DNI-e sobre GNU/Linux (Ubuntu 14.04 LTS / 16.04 LTS)

Información básica de:
http://www.ubuntu-guia.com/2014/04/instalar-dni-electronico-en-ubuntu.html[1]

1.1. Oracle Java

Para realizar trámites en línea, en la mayoría de las páginas web de la Administración será necesario tener instalado Oracle Java. Más información en:
http://www.ubuntu-guia.com/2012/04/instalar-oracle-java-7-en-ubuntu-1204.html[2]

Además, hay que estar pendiente de que el navegador no bloquee Java y darle permisos. Suele aparecer una barra en la parte superior del navegador, donde nos pedirá si deseamos que se ejecute Java.

1.2. Instalación del hardware (lector)

En mi caso he instalado el lector del ChipNet COMBI

La mayoría de los lectores de DNI-e funcionan en GNU/Linux con el driver CCID a través del servicio pcscd.

1.3. Instalación del controlador

Para Ubuntu y en general todas las derivadas de Debian, instalar los siguientes paquetes:

- **libccid**
  (biblioteca que proporciona una implementación PC/SC del controlador de IFD para lectores USB de tarjetas inteligentes, compatibles con el protocolo CCID. Este paquete es necesario para comunicarse con los lectores de tarjetas inteligentes a través de CCID
- **pcscd**
  (El demonio PC/SC se utiliza para asignar / cancelar dinámicamente los controladores del lector y administrar conexiones a los lectores.)

Desde la terminal sería:

```
sudo apt-get install libccid pcscd
```

1.4. Instalación de librerías o bibliotecas

Instalar las siguientes librerías o bibliotecas y paquetes complementarios:

- **pinentry-gtk2**
  (Programa que permite garantizar la entrada de PIN o frases de contraseña. Esto significa que trata de cuidar que la información introducida no se intercambie en el disco o se almacene temporalmente en cualquier lugar. Esta funcionalidad es especialmente útil para introducir frases de contraseña cuando se utiliza software de cifrado GnuPG o como clientes de correo electrónico utilizando el mismo. Utiliza un protocolo abierto y por lo tanto, no vinculado a determinados programas)
- **pcsc-tools**
  ("Gscriptor" contiene herramientas útiles para PC/SC, como pcsc_scan que analiza lectores de tarjetas inteligentes disponibles otras detectan los eventos como la inserción y extracción de la tarjeta con ATR ...)
- **libpcsclite1** y **libpcsclite-dev**
  (El propósito de PC/SC Lite es proporcionar una interfaz de tipo SCard de Windows(R) para comunicarse con tarjetas inteligentes y lectores)
- **libreadline6** y **libreadline-dev**
  (una biblioteca readline de GNU que ayuda en la consistencia de interfaces de usuario a través de programas discretos que necesitan proporcionar una interfaz en línea de órdenes)
- **coolkey**
  (Soporte de controladores de Linux para las tarjetas inteligentes CoolKey and Common Access Card (CAC) con claves de seguridad utilizadas en una Infraestructura de Clave Pública (PKI). El módulo de libpkcs11 permite el uso de tarjetas inteligentes en aplicaciones como Mozilla Network Security Services (NSS))

Instalación de todos estos paquetes desde la terminal:

```
sudo apt-get install pinentry-gtk2 pcsc-tools libpcsclite1 libpcsclite-dev
libreadline6 libreadline-dev coolkey
```

Llegados a este punto ya podemos probar si Ubuntu detecta el lector y puede leer el DNI-e, una vez conectado el lector usb e introducido el DNI-e.

Para ver si Ubuntu detecta el lector ejecuta en una terminal el siguiente comando:

```
lspci | grep 'USB\|SD\|Card'
```

La terminal nos responderá algo parecido a:

```
00:1a.0 USB controller: Intel Corporation 6 Series/C200 Series Chipset Family USB
Enhanced Host Controller #2 (rev 05)
00:1d.0 USB controller: Intel Corporation 6 Series/C200 Series Chipset Family USB
Enhanced Host Controller #1 (rev 05)
13:00.0 Unassigned class [ff00]: Realtek Semiconductor Co., Ltd. RTS5209 PCI
Express Card Reader (rev 01)
13:00.1 SD Host controller: Realtek Semiconductor Co., Ltd. RTS5209 PCI Express
Card Reader (rev 01)
19:00.0 USB controller: NEC Corporation uPD720200 USB 3.0 Host Controller (rev 04)
```

Aparecen varias entradas con Express Card Reader, que son las del lector de tarjetas qeu lleva también lector de DNI-e (el nombre del chip variará según sea vuestro lector)

Ahora vamos a ver si lee el DNI-e con el comando:

```
pcsc_scan
```

Con Ubuntu 14.04

La terminal nos devolverá algo parecido a:

```
PC/SC device scanner
V 1.4.22 (c) 2001-2011, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.8.10
Using reader plug'n play mechanism
Scanning present readers...
0: Generic USB2.0-CRW [Smart Card Reader Interface] (20070818000000000) 00 00

Wed May  6 20:30:36 2015
Reader 0: Generic USB2.0-CRW [Smart Card Reader Interface] (20070818000000000) 00
00
  Card state: Card removed,
```

