

Configuración del equipo utilizado

Linux Mint 20.1 Cinnamon 4.8.6
Núcleo de Linux 5.8.0 – 50 - generic
Firefox Browser 88.0 (64-bit) para Linux Mint – 1.0

Certificado digital de la FNMT

1. Certificado nuevo para persona física:

Acceder a:

<https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software>

y tener muy en cuenta que desde que iniciamos el proceso de solicitud hasta que obtenemos el certificado: no podemos formatear el disco y no podemos cambiar de equipo ni de usuario.

Como navegadores podemos utilizar: Mozilla Firefox, Google Chrome, Microsoft EDGE, Opera o Safari, el resto no es compatible de momento.

Descargar la aplicación de la FNMT para la instalación del software de generación de las claves:

<https://www.sede.fnmt.gob.es/descargas/descarga-software/instalacion-software-generacion-de-claves>

Elegir el SO que utilizamos: Windows, Mac o Linux y seguir las instrucciones

2. Solicitar el Certificado:

Una vez configurado correctamente el equipo se debe proceder a llenar la solicitud de Certificado. Ojo si hemos utilizado anteriormente otro certificado de la FNMT, al solicitar uno nuevo el primero quedara sin efecto.

<https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software/solicitar-certificado>

3. Acreditar nuestra identidad:

Para ello debemos acudir personalmente a una Oficina de Acreditación de Identidad con el Código de Solicitud que habremos recibido y nuestro DNI. Debido al Covid debemos comprobar el lugar que este prestando servicio y solicitar cita previa.

Localizador de oficinas: <http://mapaoficinascert.appspot.com/>

4. Descargar certificado:

Utilizar el mismo ordenador y el mismo usuario con el que realizó la solicitud e introducir los datos requeridos exactamente tal y como los introdujo entonces.

<https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-dnie/descargar-certificado>

Lo mejor es guardar este certificado en un lugar seguro y accesible para poder instalarlo en los navegadores que vayamos a utilizar.

5. Verificación del certificado:

Si posteriormente necesitamos comprobar que el certificado esta correctamente instalado y es valido

<https://www.sede.fnmt.gob.es/certificados/persona-fisica/verificar-estado>

Instalación del certificado en Firefox

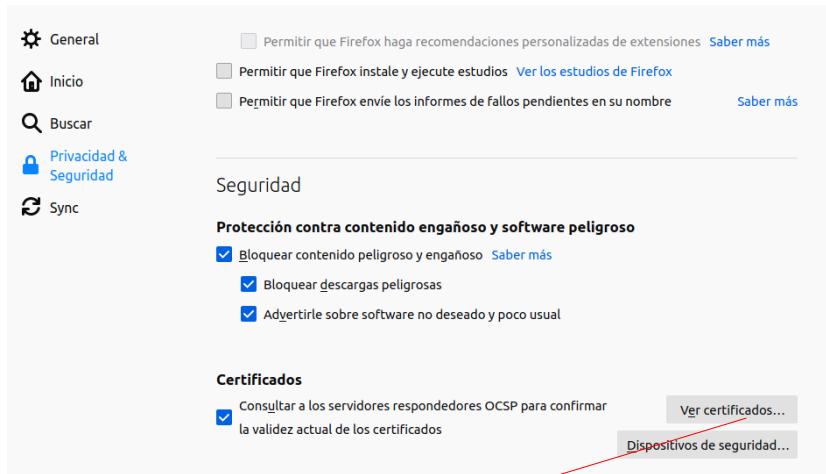
Personalmente guardo una copia de mi certificado en un Pen Drive que guardo en lugar seguro, para evitar disgustos si tengo que cambiar de equipo o de navegador.

