Índice de contenido

Este es el documento de primeros pasos para la versión **2** de la máquina virtual Linux para la Administración Electrónica.

> Para instalar software y otras tareas, el usuario de la máquina virtual es **ciudadano** y la contraseña **ciudadano** ***(aunque recomendamos cambiarla inmediatamente)***.

Pasar a pantalla completa

Ahora que has iniciado esta máquina virtual para Administración Electrónica es **muy recomendable** que pases a pantalla completa la ventana de Virtual Box. Para ello puedes pulsar **Ctrl derecho + F** o bien ir al menú de la ventana de Virtual Box y seleccionar **Ver > Cambiar a pantalla completa**.

Cambiar la resolución de pantalla

He dejado la resolución en 1024x768 para que sea visible desde la mayoría de las pantallas, sin embargo es probable que tengas un monitor que admita más. Se puede modificar en **Inicio > Preferencias > Ajustes del monitor**.

Compartiendo un pendrive o disco duro USB

Para acceder a archivos que necesites (como el certificado FNMT) o para guardar archivos que vayas generando en tu vida administrativa electrónica puedes hacer que un pendrive que tengas conectado a tu ordenador se vea desde la máquina virtual. Es muy recomendable que el certificado **.p12** que vas a instalar más adelante esté en este pendrive.

Para ello conecta normalmente el pendrive. Luego ve a la parte superior de la pantalla a **Dispositivos > Dispositivos USB** y allí encontrarás tu pendrive (o disco duro externo, es indiferente). Pulsa sobre él. A partir de este momento se montará en la máquina virtual (aparecerá un diálogo en la máquina virtual pidiendote si quieres ver el contenido). Si el pendrive o disco duro

no es visible, se puede arreglar pero depende de tu plataforma base (windows, linux, etc.). Una búsqueda por “virtualbox usb *<tu sistema operativo>*” te podría ayudar.

Pasos preliminares

Una serie de pasos orientados a mejorar la seguridad. El primero es prácticamente obligatorio, cambiar la contraseña por una segura. Los siguientes están orientados a tener un entorno muy seguro de navegación, aunque no están activados por defecto para no interferir en el funcionamiento general. Aun así, los pasos que indico a continuación (yo personalmente lo tengo configurado así) funciona bien hasta donde he podido probar.

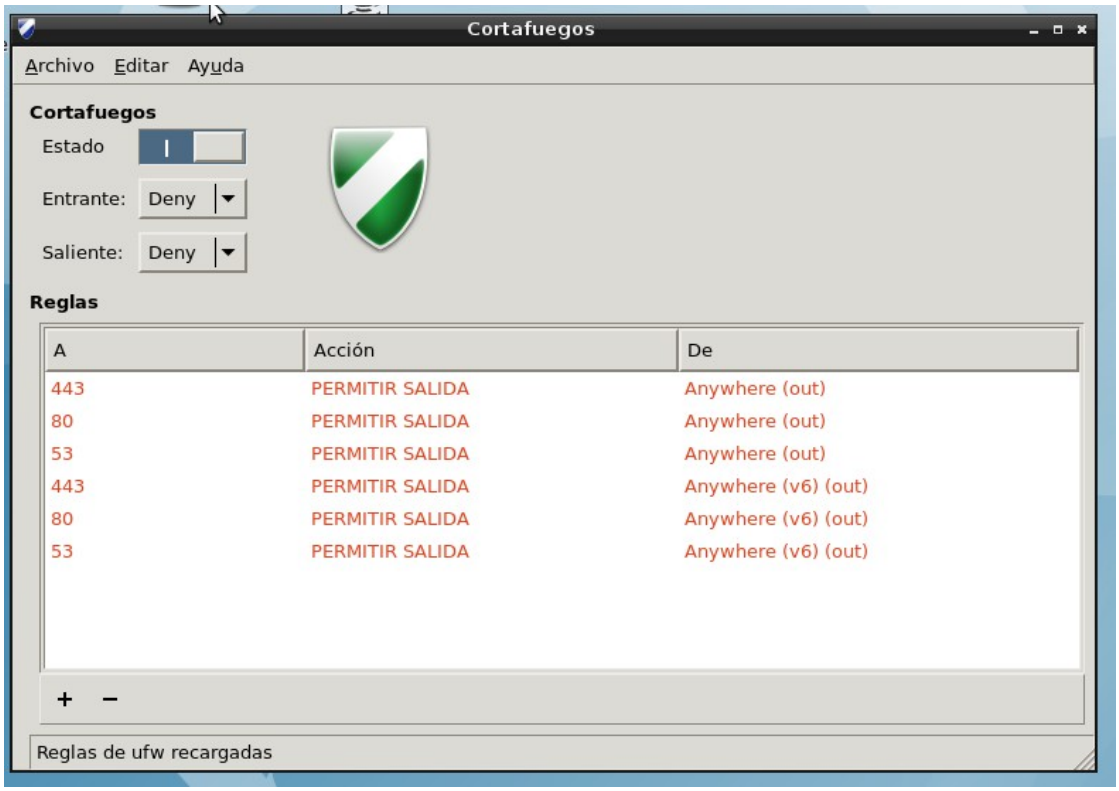
> Podrías saltarte la mayoría de esta sección e ir directamente a [Instalación de los certificados], lo que sí se recomienda es **al menos cambiar la contraseña del usuario ciudadano**.

