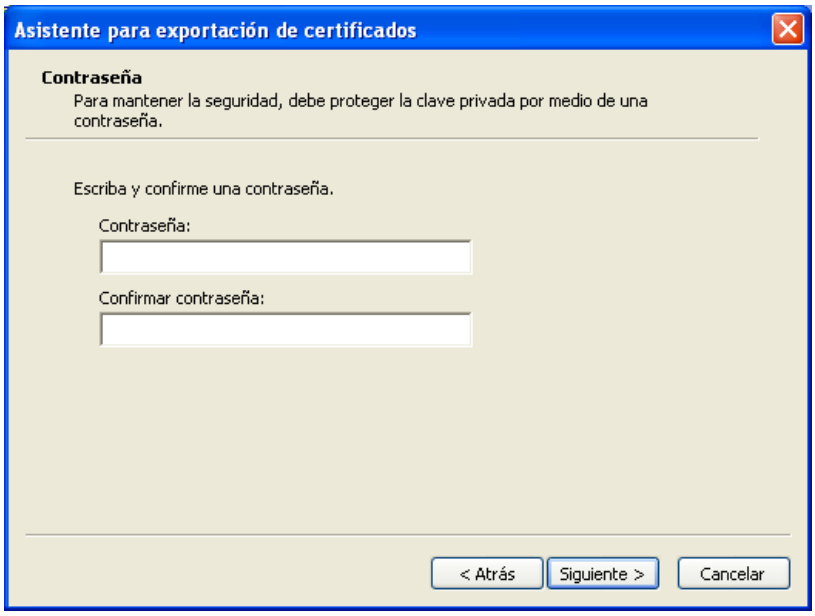


Pulsamos en **Siguiente.**

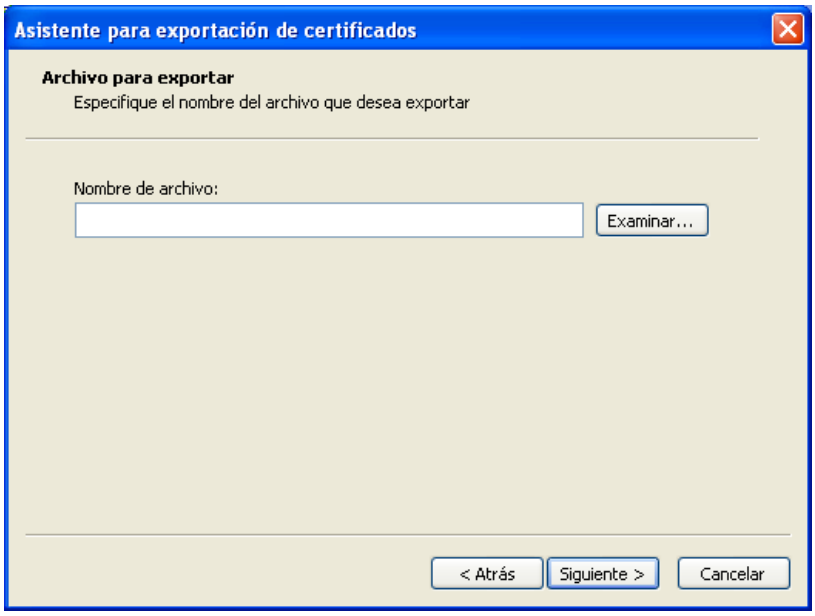


Pulsamos en **Siguiente.**

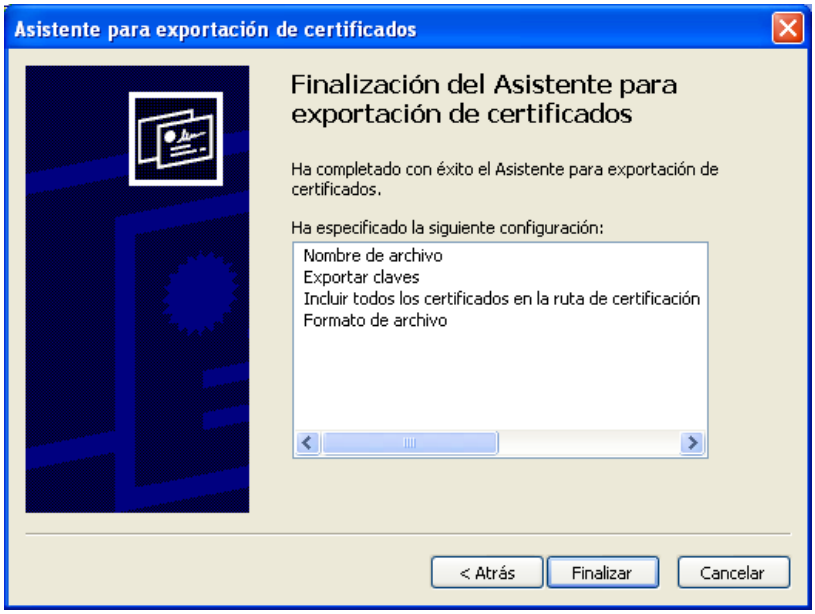
Establecemos una contraseña que se nos solicitará en el momento de la importación (restablecimiento) de la clave privada, no es obligatoria, pero si se establece una no la olvide o no se podrá volver a importar la clave privada del certificado.



Pulsamos en **Siguiente,** seleccionamos el nombre del archivo y la ubicación del mismo.



Pulsamos en **Siguiente,** aparece el resumen del proceso de exportación.



Pulsamos en **Finalizar.** Si todo ha ido correctamente el asistente nos avisará del éxito de la exportación.

Nota: El fichero generado en esta fase tiene extensión .pfx, pero no hay que confundirlo con el que se genera en la exportación del certificado, este fichero es únicamente la clave privada.