Instalar el Certificado en Firefox es sencillo:

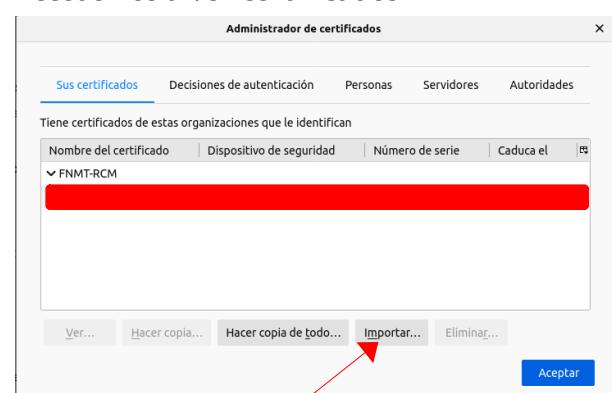
Abrimos el navegador

Vamos a Preferencias: about:preferences

Privacidad y seguridad: about:preferences#privacy
y buscamos **certificados**



Accedemos a ver certificados

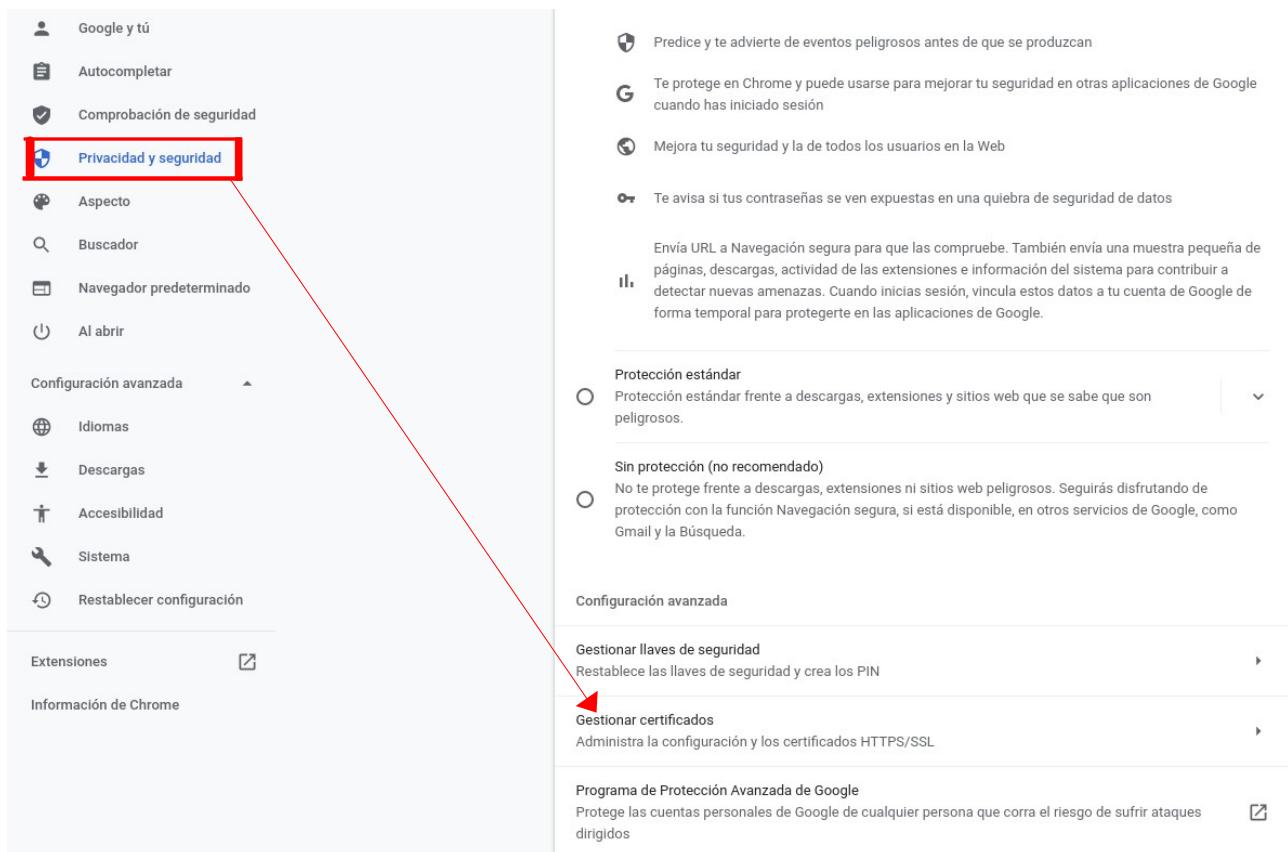


Solo nos queda **importar** el certificado obtenido de la FNMT

Instalación del certificado en Chrome

Accedemos a su configuración: chrome://settings/

Privacidad y seguridad: chrome://settings/security?search=certifi



Google y tú

Autocompletar

Comprobación de seguridad

Privacidad y seguridad

Aspecto

Buscador

Navegador predeterminado

Al abrir

Configuración avanzada

Idiomas

Descargas

Accesibilidad

Sistema

Restablecer configuración

Extensiones

Información de Chrome

Predice y te advierte de eventos peligrosos antes de que se produzcan

Te protege en Chrome y puede usarse para mejorar tu seguridad en otras aplicaciones de Google cuando has iniciado sesión