Cambio de la contraseña

Para ello podemos ir a **Inicio > Accesorios > LxTerminal** y teclear **passwd**. Seguiremos el proceso de cambio de contraseña.

Firewall

El firewall está configurado para denegar todas las conexiones entrantes y permitir todas las conexiones salientes. Esto está bien para evitar intrusiones en la máquina.



Captura 1: Configuración final de reglas del firewall

Pero lo más seguro es habilitar solo el tráfico saliente -iniciado por ti- que realmente se necesita y evitar todo lo demás.

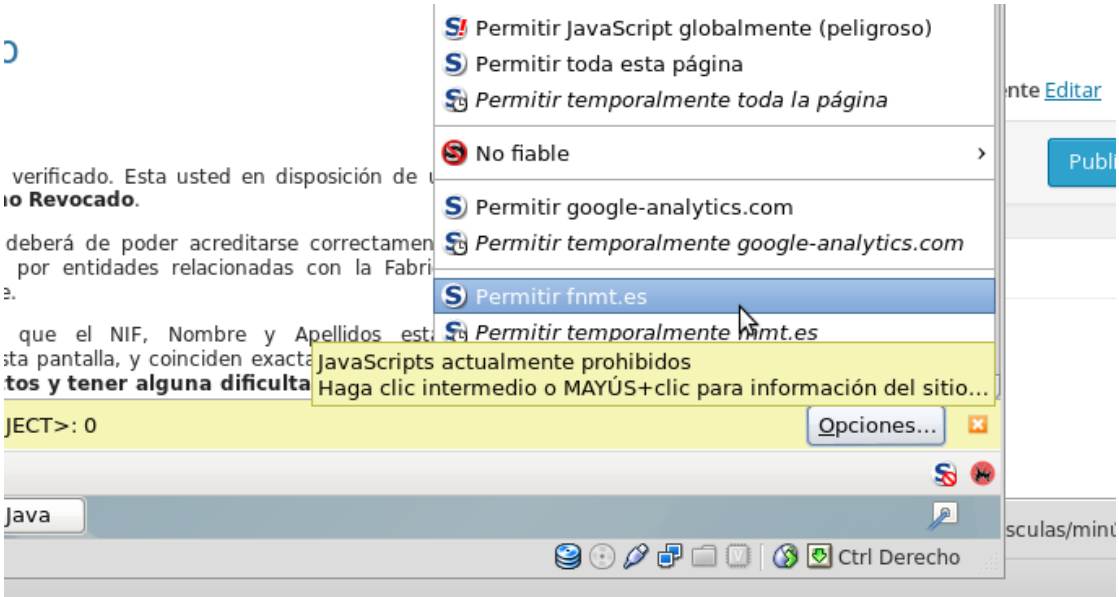
Si quieres activar el modo paranoico, puedes permitir solo las conexiones salientes hacia los puertos 80 -http-, 443 -https- y 53 -DNS- que es lo que yo pienso hacer. Debes hacer doble clic en el icono **Firewall** del escritorio. Introduce la contraseña del usuario ciudadano -espero que la hayas cambiado ya- y luego pulsaremos en **Desbloquear**. Pondremos el valor de **Saliente** a **Deny** (denegar). Ahora crearemos las reglas para permitir únicamente las conexiones hacia los puertos 80, 443 y 53.

