Manual Instalación y Configuración de Multicard PKCS11

FNMT-DNIe

Índice

FNMT-DNIe 1

1. Introducción 3

1.1. Convenciones tipográficas utilizadas en este manual 3

2. Instalación y configuración de sistemas GNU/Linux 3

2.1. Instalación 3

2.1.1. GNU/Linux basados en Debian 3

2.1.2. GNU/Linux basados en Red Hat 4

2.2. Configuración 5

3. Instalación y configuración en Mac OS X 8

3.1. Instalación 8

3.2. Configuración 9

1. Introducción

El objetivo de este breve manual es detallar los pasos necesarios para instalar y configurar los paquetes del Multicard PKCS11.

En los siguientes apartados se comenta cómo realizar el procedimiento de instalación y configuración en cada una de los siguientes entornos:

- GNU/Linux Ubuntu
- GNU/Linux Debian
- GNU/Linux Fedora
- GNU/Linux OpenSuse
- Mac OS X

1.1. Convenciones tipográficas utilizadas en este manual

Cursiva

Se escribirán en cursiva las opciones que tendrá que seleccionar en su pantalla, como por ejemplo: Pulse *Aceptar*.

Carácter Monoespaciado

Se escribirán en caracteres monoespaciados aquellas palabras que indiquen nombres de archivos, carpetas o una dirección url, como por ejemplo: Setup.exe.

Añadir también que las frases que empiezan por el carácter "#" son usadas para indicar un comando de terminal.

2. Instalación y configuración de sistemas GNU/Linux

En este punto se describen todos los pasos necesarios para la instalación y configuración del Multicard PKCS11 en las distribuciones Linux.

2.1. Instalación

2.1.1. GNU/Linux basados en Debian

Se debe descargar el paquete Multicard PKCS11 correspondiente a la distribución sobre la que se quiere realizar la instalación:

- Para sistemas de 32 bits:
    - `libpkcs11-fnmtdnie_x.x.x_i386.deb`
- Para sistemas de 64 bits:
    - `libpkcs11-fnmtdnie_x.x.x_amd64.deb`

Una vez descargado el paquete se procede a su instalación usando una de las dos metodologías siguientes:

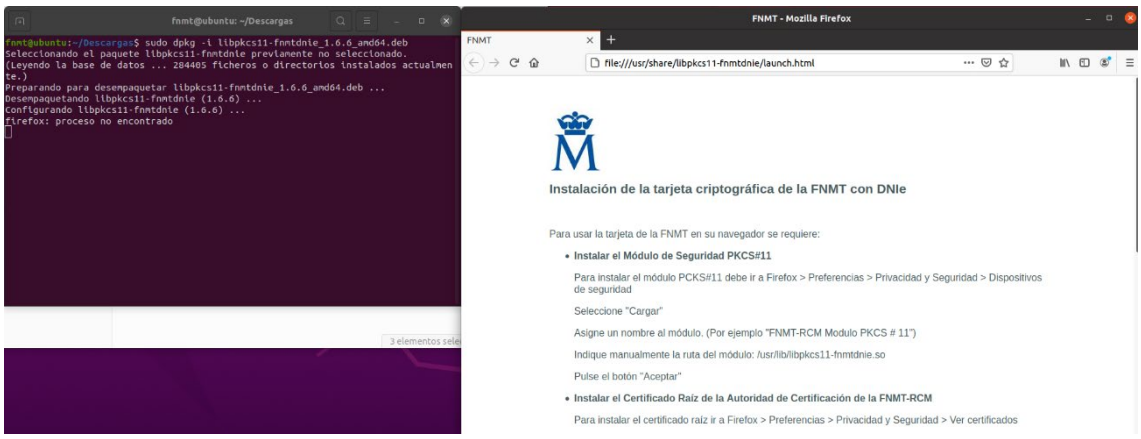
Modo automático

- hacer doble clic y seguir el asistente de instalación.