2.3. SALVAR EL FICHERO ASOCIADO A LA CLAVE PRIVADA.

Para guardar la clave privada iremos a C:\Documents and Settings*****\Datos de programa\Microsoft\Crypto\RSA\S-1-5-21-1479873048-1369066082-1663972903-6908.

***** = usuario con el que se ha realizado la solicitud del certificado.

La secuencia de números varía de un equipo a otro.

De esta carpeta, haremos copia en otro directorio (cualquiera), del último fichero generado, que debe corresponder con la fecha y hora de la generación de la clave.

3. INSTALACIÓN DEL CERTIFICADO

Para realizar la instalación correcta del certificado son necesarios tres elementos.

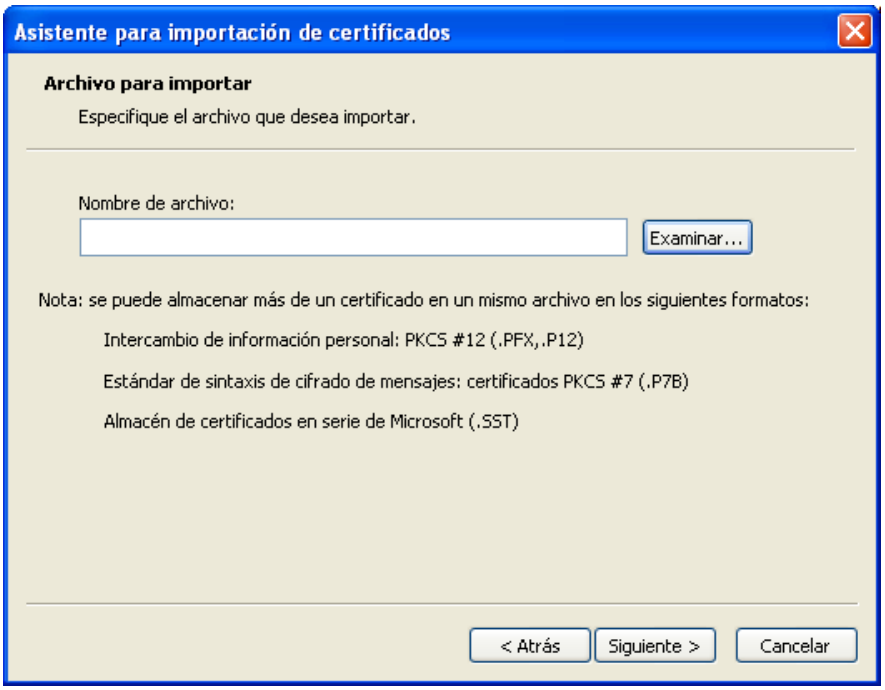
- La clave privada exportada. Paso 2.2 de este manual.
- El fichero asociado a la clave privada. Paso 2.3 de este manual.
- El certificado, que se descarga de las páginas de solicitud de certificados mencionadas al principio del documento.

