INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

GUÍA DE INSTALACIÓN Y CONFIGURACIÓN DE OPENSC-DNIE

CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD (INTECO-CERT)

NOVIEMBRE 2007

ÍNDICE

1. INTRODUCCIÓN 3
1.1. Convenciones tipográficas utilizadas en este manual 3
2. INSTALACIÓN Y CONFIGURACIÓN SIN REPOSITORIO 4
2.1. GNU/Linux Ubuntu Breezy y Dapper 4
2.2. GNU/Linux Debian Sarge 5
2.3. GNU/Linux Fedora Core 5 6
2.4. Mac OS X 6
3. INSTALACIÓN Y CONFIGURACIÓN CON REPOSITORIO 8
3.1. GNU/Linux Ubuntu Breezy 8
3.2. GNU/Linux Debian Sarge 8
3.3. GNU/Linux Fedora Core 5 8
3.4. Mac OS X 8
4. CONFIGURACIÓN DEL PKCS#11 DEL DNI ELECTRÓNICO EN FIREFOX 9
4.1. GNU/Linux 9
4.2. Mac OS X 9

1. INTRODUCCIÓN

Manual de Instalación y Configuración de OpenSC-DNI-e

El objetivo de este breve manual es detallar los pasos nece sarios para instalar y configurar las librerías de OpenSC-DNIe en entornos UNIX.

En los siguientes apart ados se co menta cómo realizar el procedimiento de insta lación y configuración en cada una de las siguientes distribuciones:

- GNU/Linu x Debian Sarge
- GNU/Linu x Ubuntu Breezy
- GNU/Linu x Ubuntu Dapper
- Fedora Core 5
- y Mac OS X.

1.1. Convenciones tipográficas utilizadas en este manual

Cursiva

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

`Carácter Monoespaciado`

Se escribirán en caract eres monoespaciados a quellas pala bras que in diquen nombres de archivos, carpetas o una dirección url, como por ejemplo: **Setup.exe**.

2. INSTALACIÓN Y CONFIGURACIÓN SIN REPOSITORIO

En este punto se describe todos los pasos necesarios en caso de disponer los paquetes ya descargados en el equipo local.

2.1. GNU/Linux Ubuntu Breezy y Dapper

Se debe tener instalado previamente los paquetes siguientes: libc6, libltdl3, libopenct1, libssl0.9.7, zlib1g. Se puede solicitar que se instalen todos y el propio sistema sólo instalará aquellos paquetes que falten. Para la instalación se puede ejecutar en un terminal:

```
# aptitude update
# aptitude install libc6 libltdl3 libopenct1 libssl0.9.7 zlib1g
```

Una vez que ya están instalados estos paquetes se instalarán todos los paquetes de l OpenSC. Para la instalación se ejecuta en un terminal:

```
# cd <directorio_donde_tengamos_los_paquetes_del_OpenSC>
# dpkg -i libopensc2_0.11.1-svn1_i386.deb libopensc2-dev_0.11.1-svn1_i386.deb mozilla-opensc_0.11.1-svn1_i386.deb opensc_0.11.1-svn1_i386.deb
```

Para instalar el paquete OpenSC-DNIe, se debe comprobar también si está instalada la aplicación pinentry. Dependiendo de qué interfaz de ventanas se tenga configurada, Gnome o KDE, se instalará pinentry-gtk2 o pinentry-qt. Para la instalación se ejecuta en un terminal:

```
# aptitude install <nombre_paquete_pinentry>
```

Y a continuación, se instalará manualmente el paquete del OpenSC-DNIe. Para la instalación se ejecuta en un terminal:

```
# dpkg -i opensc-dnie_1.2.1-3_i386.deb
```

En este punto de la instalación se pide al usuario reiniciar para que se pueda configurar el navegador.

NOTA: en el caso de querer desinstalar los paquetes se debe usar el comando dpkg –r seguido del nombre del paquete.