Modo manual, desde un terminal

- `# sudo apt-get install pinentry-gtk2 pcscd libassuan0`
- `# sudo dpkg -i libpkcs11-fnmtdnie_x.x.x_amd64.deb`

Se abrirá el navegador web con la guía para configurar el módulo criptográfico en Firefox (también descrito en el apartado 2.2 Configuración).



Modo automático

- Desinstalar a través de la herramienta de gestión de paquetes Synaptic

Modo manual, desde un terminal

- `# dpkg --purge libpkcs11-fnmtdnie`

2.1.2. GNU/Linux basados en Red Hat

Se debe descargar el paquete Multicard PKCS11 correspondiente a la distribución sobre la que se quiere realizar la instalación:

- Para sistemas de 32 bits:

    - `libpkcs11-fnmtdnie-x.x.x-1.i586.rpm`

- Para sistemas de 64 bits:
    - `libpkcs11-fnmtdnie-x.x.x-1.x86_64.rpm`

Una vez descargado el paquete se procede a su instalación usando una de las dos metodologías siguientes:

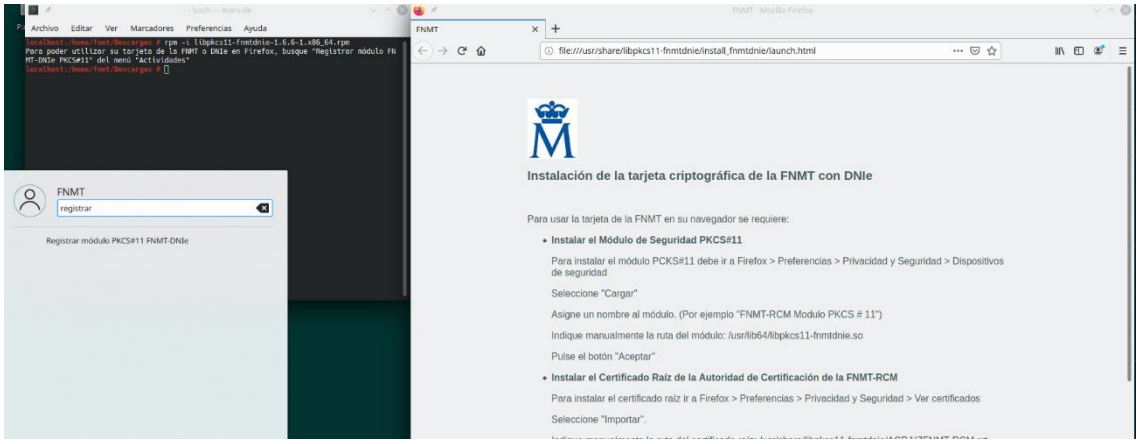
Modo automático

- hacer doble clic y seguir el asistente de instalación.

Modo manual, desde un terminal

- `# sudo yum install perl pcsc-lite.i386`
- `# sudo rpm -i libpkcs11-fnmtdnie-x.x.x-1.i586.rpm`

Al finalizar, se indicará que busque en el menú de actividades "Registrar módulo FNMT-DNIe PKCS#11", al hacer clic se abrirá el navegador web con la guía para configurar el módulo criptográfico en Firefox (también descrito en el apartado 2.2 Configuración).



Modo automático

- Desinstalar a través de la herramienta de gestión de paquetes de la distribución.