Pongo el DNI-e y entonces mostrará algo como:

```
Wed May  6 20:31:25 2015
Reader 0: Generic USB2.0-CRW [Smart Card Reader Interface] (20070818000000000) 00
00
  Card state: Card inserted,
  ATR: 3B 7F 96 00 00 00 6A 44 4E 49 65 10 01 77 98 03 11 03 90 00

ATR: 3B 7F 96 00 00 00 6A 44 4E 49 65 10 01 77 98 03 11 03 90 00
+ TS = 3B --> Direct Convention
+ T0 = 7F, Y(1): 0111, K: 15 (historical bytes)
  TA(1) = 96 --> Fi=512, Di=32, 16 cycles/ETU
    250000 bits/s at 4 MHz, fMax for Fi = 5 MHz => 312500 bits/s
  TB(1) = 00 --> VPP is not electrically connected
  TC(1) = 00 --> Extra guard time: 0
+ Historical bytes: 00 6A 44 4E 49 65 10 01 77 98 03 11 03 90 00
  Category indicator byte: 00 (compact TLV data object)
    Tag: 6, len: A (pre-issuing data)
      Data: 44 4E 49 65 10 01 77 98 03 11
    Mandatory status indicator (3 last bytes)
      LCS (life card cycle): 03 (Initialisation state)
      SW: 9000 (Normal processing.)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
        NONE

find: «/home/xavi/.cache/smartcard_list.txt»: El fitxer o directori no existeix
Your card is not present in the database.
Please submit your unknown card at:
http://smartcard-atr.appspot.com/parse?ATR=3B7F9600...
```

Pulsamos la combinación de teclas CTRL+Z para detener el proceso y cerramos la terminal.

Nota: Si la terminal se queda pensando intentando leer el DNIe, puede ser necesario reiniciar el sistema con el lector conectado y el DNIe introducido.

Con Ubuntu 16.04

La terminal nos devolverá algo parecido a:



```
PC/SC device scanner
V 1.4.25 (c) 2001-2011, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.8.14
Using reader plug'n play mechanism
Scanning present readers...
0: Generic USB2.0-CRW [Smart Card Reader Interface] (20070818000000000) 00 00
```

```
Tue May 24 12:31:38 2016
Reader 0: Generic USB2.0-CRW [Smart Card Reader Interface] (20070818000000000) 00
00
  Card state: Card removed,
```

Pongo el DNI-e y entonces mostrará algo como:



```
Tue May 24 12:31:53 2016
Reader 0: Generic USB2.0-CRW [Smart Card Reader Interface] (20070818000000000) 00
00
  Card state: Card inserted,
  ATR: 3B 7F 96 00 00 00 6A 44 4E 49 65 10 01 77 98 03 11 03 90 00

ATR: 3B 7F 96 00 00 00 6A 44 4E 49 65 10 01 77 98 03 11 03 90 00
+ TS = 3B --> Direct Convention
+ T0 = 7F, Y(1): 0111, K: 15 (historical bytes)
  TA(1) = 96 --> Fi=512, Di=32, 16 cycles/ETU
    250000 bits/s at 4 MHz, fMax for Fi = 5 MHz => 312500 bits/s
  TB(1) = 00 --> VPP is not electrically connected
  TC(1) = 00 --> Extra guard time: 0
+ Historical bytes: 00 6A 44 4E 49 65 10 01 77 98 03 11 03 90 00
  Category indicator byte: 00 (compact TLV data object)
    Tag: 6, len: A (pre-issuing data)
      Data: 44 4E 49 65 10 01 77 98 03 11
    Mandatory status indicator (3 last bytes)
      LCS (life card cycle): 03 (Initialisation state)
      SW: 9000 (Normal processing.)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 7F  (un monton de numeros de dos crifras por aqui seguidas de espacios) 00
        DNI electronico (Spanish electronic ID card) (eID)
        http://www.dnielectronico.es
```

1.5. Instalación del software del DNI-e

1.5.1. Añadir Certificado y Validación de las Autoridades:

Lo primero que vamos a hacer es descargar los certificados del DNI-e para instalarlos en el navegador, uno para la autoridad de certificación y otro para la Autoridad de validación del DNIe. Para ello vamos a la siguienta página: http://www.dnielectronico.es/seccion_integradores/certs.html[3]

- Para la Autoridad de certificación (La Dirección General de la Policía (Ministerio del Interior) actúa como Autoridad de Certificación (AC)):
  Haz clic en el enlace: "**AC Raíz**"
  y descarga el archivo: "**pkcs1-sha256WithRSAEncryption**".
- Para la Autoridad de validación del DNIe (certificado que suministra información sobre la vigencia de los certificados electrónicos, que será el de la FMNT (Fábrica Nacional de Moneda y Timbre)):
  Haz clic en el enlace: “AV DNIE FNMT"
  y descarga el archivo: "pkcs1-sha256WithRSAEncryption".