2.2. GNU/Linux Debian Sarge

Se debe tener instalado previamente los paquetes siguientes: libc6, libltdl3, libopenct1, libssl0.9.7, zlib1g. Se puede solicitar que se instalen todos y el propio sistema sólo instalará aquellos paquetes que falten. Para la instalación se puede ejecutar en un terminal:

```
# aptitude update
# aptitude install libc6 libltdl3 libopenct1 libpcsclite1
libssl0.9.7 zlib1g
```

Una vez que ya están instalados estos paquetes se instalarán todos los paquetes de l OpenSC. Para la instalación se ejecuta en un terminal:

```
# cd <directorio_donde_tengamos_los_paquetes_del_OpenSC>
# dpkg -i libopensc2_0.11.1-svn1_i386.deb libopensc2-dev_0.11.1-
svn1_i386.deb mozilla-opensc_0.11.1-svn1_i386.deb opensc_0.11.1-
svn1_i386.deb
```

Para instalar el paquete OpenSC-DNIe, se debe comprobar también si está instalada la aplicación pinentry. Dependiendo de qué interfaz de ventanas se tenga configurada, Gnome o KDE, se instalará pinentry-gtk2 o pinentry-qt. Para la instalación se ejecuta en un terminal:

```
# aptitude install <nombre_paquete_pinentry>
```

Y a continuación, se instalará manualmente el paquete del OpenSC-DNIe. Para la instalación se ejecuta en un terminal:

```
# dpkg -i opensc-dnie_1.2.1-3_i386.deb
```

En este punto de la instalación se pide al usuario reiniciar para que se pueda configurar el navegador.

NOTA: en el caso de querer desinstalar los paquetes se debe usar el comando dpkg –r seguido del nombre del paquete.

2.3. GNU/Linux Fedora Core 5

Se debe tener instalado previamente los paquetes siguientes: libc6, libltdl3, libopenct1, libssl0.9.7, zlib1g. Se puede solicitar que se instalen todos y el propio sistema sólo instalará aquellos paquetes que falten. Para la instalación se puede ejecutar en un terminal:

```
# yum update
# yum install libc6 libltdl libopenct libpcsclite zlib
```

Una vez que ya están instalados estos paquetes se instalarán todos los paquetes del OpenSC. Para la instalación se ejecuta en un terminal:

```
# cd <directorio_donde_tengamos_los_paquetes_del_OpenSC>
# rpm -i mozilla-opensc-signer-0.11.1-1.i386.rpm opensc-devel-
0.11.1-1.i386.rpm opensc-0.11.1-1.i386.rpm
```

Para instalar el paquete OpenSC-DNIe, se debe comprobar también si está instalada la aplicación pinentry. Dependiendo de qué interfaz de ventanas se tenga configurada, Gnome o KDE, se instalará pinentry-gtk2 o pinentry-qt. Para la instalación se ejecuta en un terminal:

```
# yum install <nombre_paquete_pinentry>
```

Y a continuación, se instalará manualmente el paquete del OpenSC-DNIe. Para la instalación se ejecuta en un terminal:

```
# rpm -i opensc-dnie-1.2.1-3.i386.rpm
```

En este punto de la instalación se pide al usuario reiniciar para que se pueda configurar el navegador.

NOTA: en el caso de querer desinstalar los paquetes se debe usar el comando rpm -e seguido del nombre del paquete.

2.4. Mac OS X

Los pasos para poder utilizar la tarjeta del DNI electrónico en Mac OS X son los siguientes:

Descargar SCA (Smart Card for Apple Mac OS X), requiere Mac OS X 10.4.3 o superior. Se puede descargar de http://www.opensc-project.org/files/sca/experimental/sca-0.1.9pre7.dmg

- Para instalarlo, hacer doble click en el fichero para montar el volumen y doble click en el fichero generado dentro del paquete. Siguiendo el asistente de instalación, se instalará en el sistema.
- Para instalar OpenSC-DNIe, hacer doble click en el fichero **opensc.dnie-1.0.0.dmg**. De forma similar que antes, se montará el volumen y seguiendo el asistente de instalación para tenerlo instalado.