Modo manual, desde un terminal

- `# rpm -e libpkcs11-fnmtdnie`

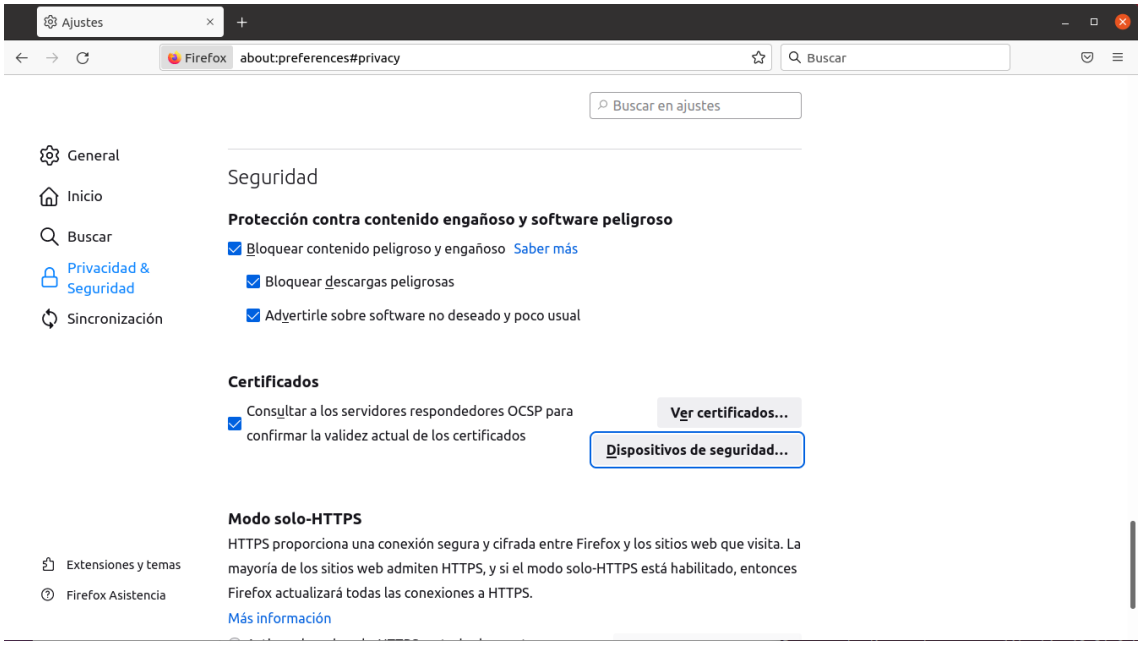
2.2. Configuración

Para evitar comportamientos anómalos, se recomienda marcar en la sección "*Firefox > Preferencias (o Ajustes) > Privacidad y Seguridad > Certificados*" la opción "*Preguntar cada vez*" referente a "Cuando un servidor solicite su certificado personal". De este modo cada vez que el navegador

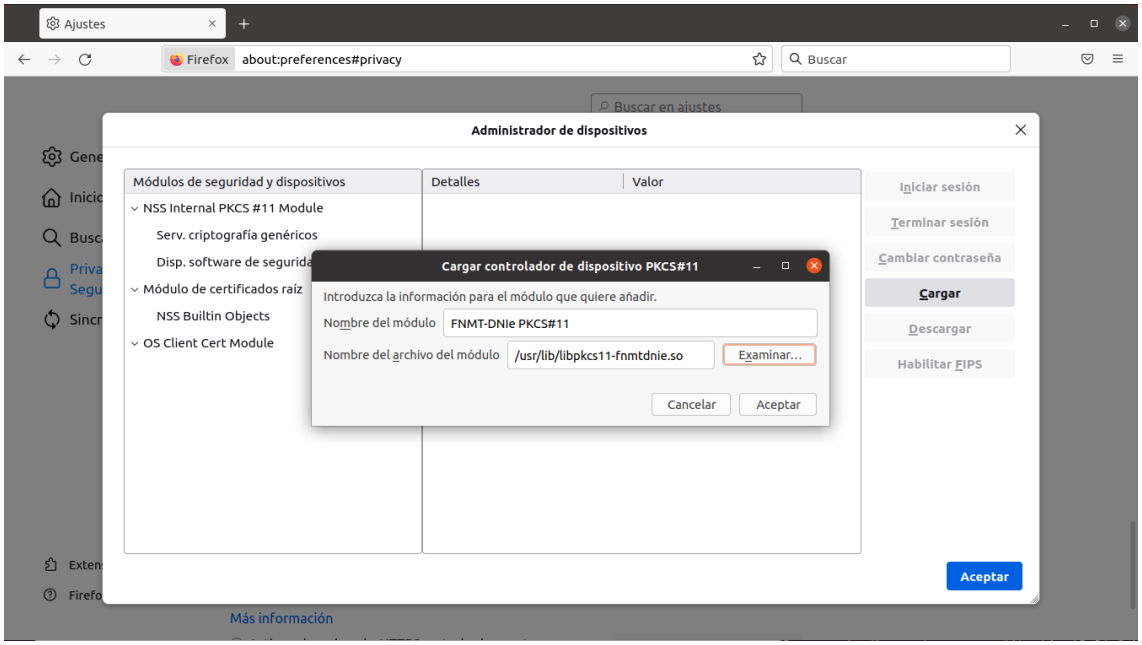
quiera usar un certificado le mostrará al usuario la lista de certificados disponibles y el usuario podrá elegir uno.

