Manual Instalación y Configuración de Multicard PKCS11

FNMT / DNIe

Versión 1.4b

Índice

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 16.04 LTS - Xenial Xerus
- GNU/Linux Ubuntu 15.10 Wily Werewolf
- GNU/Linux Fedora 24
- GNU/Linux Debian 8 Jessie
- GNU/Linux OpenSUSE 13.2
- Mac OS El Capitan 10.11
- Mac OS Yosemite 10.10
- Solaris 10 - Intel / SPARC

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_i386.deb`

Al finalizar, se abrirá el navegador web con la guía para configurar el módulo criptográfico en Firefox.

En el caso de querer desinstalar el paquete se debe usar una de las dos metodologías siguientes:

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 abrirá el navegador web con la guía para configurar el módulo criptográfico en Firefox

En el caso de querer desinstalar el paquete se debe usar una de las dos metodologías siguientes:

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 "*Preferencias* / *Privacidad y Seguridad* / *Certificados*" del navegador Firefox la opción "*Preguntar siempre*" referente a "Cuando un servidor requiera mi 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 "*Preferencias* / *Avanzado* / *Cifrado* / *Dispositivos de seguridad*" de Firerfox
- Seleccione "*Cargar"*
- Dele 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 deberá importar el certificado raíz de la FNMT y del DNIe.

- Ir a "*Preferencias* / *Priv. y Seguridad* / *Certificados* / *Ver certificados*" de Firefox
- Seleccione "*Importar*"
- Indique manualmente la ruta del certificado raíz: `/usr/share/libpkcs11-fnmtdnie/AC_Raiz_FNMT-RCM_SHA256.cer`
- El asistente le pedirá que establezca la confianza para el certificado.
- Marque las tres casillas de confianza.
- Pulse el botón "Aceptar"

Realizar los mismos pasos para importar el certificado raíz del DNIe. Este se encuentra ubicado en `/usr/share/libpkcs11-fnmtdnie/ac_raiz_dnie.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.

En el caso de querer desinstalar el paquete:

- Eliminar la carpeta `Libpkcs11-fnmtdnie`, ubicada en `/Library/Libpkcs11-fnmtdnie`.

3.2 Configuración

El navegador se configura del siguiente modo:

- Ir a "*Firefox* > *Preferencias* > *Priv. y Seguridad* > *Certificados* > *Dispositivos de seguridad*".
- Seleccione "*Cargar*".
- Dele un nombre al módulo (por ejemplo "FNMT-DNIE Módulo P11").
- Indique manualmente la ruta del módulo: `/Library/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* > *Priv. y Seguridad* > *Certificados* > *Ver certificados*".
- Seleccione "*Importar*"
- Indique manualmente la ruta del certificado raíz: `/Library/Libpkcs11-fnmtdnie/share/AC_Raiz_FNMT-RCM_SHA256.cer`
- El asistente le pedirá que establezca la confianza para el certificado.
- Marque las tres casillas de confianza.

- Pulse el botón "Aceptar"

Realizar los mismos pasos para el certificado raíz del DNIe. Este se encuentra ubicado en `/Library/Libpkcs11-fnmtdnie/share/ac_raiz_dnie.crt`

4 Instalación y configuración de sistemas Solaris 10

4.1 Instalación de las dependencias

Para el correcto funcionamiento de Multicard PKCS11 deberemos realizar unas tareas antes de poder instalar el paquete de la aplicación.

Eliminar los siguientes paquetes:

```
# pkgrm SUNWocfd
# pkgrm SUNWocfh
# pkgrm SUNWocfr
# pkgrm SUNWpcsclite
# pkgrm SUNWpcsclite-devel
```

Descargar las dependencias de la web ("http://www.sun-rays.org/add-ons/pcsclite/1.3/x86/")

- PCSC-lite_1.3_i386.zip
- SUNWusb-scrdr_i386.zip

Una vez descargados, descomprimirlos e instalarlos mediante los siguientes comandos (todo desde el mismo directorio):

```
# pkgadd -d . SUNWpcsc
# svcadm disable pcscd
# pkgadd -d . SUNWpcscdtu
# pkgadd -d . SUNWusb-scrdr
# svcadm enable pcscd
```

Para finalizar la instalación de dependencias, se deberá reiniciar el ordenador.

4.2 Instalación de Multicard PKCS11

Se deberá instalar

Arquitectura Intel:

- libpkcs11-fnmtdnie-x.x.x-SunOS-5.10-i386.pkg

Arquitectura SPARC:

- libpkcs11-fnmtdnie-x.x.x-SunOS-5.10-sparc.pkg

Para ello, se accede a un terminal y se ejecuta los siguientes comandos:

```
# pkgadd –d libpkcs11-fnmtdnie-x.x.x-SunOS-5.10-i386.pkg
```

Una vez instalado el paquete, deberá configurar el módulo criptográfico en su navegador Mozilla. (Descrito en el apartado 4.3 Configuración)

4.3 Configuración

El navegador Mozilla se configura del siguiente modo:

- Ir a "Edición > *Preferencias* > *Privacidad y Seguridad* > *Certificados* > *Administrar dispositivos de seguridad*".
- Seleccione "*Cargar*"
- Dele un nombre al módulo (por ejemplo "FNMT-DNIE Módulo P11").
- Indique manualmente la ruta del módulo: `/opt/FNMTpkcs11fnmtdnie/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 "*Edición* > *Preferencias* > *Privacidad y Seguridad* > *Certificados* > *Administrar certificados*" de Mozilla
- Seleccione "*Importar*"
- Indique manualmente la ruta del certificado raíz: `/opt/FNMTpkcs11fnmtdnie/share/AC_Raiz_FNMT-CM_SHA256.cer`
- El asistente le pedirá que establezca la confianza para el certificado.
- Marque las tres casillas de confianza.
- Pulse el botón "Aceptar"

Realizar los mismos pasos para el certificado raíz del DNIe. Este se encuentra ubicado en `/opt/FNMTpkcs11fnmtdnie/share/ac_raiz_dnie.crt`