



MANUAL DE USUARIO

DNIERemote v1.3.28



15 de septiembre de 2020

DNIEREMOTE v1.3.28

Versión	Fecha	Autores	Descripción
1.0	11.12.2018	CNP- FNMT	Creado.
1.1	20.03.2019	CNP- FNMT	Correcciones y ampliación de funcionalidad.
1.2	24.05.2019	CNP- FNMT	Ampliación de funcionalidad.
1.2.25	27.06.2019	CNP- FNMT	Corrección de errores y ampliación de funcionalidad.
1.3.26	05.03.2020	CNP- FNMT	Corrección de errores y ampliación de funcionalidad.
1.3.28	14.09.2020	CNP- FNMT	Corrección de errores y mejora de la funcionalidad.

Índice

1. Introducción	5
2. Componentes	5
3. Requisitos técnicos	6
3.1. Software	6
3.2. Hardware	6
3.3. Conectividad	6
4. Instalación	6
4.1. Windows	7
4.2. Linux	7
4.3. Android	8
5. Uso	8
5.1. Vinculación con el DNIE	9
5.2. Integración con Mozilla Firefox	19
5.3. Integración con Autofirm@	22
6. Preguntas frecuentes (FAQ)	24

Índice de figuras

1.	Reverso DNIE v3.0	5
2.	Paquete de instalación Windows.	7
3.	Accesos a la aplicación.	8
4.	Android App: DNIE conectado.	9
5.	Acceso directo.	10
6.	Asistente de conexión: Introducción.	10
7.	Asistente de conexión: Pasos previos.	11
8.	Asistente de conexión: Información de uso.	12
9.	Android: Inicio de aplicación.	13
10.	Windows. Asistente: Fase de activación.	14
11.	Windows. Asistente: Medios de vinculación.	14
12.	Linux. Asistente: Medio de vinculación.	15
13.	Android: Medios de vinculación.	15
14.	Asistente de conexión: Fase de lectura.	16
15.	Android App: Lectura de certificados.	17
16.	Asistente de conexión: Resultado.	18
17.	Opciones en Firefox.	19
18.	Privacidad y seguridad en Firefox.	19
19.	Nuevo dispositivo	20
20.	Carga del módulo PKCS#11	20
21.	Dispositivo creado	21

3. Requisitos técnicos

Para que la aplicación funcione correctamente, el entorno donde se despliega debe cumplir con unos mínimos, indicados a continuación.

3.1. Software

Windows: versiones 7, 8, 8.1 y 10. Los navegadores web compatibles son *Microsoft Edge* (basado en Chromium), *Internet Explorer*, *Google Chrome*, *Opera* y *Mozilla Firefox* (ver 5.2).

Linux: distribuciones Debian y Ubuntu. El navegador web compatible es *Mozilla Firefox* (ver 5.2).

Android: a partir de la versión 5.1 o *Lollipop*.

3.2. Hardware

Dispositivo móvil con tecnología NFC, cable USB para conectar a PC/-portátil (sólo en Windows), capacidad para conectarse a redes Wi-Fi[®], y captura de imágenes con cámara trasera.

3.3. Conectividad

En caso de vinculación por Wi-Fi, ambos dispositivos (PC y móvil) deben estar conectados a la misma red para obtener visibilidad entre ellos. Dado que la comunicación entre ambos se realiza a través de un canal seguro, no es relevante si la red es pública o privada.

4. Instalación

Los dos módulos que componen la aplicación se pueden descargar de Internet a través de los medios oficiales y reconocidos que se indican a continuación. La obtención de éstos a través de otros canales no garantiza un buen funcionamiento y por tanto el proveedor no se hace responsable de las consecuencias derivadas de su uso.

4.1. Windows

La aplicación de escritorio para Windows DNIERemote v1.3.28 se puede obtener directamente a través de la propia aplicación Android, en la opción del menú principal '**Software para PC**', o accediendo portal del [DNI electrónico](#) en el área de descargas.

Se instala mediante un paquete con extensión *.msi* (Microsoft Installer) sin dependencias y para entornos de 32 y 64 bits (fig. 2), lanzando un proceso guiado con formato de asistente. Debido a la necesidad de incorporar componentes a nivel de sistema, el asistente solicitará la elevación de privilegios de administrador en algún momento del proceso, si el usuario no tuviera asignado ya los permisos. Una vez finalice la instalación se añade un acceso directo a la aplicación en el escritorio del usuario.

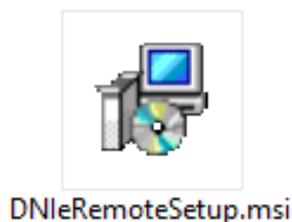


Figura 2: Paquete de instalación Windows.