Vamos a **Archivo > Añadir Regla**, elegiremos **Simple** y seleccionamos los valores **Allow, Out, Both** y como puerto ponemos el 80. Pulsamos **Añadir**. Repetimos la acción para el 443 (podemos simplemente borrar el 80, poner 443 y darle otra vez a **Añadir**). Volvemos a repetirla para el puerto 53, que es el DNS. En el futuro, si quisiéramos instalar un cliente de correo o de chat deberíamos añadir aquí los puertos correspondientes. Le damos a **Cerrar**, pulsamos **F5** para recargar reglas y ya podemos cerrar esta ventana, que el firewall seguirá a lo suyo. La cosa debería quedar como en la [Captura 1].

Configuración de NoScript

JavaScript -esos pequeños programas que hacen cosas dinámicas en las páginas- se ha convertido en un medio de ataque muy utilizado. Lo que hace **NoScript** es evitar la ejecución de TODO el código JavaScript. Es evidente que muchos sitios no funcionarán. Por defecto viene desactivada tal extensión pero los/as atrevido/as seguro que querrán habilitarla haciendo **Firefox > Complementos > Extensiones > NoScript > Activar**.

La idea es que se puede definir una lista blanca de sitios que sí tienen permitido ejecutar JavaScript, sitios en los que confías, mientras evitas que se ejecute en todos los que no están en la lista blanca. La lista blanca admite sitios concretos (como **administracionelectronica.gob.es**) pero también patrones (como **gob.es**). Yo tengo añadidos **gob.es**, **060.es** y **redara.es** y así todas las páginas cuyo dominio termine en esos valores, funcionarán bien.



Captura 2: Configuración de NoScript para un sitio web

Pero a veces incluso estas páginas -las que están en lista blanca- pueden dar una advertencia. Eso pasa cuando las páginas traen JavaScript desde sitios diferentes. El ejemplo típico es código de Google Analytics. Por ejemplo la página que tengo puesta como página de inicio, **masdestacados.060.es**, veréis que trae código de Google Analytics. A nosotros eso no nos aporta nada, así que en vuestra mano está si queréis permitirlo o no. Comprobaréis que **masdestacados.060.es** funciona perfectamente sin Google Analytics.

La [Captura 2] muestra el procedimiento para admitir una página en concreto. El menú sale haciendo clic en el icono que tiene una **S** abajo a la derecha en Firefox.

Instalación de los certificados

Estos son los pasos más importantes, instalar el certificado tanto en el navegador como en la máquina virtual de Java.

Certificado FNMT

Vamos a instalar el certificado de la FNMT. El paso más importante es el de Firefox pero algunas webs necesitan que esté también directamente en la máquina virtual de Java.