Mejora tu seguridad y la de todos los usuarios en la Web

Te avisa si tus contraseñas se ven expuestas en una quiebra de seguridad de datos

Envía URL a Navegación segura para que las compruebe. También envía una muestra pequeña de páginas, descargas, actividad de las extensiones e información del sistema para contribuir a detectar nuevas amenazas. Cuando inicias sesión, vincula estos datos a tu cuenta de Google de forma temporal para protegerte en las aplicaciones de Google.

Protección estándar

○ Protección estándar frente a descargas, extensiones y sitios web que se sabe que son peligrosos.

○ Sin protección (no recomendado)

No te protege frente a descargas, extensiones ni sitios web peligrosos. Seguirás disfrutando de protección con la función Navegación segura, si está disponible, en otros servicios de Google, como Gmail y la Búsqueda.

Configuración avanzada

Gestionar llaves de seguridad

Restablece las llaves de seguridad y crea los PIN

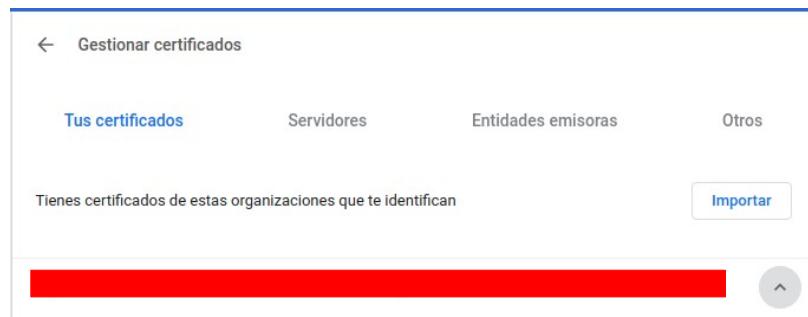
Gestionar certificados

Administra la configuración y los certificados HTTPS/SSL

Programa de Protección Avanzada de Google

Protege las cuentas personales de Google de cualquier persona que corra el riesgo de sufrir ataques dirigidos

Y se mostrarán los certificados instalados y la forma de importarlos:



← Gestionar certificados

Tus certificados

Servidores

Entidades emisoras

Otros

Tienes certificados de estas organizaciones que te identifican

Importar

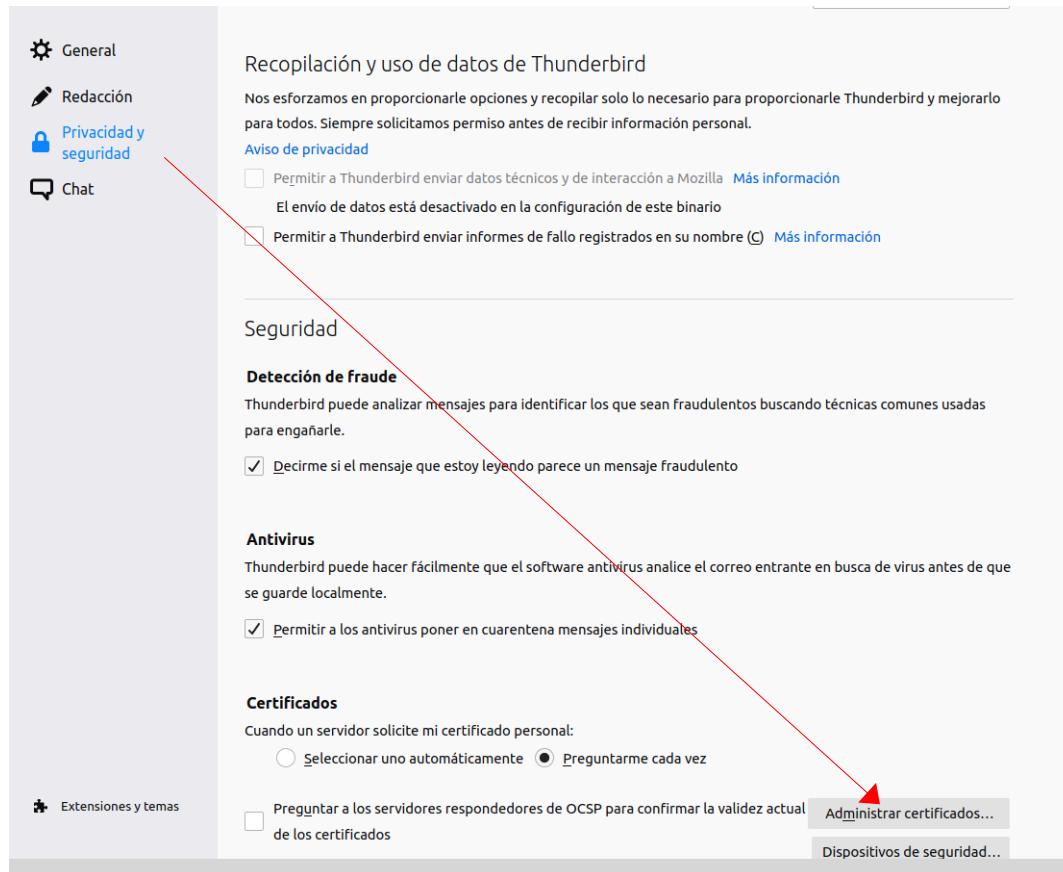
A partir de aquí solo debemos pulsar en importar, acceder a nuestro certificado de la FNMT y ya esta.

Firmar digitalmente correos con certificado en Thunderbird

Abrimos Thunderbird

Editar

Preferencias



General

Redacción

Privacidad y seguridad

Chat

Recopilación y uso de datos de Thunderbird

Nos esforzamos en proporcionarle opciones y recopilar solo lo necesario para proporcionarle Thunderbird y mejorarlo para todos. Siempre solicitamos permiso antes de recibir información personal.

Aviso de privacidad

Permitir a Thunderbird enviar datos técnicos y de interacción a Mozilla [Más información](#)
El envío de datos está desactivado en la configuración de este binario

Permitir a Thunderbird enviar informes de fallos registrados en su nombre (C) [Más información](#)

Seguridad

Detección de fraude

Thunderbird puede analizar mensajes para identificar los que sean fraudulentos buscando técnicas comunes usadas para engañarle.

Decírmelo si el mensaje que estoy leyendo parece un mensaje fraudulento

Antivirus

Thunderbird puede hacer fácilmente que el software antivirus analice el correo entrante en busca de virus antes de que se guarde localmente.

Permitir a los antivirus poner en cuarentena mensajes individuales

Certificados

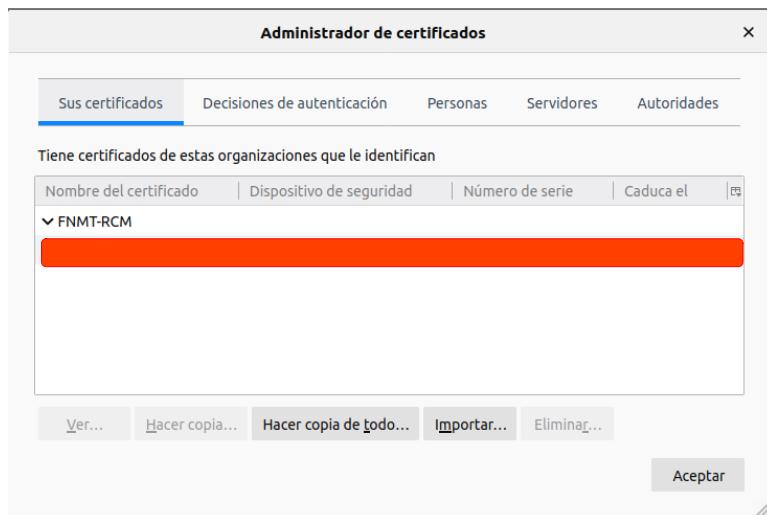
Cuando un servidor solicite mi certificado personal:

Seleccionar uno automáticamente Preguntarme cada vez

Preguntar a los servidores respondedores de OCSP para confirmar la validez actual de los certificados [Administrar certificados...](#) [Dispositivos de seguridad...](#)

Extensões y temas

Pulsando en Administrar certificados encontramos:



Administrador de certificados

Sus certificados

Tiene certificados de estas organizaciones que le identifican

Nombre del certificado	Dispositivo de seguridad	Número de serie	Caduca el
FNMT-RCM			

Ver... Hacer copia... Hacer copia de todo... Importar... Eliminar... Aceptar

Solo tenemos que importar el certificado.