El navegador se configura del siguiente modo:

- Ir a "*Firefox > Preferencias (o Ajustes) > Privacidad y Seguridad > Dispositivos de seguridad*

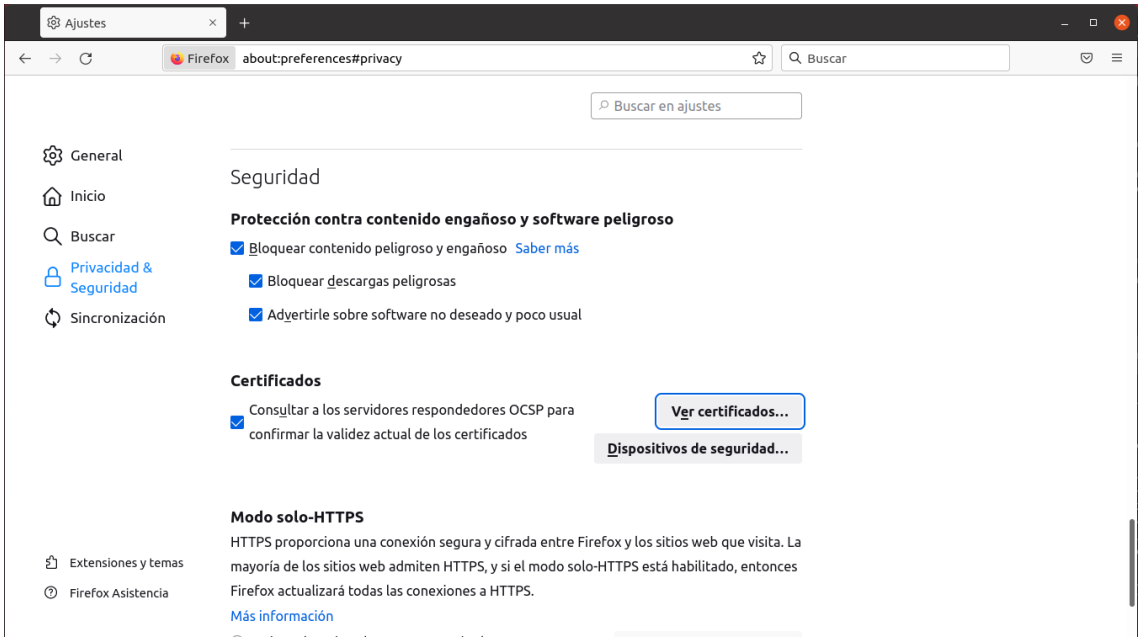


- Asigne un nombre al módulo (Por ejemplo "FNMT-DNIE Módulo P11").
- Indique manualmente la ruta del módulo:
  - `/usr/lib/libpkcs11-fnmtdnie.so`
  - `/usr/lib64/libpkcs11-fnmtdnie.so`
- Pulse el botón "*Aceptar*"