Nota: En este último podréis ver que hay varias versiones con diferentes periodos de validez. Descargaremos el actual y si en un futuro nos falla puede ser debido a que tengamos que volver a descargar / instalar una nueva versión con la fecha de validez actualizada.

Una vez descargados, hacemos en cada uno respectivamente, clic derecho y seleccionamos "extraer aquí" y ya tendremos los certificados "ACRAIZ-SHA2.crt" (el archivo zip era ACRAIZ-SHA2.zip) y ~~"AVDNIEFNMTSHA2.cer"~~ "OCSP_VA_DNIE_FNMT_SHA2.cer" (el archivo zip era AVDNIEFNMTSHA2_new.zip).

1.5.2. Importar certificiados en Firefox

Abrimos Firefox e importamos los certificados:

Para la Autoridad de certificación vamos al menú: "**Editar > Preferencias > Avanzado > Cifrado > Ver certificados" y en la pestaña "Autoridades**", hacemos clic en "**Importar**" y seleccionamos el archivo descomprimido "**ACRAIZ-SHA2.crt**".

Se nos abrirá una ventana en la que debemos de marcar las 3 opciones de confianza (muy importante). Si lo hubieramos dejado en blanco se pueden volver a activar, pulsando en el certificado "AC RAIZ DNIE" y pulsando en (editar confianza ...):

Click to expand

Nos aseguramos de se ha importado buscando en la lista de certificados "DIRECCIÓN GENERAL DE LA POLICIA (AC RAIZ DNIE)":

Click to expand

Para la Autoridad de validación del DNIe en el mismo menú (**Editar > Preferencias > Avanzado > Cifrado > Ver certificados**), en la pestaña "**Servidores**", hacemos clic en "**Importar**" y seleccionamos el archivo descomprimido "**OCSP_VA_DNIE_FNMT_SHA2.cer**".

Nos aseguramos de se ha importado buscando en la lista de certificados "DIRECCIÓN GENERAL DE LA POLICIA (AC DNIE FNMT)":

Click to expand

1.5.3. Importar certificiados en Chrome/Chromium

Abrimos Chrome o Chromium-browser e importamos los certificados de forma análoga a como hicimos antes con Firefox.

Para la Autoridad de certificación vamos al menú: "**Configuración > Muestra la configuración avanzada (abajo de todo) > HTTPS/SSL > Gestiona los certificados > Entidades emisoras (pestaña) > Importa**" y seleccionamos el archivo descomprimido "**ACRAIZ-SHA2.crt**".

Click to expand

Luego hacemos algo parecido en la pestaña de "Servidores (pestaña) > Importa", y seleccionamos el archivo descomprimido "**OCSP_VA_DNIE_FNMT_SHA2.cer**":

Click to expand

Ahora, no veremos el certificado en esta pestaña, sino por alguna razon desconocida, lo muestra en la pestaña "Otros":

Click to expand

Y ya está.

1.6. Info extra

No confirmado, pero según la web del dnielectronico, hay que instalar este sobreware del PKCS#11-dnie

http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1112[4]

```
Instalación del DNI Electrónico

Para usar el DNI electrónico se requiere:

    Instalar el Módulo de Seguridad PKCS#11

    Para instalar el módulo PCKS#11 debe ir a
Editar/Preferencias/Avanzado/Cifrado/Dispositivos de seguridad

    Seleccione "Cargar"

    Dele un nombre al módulo. (Por ejemplo "DNIe Modulo PKCS # 11")
```

```
    Indique manualmente la ruta del módulo: /usr/lib/libpkcs11-dnie.so

    Pulse el botón "Aceptar"

    Instalar el Certificado Raíz de la Autoridad de Certificación del DNIe

    Para instalar el certificado raíz ir a Editar/Preferencias/Avanzado/Cifrado/Ver
certificados

    Seleccione "Importar".

    Indique manualmente la ruta del certificado raíz: /usr/share/libpkcs11-
dnie/ac_raiz_dnie.crt

    El asistente le pedirá que establezca la confianza para el certificado.

    Marque las tres casillas de confianza.

    Pulse el botón "Aceptar"
```

1.7. Veure també la documentació per a Linkat 14.04/16.04

https://docs.google.com/document/d/1o7YCMn8c2r_fF5iCqnU6JcxFbFjjkNMRMy0u5tADd3s/edit[5]

Nombres alias de esta página: DNIe | DNI

---

[1] http://www.ubuntu-guia.com/2014/04/instalar-dni-electronico-en-ubuntu.html

[2] http://www.ubuntu-guia.com/2012/04/instalar-oracle-java-7-en-ubuntu-1204.html

[3] http://www.dnielectronico.es/seccion_integradores/certs.html

[4] http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1112

[5] https://docs.google.com/document/d/1o7YCMn8c2r_fF5iCqnU6JcxFbFjjkNMRMy0u5tADd3s/edit