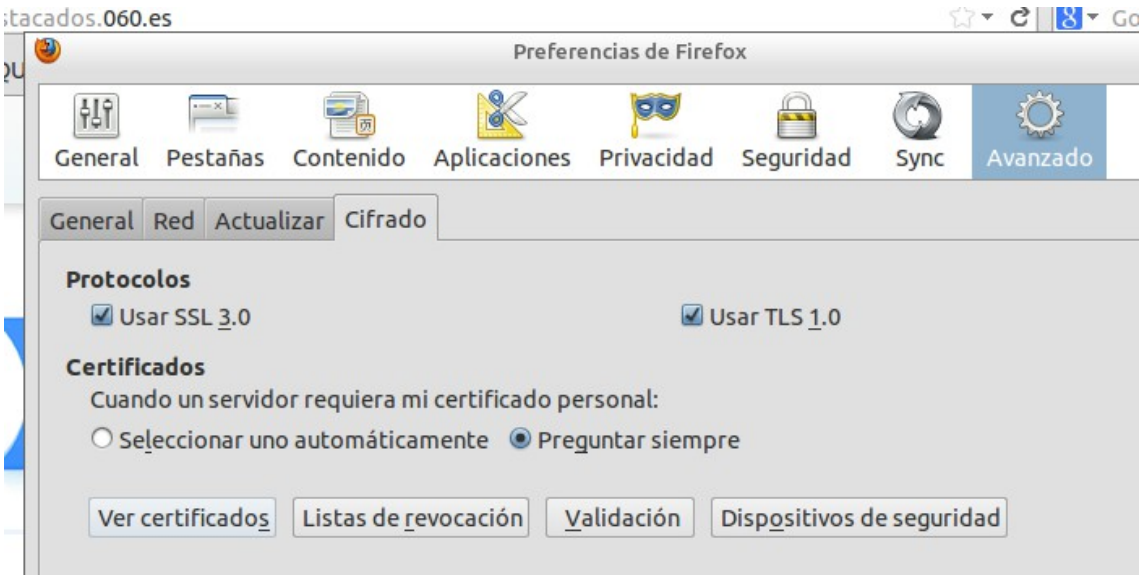
Firefox

Contamos con que tienes al menos un certificado digital de la Fábrica Nacional de Moneda y Timbre (FNMT) que sirve para identificarse y firmar la mayoría de las operaciones de Administración Electrónica. Si no cuentas con uno, ve a la [Dirección 1] para obtenerlo.

https://www.sede.fnmt.gob.es/certificados/persona-fisica
Dirección 1: Obtención del certificado FNMT

Si ya lo tienes instalado en el navegador de tu ordenador debes proceder a exportarlo a un archivo **.p12** que cuente con las claves pública y privada. Esta operación depende del navegador que estés utilizando, Google es tu amigo: “exportar certificado fnmt p12 *<navegador que utilices>*”.

Abre Firefox y ve a **Firefox** (arriba del todo a la izquierda) **> Preferencias > Preferencias**. Ve a la pestaña **Avanzado >** subpestaña **Cifrado** y pulsa el botón **Ver Certificados** [Captura 3].



Captura 3: Abrir el menú de preferencias

Ve a la pestaña **Sus certificados** y luego, un poco más abajo, pulsa el botón **Importar**. Ahora busca el archivo **.p12** que contiene el certificado. Te pedirá la contraseña con la que se exportó.