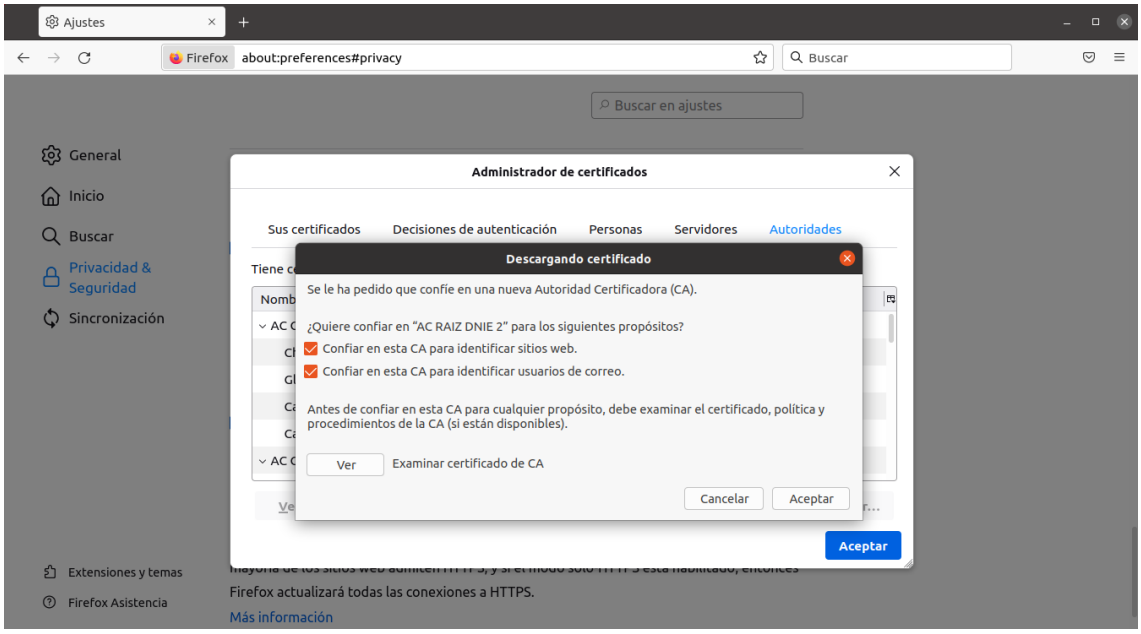


Una vez instalado el módulo, se deberán importar el certificado raíz del DNIe y el de la FNMT si no viene incluido de serie.

- Ir a "*Firefox > Preferencias (o Ajustes) > Privacidad y Seguridad*"
- Seleccione "*Ver certificados*"



- Indique manualmente la ruta del certificado raíz: `/usr/share/libpkcs11-fnmtdnie/ACRAIZDNIE-2.crt`
- El asistente le pedirá que establezca la confianza para el certificado.
- Marque todas las casillas de confianza.
- Pulse el botón "*Aceptar*"



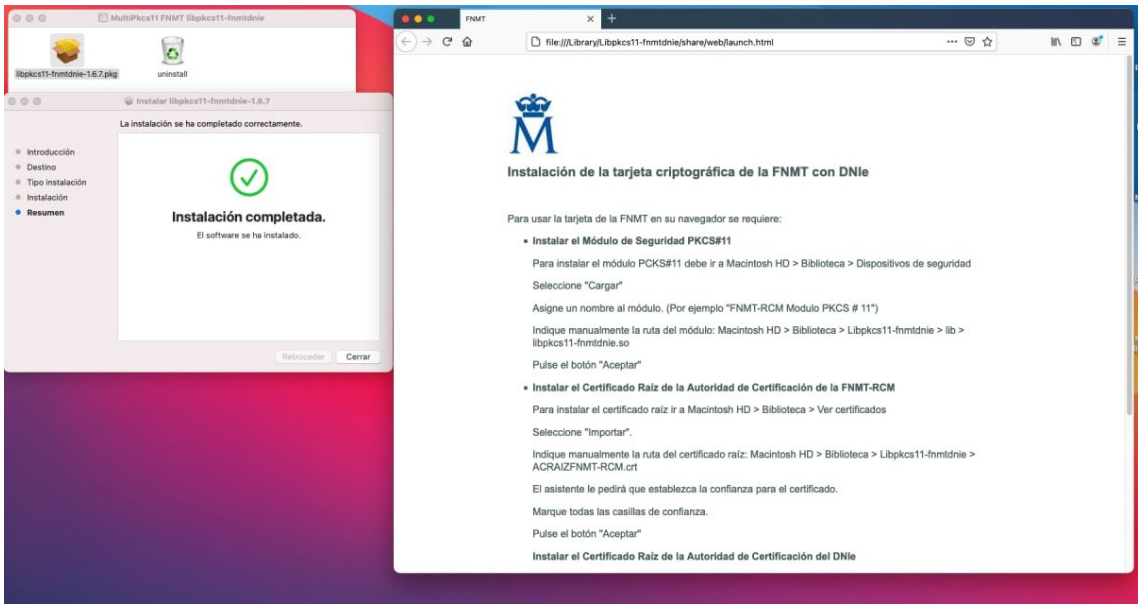
- Realizar los mismos pasos para importar el certificado raíz de la FNMT si no viene incluido de serie. Este se encuentra ubicado en `/usr/share/libpkcs11-fnmtdnie/ACRAIZFNMT-RCM.crt`