Desinstalación: A través de la herramienta de Windows *Programas y Características* ubicado en la sección *Panel de Control*, se puede desinstalar la aplicación DNIERemote.

Actualización: En caso de tener ya instalada una versión anterior, el nuevo instalable realiza un proceso de actualización. Durante ésta, si advierte de ciertos procesos que no se pueden actualizar hasta que se reinicie el equipo, simplemente continúe con el proceso y siga las instrucciones. El software queda totalmente actualizado una vez se reinicie el equipo.

4.2. Linux

La aplicación de escritorio para Linux DNIERemote v1.3.28 se puede obtener directamente a través de la aplicación Android, en la opción del menú principal '**Software para PC**', o accediendo portal del [DNI electrónico](#) en el área de descargas.

Se instala manualmente con el comando *dpkg -i* un paquete con extensión *.deb*, para entornos de 32 y 64 bits. Para su instalación se requieren privilegios de administrador o *root*, por lo que es necesario emplear el comando *su* o *sudo* según corresponda. Se muestra un ejemplo a continuación.

```
john@debian:~$ su -  
root@debian:~# dpkg -i DNIeRemoteSetup_1.0-2_amd64.deb
```

Problemas de dependencias: Es posible que en la instalación se advierta de un problema de dependencias. Una solución es la ejecución de la siguiente sentencia:

```
root@debian:~# apt --fix-broken install
```

Una vez finalice la instalación se añade un acceso directo a la aplicación en el listado de aplicaciones disponibles. También se puede localizar la aplicación en el directorio `/usr/bin/`.

Desinstalación: A través del comando `dpkg -r DNIeRemoteSetup` se puede desinstalar la aplicación DNIeRemote.

4.3. Android

Esta App para sistemas operativos Android se obtiene a través de [Google Play](#). Se localiza con el nombre `DNIeSmartConnect` vinculada al desarrollador **CNP-FNMT**.

Una vez instalada la App, se puede iniciar bien por el icono (fig. 3a) o añadiendo opcionalmente el *widget* (ver [2]) (fig. 3b) al escritorio de su dispositivo móvil. Éste le proporciona información de estado de la conexión, y acceso directo a la configuración.



(a) Icono



(b) Widget

Figura 3: Accesos a la aplicación.

5. Uso

El objetivo de esta aplicación es que los certificados del DNIe 3.0 estén disponibles en la sesión de Windows/Linux del usuario para que las aplicaciones puedan hacer uso de éstos.

A continuación se describe con detalle el proceso de carga y vinculación del DNIE con los sistemas operativos Windows/Linux a través de la aplicación de escritorio y la App de Android.

Por último, se explica cómo se realiza la integración en el navegador web Mozilla Firefox para usar los certificados con el DNIE 3.0 a través de la aplicación DNIERemote.

Importante: para que se pueda utilizar el DNIE para procesos de autenticación y firma digital, es necesario que la App DNISmartConnect **permanezca en funcionamiento y con el DNIE conectado** (fig. 4).



Figura 4: Android App: DNIE conectado.

5.1. Vinculación con el DNIE

Para acceder a los certificados digitales del DNIE 3.0 en el PC es necesario completar la conexión de éste con el dispositivo móvil a través del asistente de conexión o *DNIERemoteWizard*. Para ello se lanza el ejecutable mediante el acceso directo del escritorio colocado por el instalable (fig. 5).

Una vez iniciado el asistente, éste informa en las primeras páginas de los requisitos y la funcionalidad de la aplicación (fig. 6a y 6b). Se puede ir seleccionando *siguiente* (fig. 7a, 7b y 8a, 8b) hasta llegar a la página donde se efectúa la conexión con el dispositivo móvil y finalmente se cargan los certificados digitales del DNIE 3.0 en el sistema operativo de nuestro PC (en Windows fig. 10 y en Linux fig. 12).



Figura 5: Acceso directo.



(a) Windows



(b) Linux

Figura 6: Asistente de conexión: Introducción.