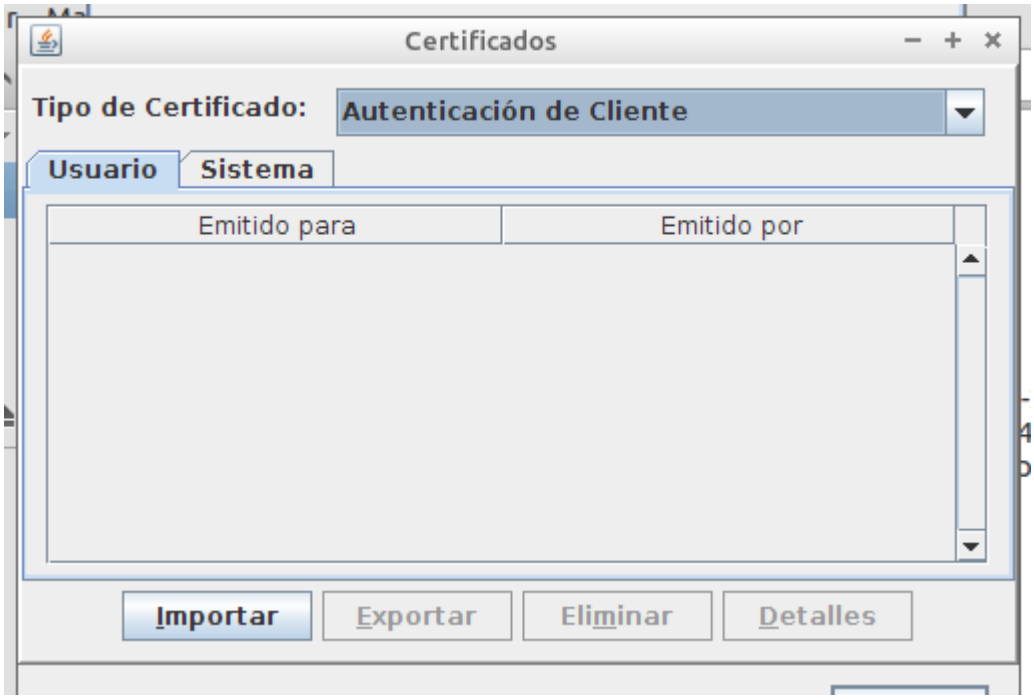
Java

***Importante**: Este paso es esencial si queremos que funcione la Dirección Electrónica Habilitada, para recibir notificaciones electrónicas de varios organismos.*

En el escritorio abre **Java 1.7.0_07**. Una vez abierto ve a la pestaña **Seguridad** y pulsa el botón **Certificados...** [Captura 4]

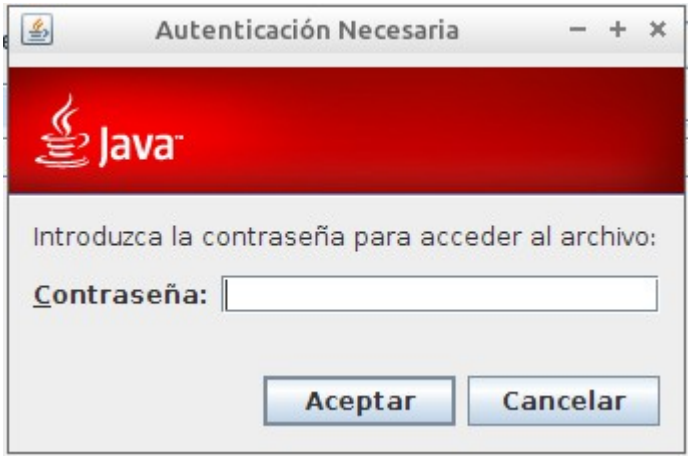
Captura 4: Abrir el menú Certificados en Java

Hay que añadir el certificado seleccionando previamente **Autenticación de Cliente** en Tipo de Certificado. Primero se selecciona en el desplegable el tipo de certificado y luego se pulsa el botón **Importar** y se busca tal y como lo hicimos con Firefox [Captura 5].



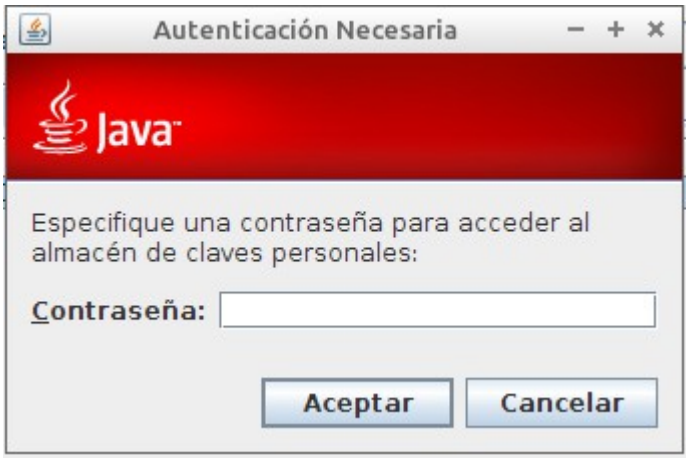
Captura 5: Importando certificado en Java (Autenticación)

Llegados a este punto **nos van a pedir dos contraseñas**. La primera es la que sirve para abrir el archivo .p12 que contiene el certificado, el archivo que habíamos exportado desde nuestro navegador. La segunda es una **contraseña nueva** que usará Java para el acceso al almacén de certificados. **Aquí lo más práctico es ponerla igual que la contraseña del archivo .p12** y así no habrá confusiones.