3. Instalación y configuración en Mac OS X

3.1. Instalación

Los pasos para instalar el Multicard PKCS11 en Mac OS X son los siguientes:

- Descargar el fichero `libpkcs11-fnmtdnie-x.x.x.dmg`
- Hacer doble clic en el fichero.
- Se le abrirá una ventana con el instalador.
- Hacer doble clic en el icono del instalador.
- Siga las instrucciones del asistente para completar el proceso.
- Al finalizar la instalación, se abrirá el navegador web con la guía para configurar el módulo criptográfico en Firefox (también descrito en el apartado 3.2 Configuración).



En el caso de querer desinstalar el paquete:

Modo manual:

- Eliminar la carpeta `Libpkcs11-fnmtdnie`, ubicada en *Macintosh HD > Biblioteca*.

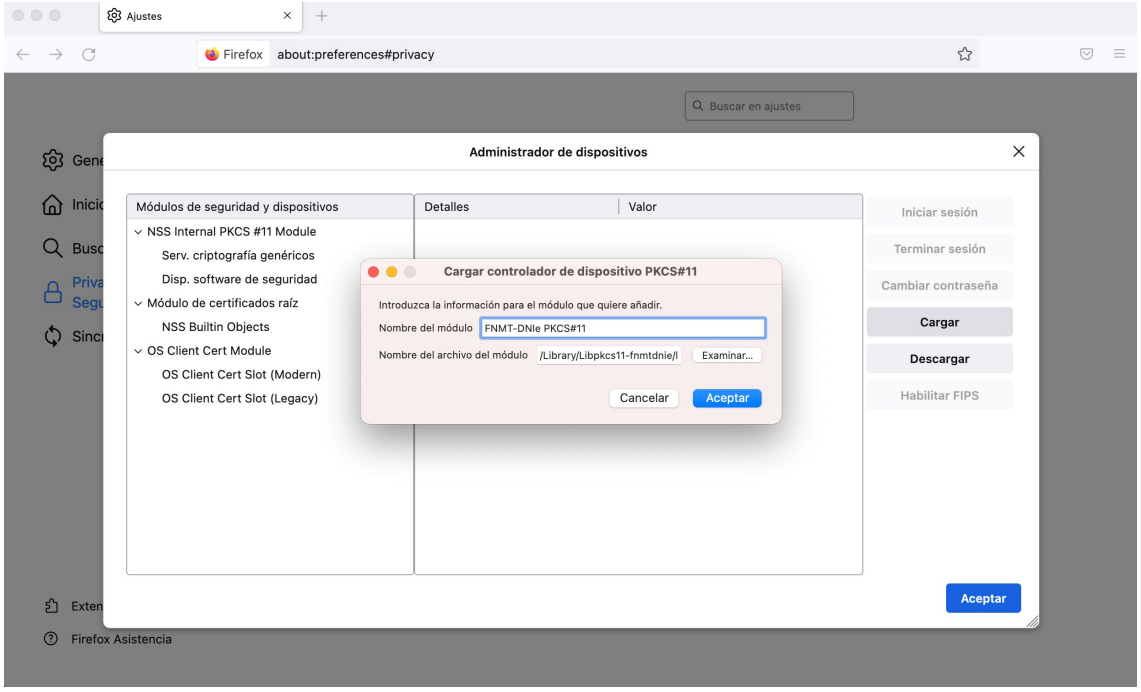
Modo automático:

- Ejecutar archivo *uninstall*.