3.1. RESTABLECIMIENTO DE LA CLAVE PRIVADA

Diríjase a Inicio → Ejecutar y teclee certmgr.msc → Aceptar. Esta acción abre el almacén de certificados de la cuenta en uso.

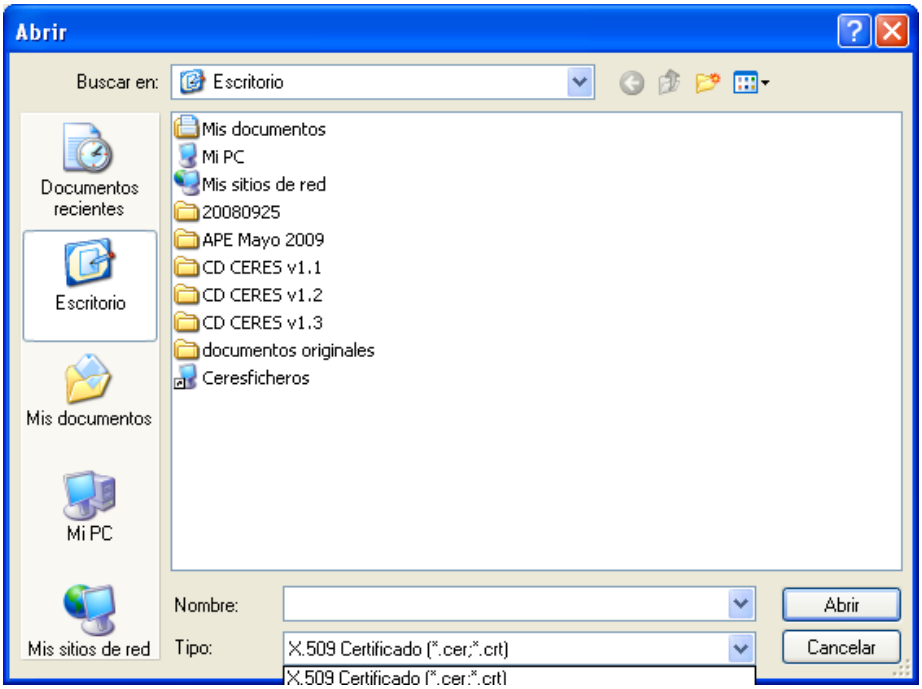
En esta ventana seleccionaremos la carpeta "Solicitud de inscripción de Certificados" y dentro de esta certificados. Ahora pulsamos con el botón derecho del ratón en la zona libre de la parte derecha de la pantalla. Del menú contextual seleccionamos **Todas las Tareas → Importar.**

Iniciamos el asistente para la importación de certificados. Pulsamos en **Siguiente** para iniciar la importación.

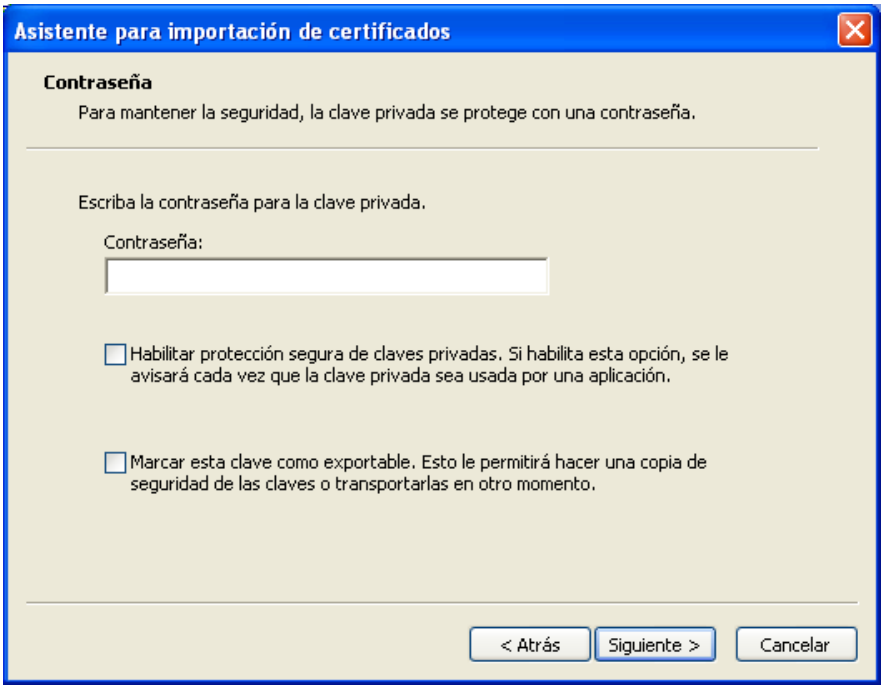


Pulsamos en **Examinar** y seleccionamos el fichero generado en el paso 2.2 del manual.