Captura 6: En este paso introducimos la contraseña de acceso al archivo .p12 del certificado

Remarco que en el paso siguiente es importante -no obligatorio- especificar la misma contraseña de antes para que no haya confusiones posteriormente. **Recuerda que esta segunda contraseña será la que se te pedirá para firmar con el certificado, no la olvides**.

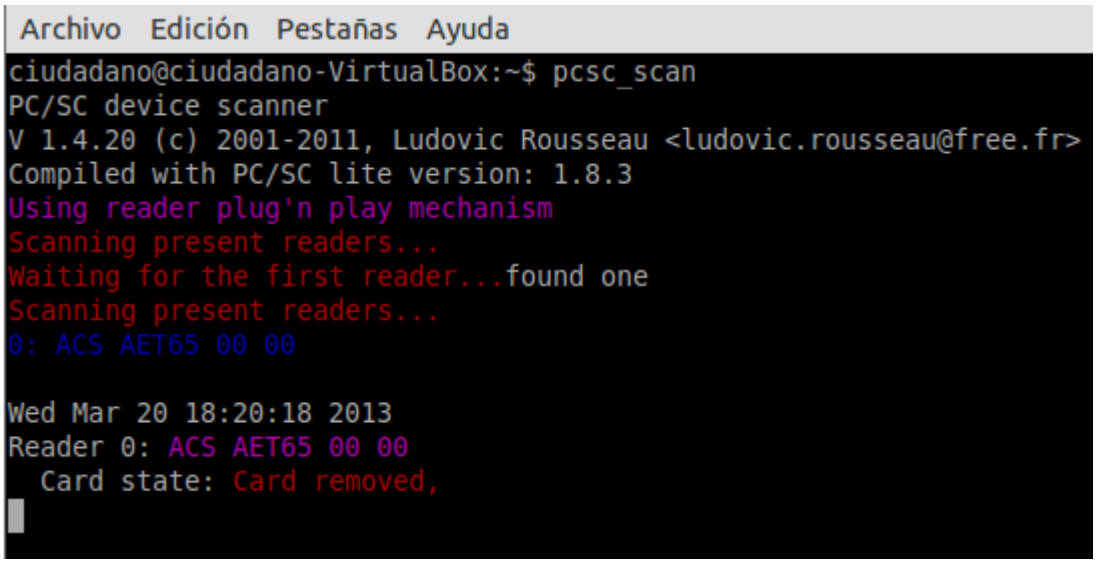


Captura 7: En este paso creamos la contraseña para el almacén de certificados

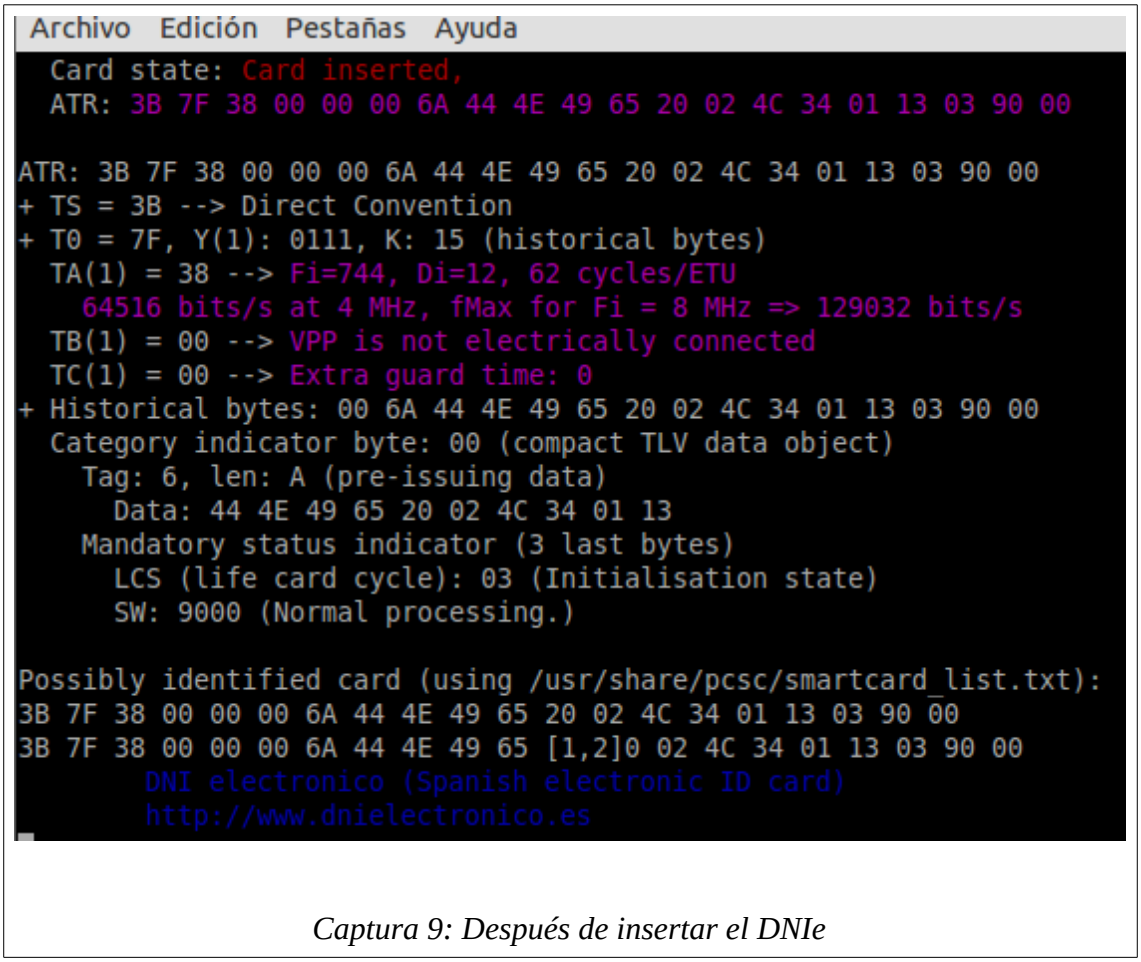
DNI electrónico

Lo importante en este paso es encontrar un lector que funcione en Linux. Es indiferente que funcione o no en el sistema que empleamos de anfitrión -el sistema de nuestro PC; donde instalamos Virtual Box- porque le “pasaremos” el lector a la máquina virtual. El procedimiento será igual que cuando le “pasamos” un pendrive a la máquina virtual. Vamos a la parte superior de la pantalla a **Dispositivos** > **Dispositivos USB** y allí seleccionamos nuestro lector (debe estar conectado en el PC previamente).

Para que la máquina virtual pueda tomar el control del lector no es igual si tu ordenador tiene un Windows, un MacOS o un Linux. En linux con conectarlo y pasárselo basta, pero probando con un anfitrión Windows XP he comprobado que es más recomendable terminar el proceso de instalar los drivers y todo lo que te pida el asistente y luego pasárselo. En MacOS no he probado.



Captura 8: Antes de insertar el DNIe



Captura 9: Después de insertar el DNIe

Algunos lectores que funcionan bien con Linux son:

- bit4id miniLector (www.bit4id.com)
- C3PO LTC31 (https://www.c3po.es)

Si el lector funciona bien con Linux normalmente no habrá que hacer nada más que “pasárselo a la máquina virtual”. Para comprobar su correcto funcionamiento abrimos una consola en la máquina virtual (**Inicio** > **Accesorios** > **LXTerminal**) y escribimos `pcsc_scan` [Captura 8].