Si accedemos a

Editar → Configuración de la cuenta → Cifrado extremo a extremo

Cifrado extremo a extremo

Para enviar mensajes cifrados o firmados digitalmente, debe configurar una tecnología de cifrado, ya sea OpenPGP o S/MIME.

Seleccione su clave personal para habilitar el uso de OpenPGP o su certificado personal para habilitar el uso de S/MIME. Para una clave personal o certificado usted posee la clave secreta correspondiente. [Saber más](#)

OpenPGP

Thunderbird no tiene una clave personal OpenPGP para **carmen@cluengo.es** [Agregar clave...](#)

Usar OpenPGP Key Manager para ver y administrar las claves públicas de sus correspondientes y todas las demás claves que no se enumeran anteriormente.

[Administrador de claves OpenPGP](#)

S/MIME

Certificado personal para la firma digital:

Certificado personal para cifrado:

Administrador certificados S/MIME [Seleccionar...](#) [Limpiar](#)

Administrador certificados S/MIME [Seleccionar...](#) [Limpiar](#)

Configuración predeterminada para el envío de mensajes

Si no se activa el cifrado, los contenidos del mensaje quedan expuestos fácilmente a su proveedor de correo y a la vigilancia masiva.

[No activar cifrado por defecto](#)
 [Requerir cifrado por defecto](#)

Si necesita cifrado, para enviar un mensaje debe tener la clave pública o certificado de cada destinatario.

De esta forma podremos incluir nuestro certificado digital en los correos.

Renovación del Certificado

Podemos renovar el Certificado de Persona Física durante los 60 días previos a la fecha de su caducidad, accediendo a:

<https://www.sede.fnmt.gob.es/certificados/persona-fisica/renovar>

El proceso de renovación de su Certificado de Persona Física podrá realizarse durante los 60 días previos a la fecha de caducidad de su certificado y siempre y cuando no haya sido previamente revocado.

Para renovar el certificado es necesario instalar el software que se indica en este apartado.

¿Cómo puedo saber cuándo caduca mi certificado?

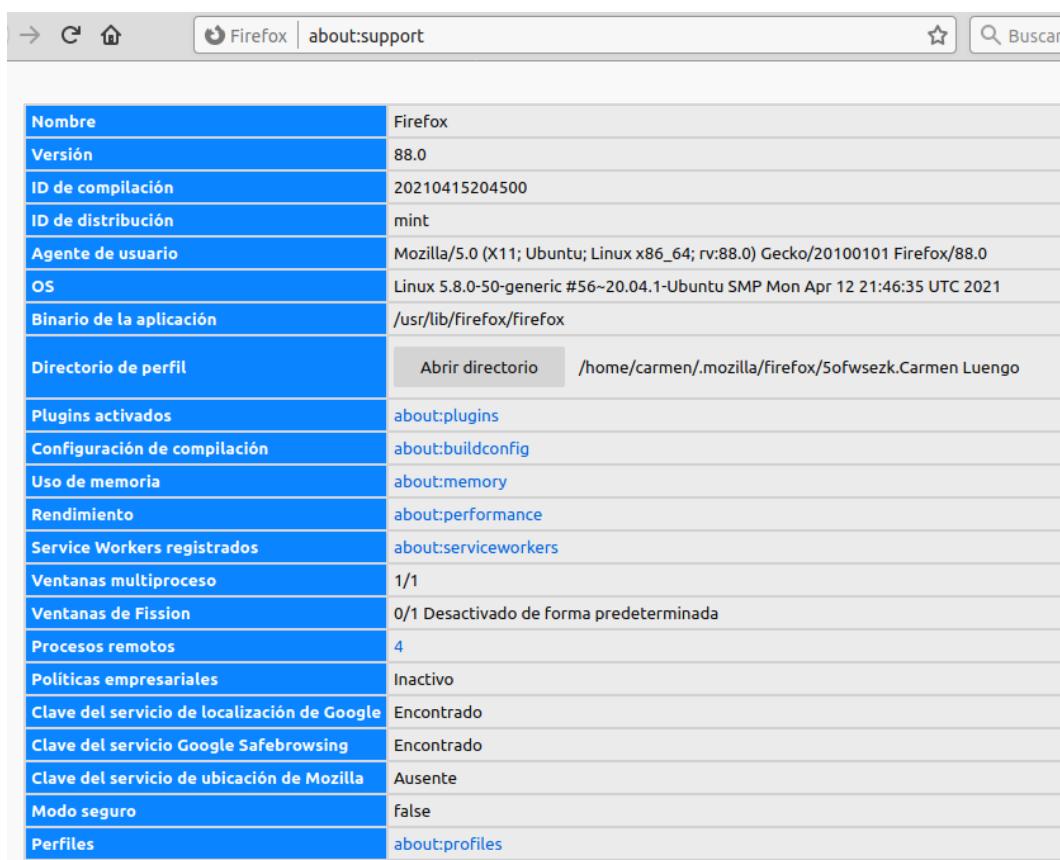
La renovación consiste en tres pasos que deben realizarse en el orden señalado:

1. Configuración previa. Para renovar el certificado es necesario instalar el software que se indica en este apartado.
2. Solicitar la renovación. Asegúrese de tener instalado su Certificado FNMT de Persona Física en el navegador desde el que va a solicitar la renovación, se autenticará con él y al final de este proceso le enviaremos un Código de Solicitud que necesitará para poder descargar su certificado renovado.
3. Descargar el certificado. Aproximadamente 1 hora después de solicitar la renovación y haciendo uso del código de solicitud que le hemos remitido a su cuenta de correo electrónico, desde aquí podrá descargar e instalar su certificado renovado y realizar una copia de seguridad (RECOMENDADO).

Si está interesado en adquirir una tarjeta o USB criptográficos de la FNMT entre en nuestro [CATÁLOGO DE SERVICIOS](#)

¿Dónde está instalado el certificado?

En el caso de Firefox los certificados se almacenan en el directorio del perfil de Firefox. Podemos utilizar la ayuda Help que encontramos en las tres rayas y después en la opción “Mas información para resolver problemas”



Nombre	Firefox
Versión	88.0
ID de compilación	20210415204500
ID de distribución	mint
Agente de usuario	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0
OS	Linux 5.8.0-50-generic #56~20.04.1-Ubuntu SMP Mon Apr 12 21:46:35 UTC 2021
Binario de la aplicación	/usr/lib/firefox/firefox
Directorio de perfil	Abrir directorio /home/carmen/.mozilla/firefox/5ofwsezk.Carmen Luengo
Plugins activados	about:plugins
Configuración de compilación	about:buildconfig
Uso de memoria	about:memory
Rendimiento	about:performance
Service Workers registrados	about:serviceworkers
Ventanas multiproceso	1/1
Ventanas de Fission	0/1 Desactivado de forma predeterminada
Procesos remotos	4
Políticas empresariales	Inactivo
Clave del servicio de localización de Google	Encontrado
Clave del servicio Google Safebrowsing	Encontrado
Clave del servicio de ubicación de Mozilla	Ausente
Modo seguro	false
Perfiles	about:profiles

Aquí se ve el Directorio de perfil, si lo abrimos veremos su contenido, de este contenido parece que los ficheros que tienen que ver con el certificado digital son: **cert9.db** y posiblemente **key4.db** y **pkcs11.txt**

En: <https://support.mozilla.org/es/kb/los-ficheros-que-almacena-tus-contraseñas-en-firefox>

En el apartado de Configuraciones de certificados de seguridad se dice: “El archivo **cert9.db** guarda todas tus configuraciones de certificados de seguridad y cualquier certificado SSL que hayas importado a Firefox. Deber ser el llamado **Almacén de certificados**”.

En la Configuraciones de los dispositivos de seguridad se dice: “El archivo **pkcs11.txt** guarda la configuración de los **módulos de seguridad**”.

Parece que en **key4.db** se almacenan passwords y names y existe alguna asociación con **cert9.db**.

Están los tres asociados a la librería NSS.