En **Tipo** de certificado seleccione **Intercambio de Información Personal (*.pfx, *p12)**

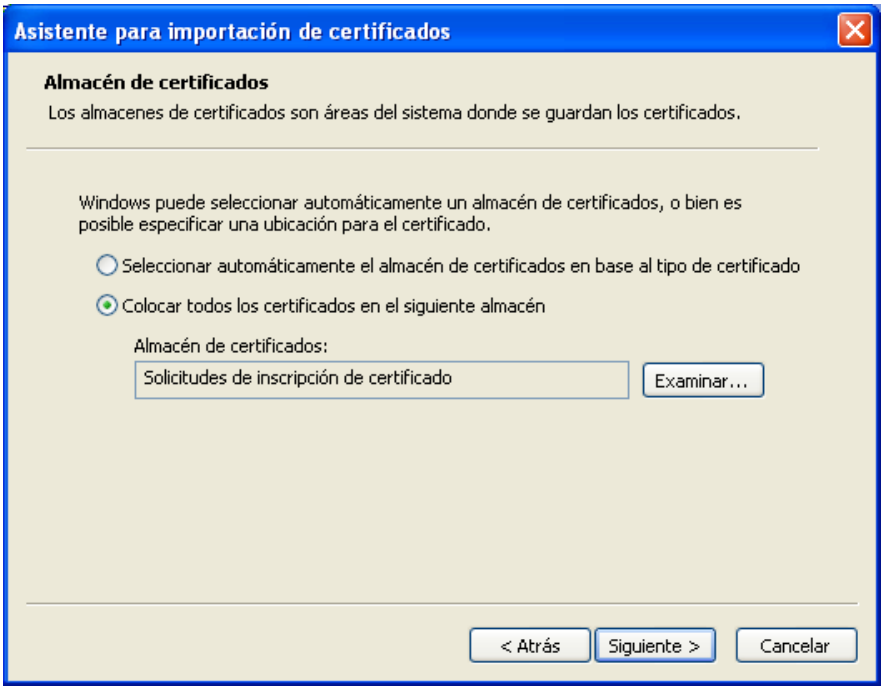


Ahora buscamos la clave privada y pulsamos **Abrir** y **Siguiente.**



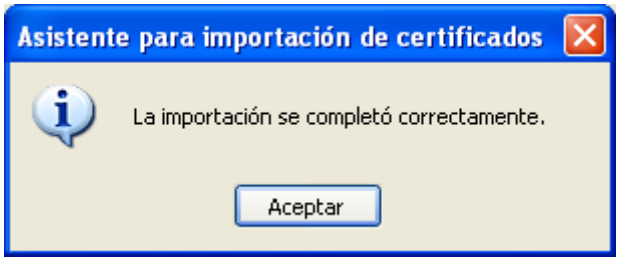
Esta pantalla nos pide la clave que le dimos al fichero en el momento de la exportación. Para poder llevar la clave a otro equipo deberá marcar la casilla de **Marcar esta clave como exportable.**

Pulsamos en **Siguiente**



En la pantalla de selección de ubicación para la importación aparecerá por defecto el Almacén de **Solicitudes de inscripción de certificado.**

Pulsamos en **Siguiente.** Nos aparece el resumen del proceso de importación y pulsamos en **Finalizar.** Si todo va correctamente el asistente nos lo indicará.