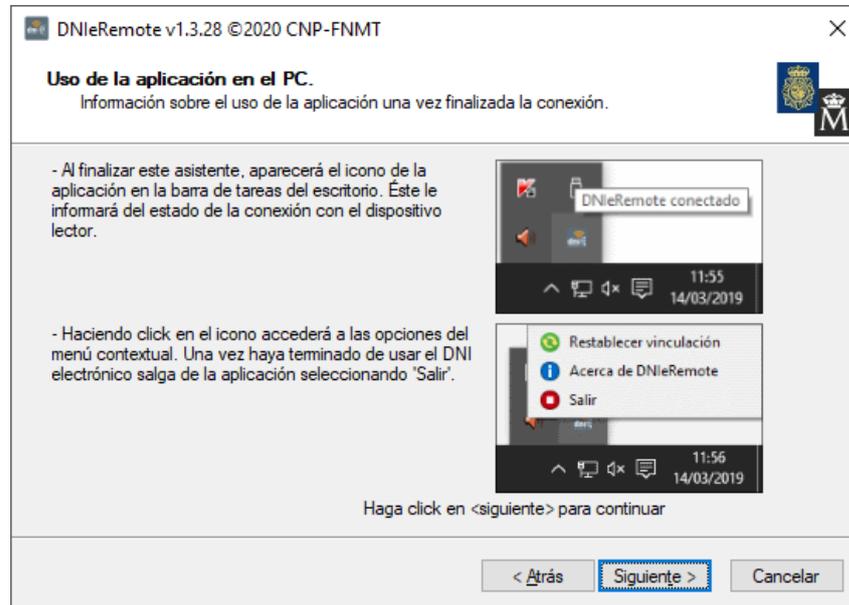


(a) Windows

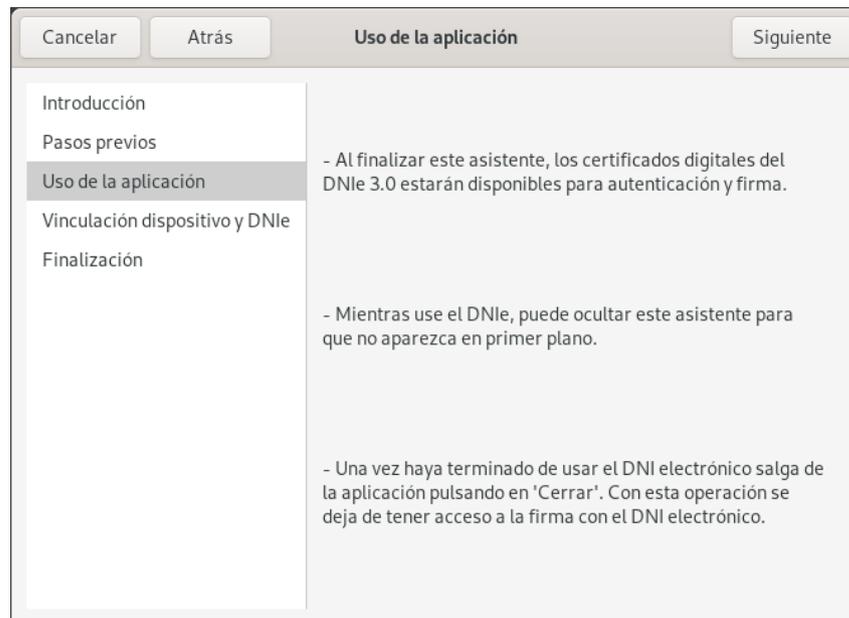


(b) Linux

Figura 7: Asistente de conexión: Pasos previos.



(a) Windows



(b) Linux

Figura 8: Asistente de conexión: Información de uso.

Como se ha comentado antes, esta aplicación funciona conjuntamente con la App del dispositivo móvil, por lo que en primer lugar se advierte de la necesidad de iniciarla. Ésta a su vez también advierte de la necesidad de instalar e iniciar el asistente en el equipo PC (fig. 9a).

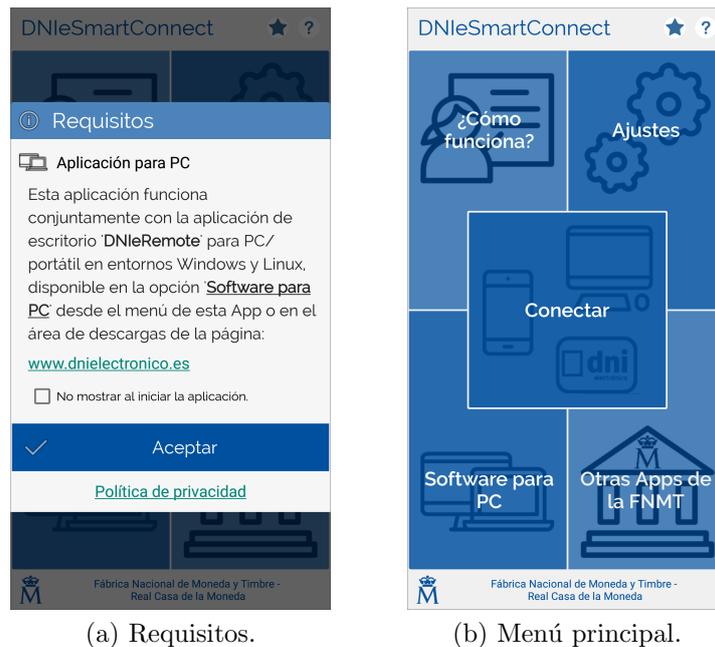


Figura 9: Android: Inicio de aplicación.