3.2. Configuración

El navegador se configura del siguiente modo:

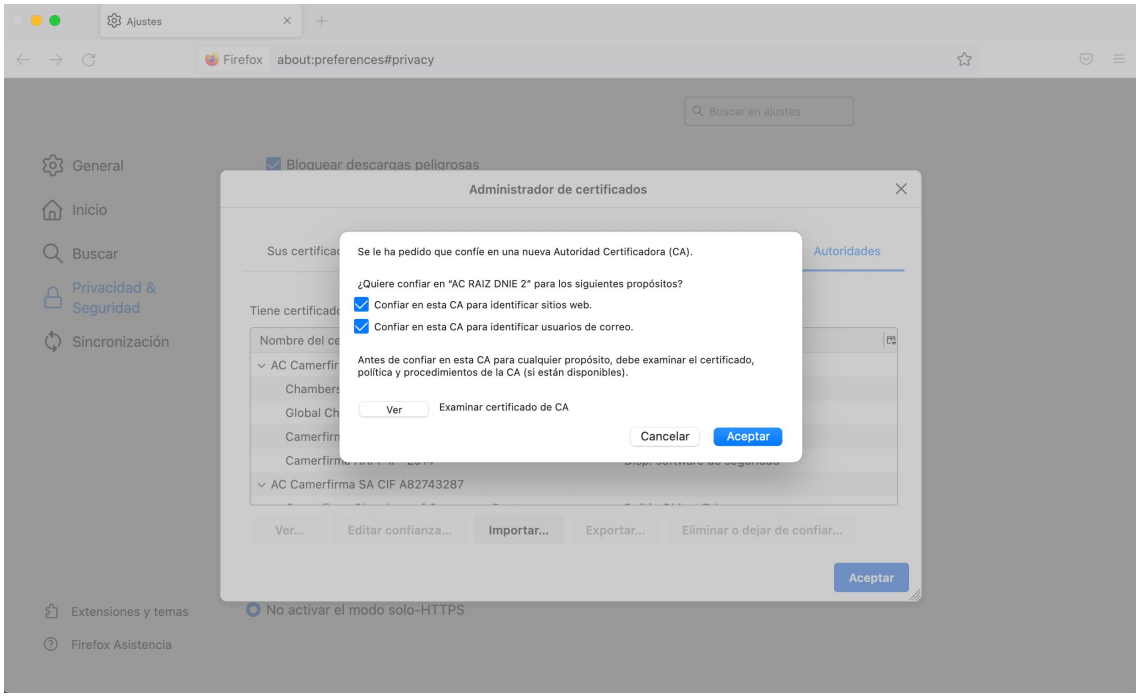
- Ir a *“Firefox > Preferencias (o Ajustes) > Privacidad y Seguridad > Dispositivos de seguridad”*.
- Seleccione *“Cargar”.*
- Asigne un nombre al módulo (por ejemplo "FNMT-DNIE Módulo P11").
- Indique manualmente la ruta del módulo: *Macintosh HD > Biblioteca > Libpkcs11-fnmtdnie > lib > libpkcs11-fnmtdnie.so*
- Pulse el botón "*Aceptar*"



Una vez instalado el módulo, se deberá importar el certificado raíz de la FNMT y del DNIe.

Para el certificado raíz de la FNMT:

- Ir a *“Firefox > Preferencias (o Ajustes) > Privacidad y Seguridad > Ver certificados”*.
- Seleccione "*Importar*"
- Indique manualmente la ruta del certificado raíz*: Macintosh HD > Biblioteca > Libpkcs11-fnmtdnie > ACRAIZFNMT-RCM.crt*
- El asistente le pedirá que establezca la confianza para el certificado.
- Marque todas las casillas de confianza.
- Pulse el botón "*Aceptar*"



Realizar los mismos pasos para el certificado raíz del DNIe. Este se encuentra ubicado en Macintosh HD > Biblioteca > Libpkcs11-fnmtdnie > ACRAIZDNIE-2.crt