3.2. COPIA DEL FICHERO ASOCIADO A LA CLAVE PRIVADA.

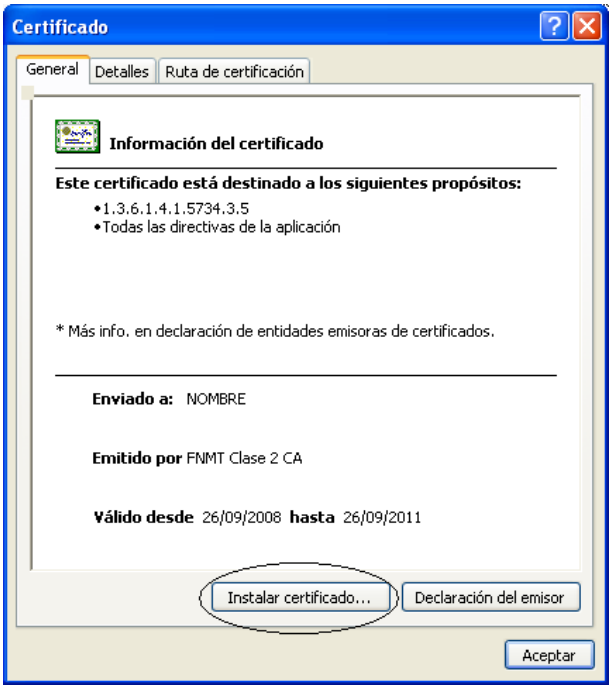
En este paso deberá copiar el archivo guardado en el punto 2.3 del manual en el directorio C:\Documents and Settings*****\Datos de programa\Microsoft\Crypto\RSA\S-1-5-21-1479873048-1369066082-1663972903-6908.

***** = usuario con el que se ha realizado la solicitud del certificado.

La secuencia de números varía de un equipo a otro.

3.3. INSTALACIÓN DE CERTIFICADO

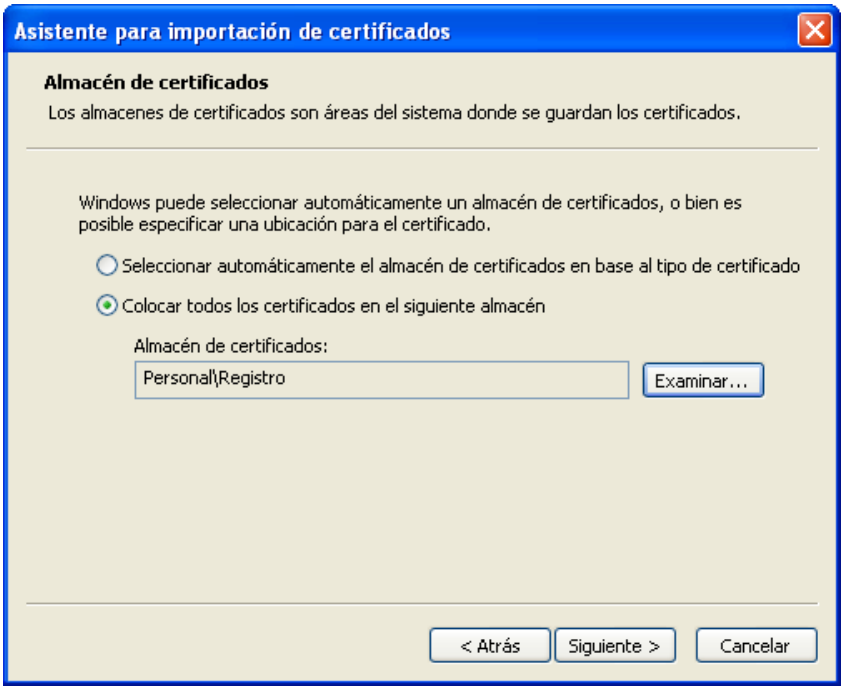
Seleccionamos el certificado descargado de la página de solicitud y hacemos doble clic sobre él.



Pulsamos en **Instalar Certificado…** se iniciará el asistente para la importación de certificados, pulsamos en **Siguiente**.

Nos aparecerá la pantalla para seleccionar la ubicación del certificado, marcamos la opción **Colocar todos los certificados en el siguiente almacén**, y pulsamos en **Examinar**…

Marcamos la casilla **Mostrar almacenes Físicos,** buscamos la carpeta **Personal,** seleccionamos la carpeta **Registro** y pulsamos **Aceptar.**



Una vez seleccionada la ubicación del certificado pulsamos en **Siguiente.** Aparece el resumen de la información de importación y pulsamos **Finalizar.** Si todo ha ido correctamente el certificado estará en el almacén Personal de la cuenta del usuario.