Si salen los mensajes parecidos a los de la [Captura 8] entonces el lector funciona correctamente. Ahora es cuando **cerramos Firefox si lo teníamos abierto y luego insertamos el DNIe en el lector**. Cerramos Firefox porque solo detectaría el DNIe si está ya insertado cuando se abre. Si el DNIe está correcto la ventana anterior debería transformarse en la [Captura 9].

Importante*: no hace falta hacer esto de pcsc_scan siempre que vayamos a utilizar el DNIe. Solo lo hacemos la primera vez para comprobar si funciona bien el lector. Luego solo será introducir el DNIe y abrir Firefox.*

Vemos que ha identificado la tarjeta insertada como `DNI electrónico (Spanish electronic ID card)`. Ahora abrimos Firefox y vamos a la [Dirección 2].

http://www.dnielectronico.es/como_utilizar_el_dnie/verificar.html

Dirección 2: Página de verificación del DNIe

En esa página vamos hacia abajo del todo y pulsamos el enlace **Comprobación de certificados**. Si todo ha ido bien debería pedirnos la contraseña (PIN) que nos dieron cuando nos hicimos el DNIe (y que deberíamos haber cambiado ya por una que recordemos). Si introducimos la contraseña correctamente saldrá una página informativa con nuestros datos y con información sobre los certificados contenidos en el DNIe.

Más abajo podemos probar a realizar una operación de firma electrónica con nuestro DNIe. Introducimos cualquier texto y pulsamos en firmar. Nos pedirá de nuevo una contraseña (que será el mismo PIN que antes) y pulsaremos en Aceptar cuando nos pregunte si deseamos permitir la operación de firma.

Hay una diferencia importante, entre firmar con el certificado FNMT y firmar con el DNIe, en cuanto a la contraseña que te pide para firmar. Con el DNIe será el PIN mientras que con el certificado FNMT **normalmente esta clave se dejará en blanco**. Solo habrá que poner clave si hemos protegido el certificado FNMT en Firefox con una contraseña maestra, que por defecto, no es el caso. Así que normalmente irá en blanco.

Resolución de problemas

Problemas que pueden surgir ocasionalmente y como tratarlos.

Habilitar USB virtualizando sobre Linux

Cuando el sistema anfitrión (el original de nuestro equipo) es GNU/Linux es posible que la máquina virtual no reconozca los dispositivos USB conectados al sistema. Llegados a este punto tenemos un par de alternativas:

- *Acceder al certificado de cualquier otra manera*. Lo más práctico es auto-enviartelo por

correo electrónico. Cuando te lo envies, abre el navegador en la máquina virtual, accede a tu correo por la interfaz web y descárgalo. Después, es conveniente no tenerlo en tu correo, borrando el mensaje.
También puedes poner el certificado en un servidor al que solo tú tengas acceso y descargarlo luego desde la máquina virtual.

- Habilitando USB
- Habilitando carpetas compartidas.

Terminar sesión con DNIe

Si por cualquier motivo, con el DNIe insertado y el lector funcionando bien (comprobado con `pcsc_scan`) vemos que Firefox no detecta el certificado podemos probar a cerrar la sesión de la comunicación de Firefox con el DNIe. Vamos a **Firefox** > **Preferencias** > **Preferencias >** **Avanzado** > **Cifrado** > botón **Dispositivos de Seguridad** y nos situamos sobre **DNI Electrónico (PIN1)**. A la derecha pulsaremos el botón **Terminar sesión**.

Captura 10: Terminar sesión de Firefox con DNIe

Seguidamente cerramos Firefox, sacamos el DNIe, lo volvemos a introducir y volvemos a abrir Firefox.

***Importante**: esto solo lo hacemos cuando tengamos problemas, no cada vez que terminemos de usar el DNIe.*

Firefox no arranca

Algunas veces cuando está insertado y funcionando el DNIe en el lector, se bloquea Firefox al arrancar. En estos casos lo mejor es reiniciar la máquina por completo y volver a intentarlo.