El paquete OpenSC-DNIe está compilado en Binario Universal, por lo que funciona tanto en las arquitecturas i386 como PPC de Apple.

NOTA: en el caso de querer desinstalar los paquetes se debe ejecutar como superusuario los ficheros /Library/OpenSC/bin/dnie-uninstall y /Library/OpenSC/bin/opensc-unistall.

3. INSTALACIÓN Y CONFIGURACIÓN CON REPOSITORIO

En este punto se describe todos los pasos necesarios en caso de disponer de un repositorio donde almacenar todos los paquetes. Si el repositorio está montado, se facilita la instalación al usuario y además se asegura que las actualizaciones de los paquetes se realicen automáticamente, ya que el sistema siempre comprueba si existen nuevas versiones de los paquetes en el repositorio.

3.1. GNU/Linux Ubuntu Breezy

Para instalar OpenSC-DNIe basta con ejecutar desde un terminal:

```
# aptitude update
# aptitude install opensc-dnie
```

3.2. GNU/Linux Debian Sarge

Para instalar OpenSC-DNIe basta con ejecutar desde un terminal:

```
# aptitude update
# aptitude install opensc-dnie
```

3.3. GNU/Linux Fedora Core 5

Para instalar OpenSC-DNIe basta con ejecutar desde un terminal:

```
# yum update
# yum install opensc-dnie
```

3.4. Mac OS X

Para este sistema operativo, los pasos a seguir son exactamente los mismos que en la sección 2.4.

4. CONFIGURACIÓN DEL PKCS#11 DEL DNI ELECTRÓNICO EN FIREFOX

La configuración del módulo PKCS#11 se hará de forma automática por el paquete OpenSC_DNIe. Se le pedirá al usuario que reinicie el ordenador para que en el proceso de arranque se configure el navegador. Esto es, se importará el certificado raíz y se configurará un nuevo módulo de seguridad.

A parte, se facilita al usuario el certificado raíz y un fichero de configuración para que él mismo pueda instalarlo en caso de necesidad (por instalación de nuevas versiones del navegador…). En este caso se describe a continuación el procedimiento a seguir para configurar el PKCS#11 del OpenSC que soporta la tarjeta del DNI electrónico en el navegador Firefox.

Para evitar comportamientos anómalos se recomienda marcar en la sección "Seguridad/Certificados/Selección del certificado del cliente" la opción "Preguntar siempre". De este modo cada vez que el navegador quiera usar un certificado le mostrará al usuario la lista de certificados disponibles y el usuario elegirá uno.

4.1. GNU/Linux

En todas las distribuciones de GNU/Linux el PKCS#11 se denomina **opensc-pkcs11.so** y está ubicado por defecto en **/usr/lib**. Entonces, en el navegador Firefox se debe especificar la ruta completa del PKCS#11 **/usr/lib/opensc-pkcs11.so** en el momento de añadir un nuevo módulo de seguridad. Esto se puede realizar arrastrando el fichero **/usr/share/opensc-dnie/instal-dni/instala_modulo.htm** sobre el navegador.

También es necesario importar en el navegador el certificado raíz de la DGP. Esto se puede realizar arrastrando el certificado raíz **/usr/share/opensc-dnie/ac_raiz_dnie.crt** sobre el navegador.

4.2. Mac OS X

En el caso del Mac OS X, el PKCS#11 se denomina también **opensc-pkcs11.so**, pero está ubicado en **/Library/OpenSC/lib**. Por lo que, la ruta completa a pasarle en el Firefox será **/Library/OpenSC/lib/opensc-pkcs11.so**. Esto se puede realizar arrastrando el fichero **/Librería/Opensc/Share/web/instala_modulo.htm** sobre el navegador.

También es necesario importar en el navegador el certificado raíz de la DGP. Esto se puede realizar pinchando en el link que aparece después de instalar el módulo.