Windows:

Una vez se pulse siguiente en la fase de activación, se muestra las opciones para la vinculación por USB o por WiFi (fig. 11). En el primer caso se tendrá que tener conectado el móvil al PC/portátil con el cable USB y la depuración USB activada (**Cómo activar depuración USB**), y en el segundo caso será necesario capturar el código QR que muestra el asistente con la cámara trasera del dispositivo móvil.

Linux:

Por ahora sólo está disponible la vinculación a través de conexión Wi-Fi, por lo que directamente se muestra el código QR (fig. 12).

Android:

A su vez, se deberá elegir el medio de vinculación en la App del dispositivo móvil. En el caso de conexión por WiFi, se pedirá permiso expreso para acceder a la cámara. A continuación se mostrará la interfaz correspondiente para completar la vinculación (fig. 13a y 13b).



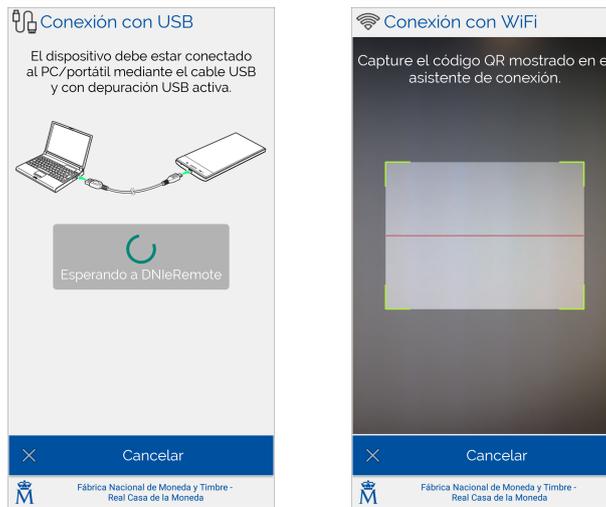
Figura 10: Windows. Asistente: Fase de activación.



Figura 11: Windows. Asistente: Medios de vinculación.



Figura 12: Linux. Asistente: Medio de vinculación.



(a) USB

(b) Wi-Fi

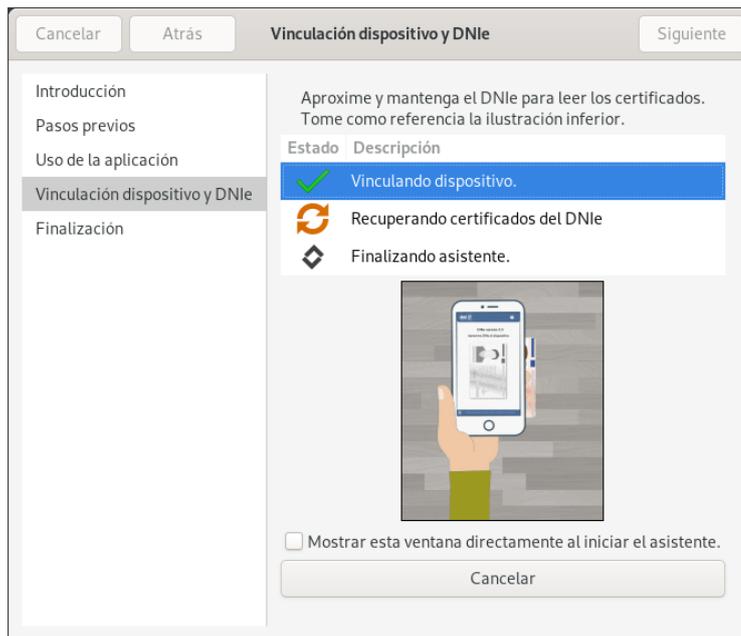
Figura 13: Android: Medios de vinculación.

Al completarse con éxito la vinculación, por cualquiera de los dos medios, el canal seguro de comunicación entre ambos dispositivos queda establecido, y el siguiente paso requiere la presentación del DNLe 3.0 en el dispositivo móvil para iniciar la comunicación a través de NFC (fig. 14a, 14b y 15).

Tanto en Windows como en Linux el asistente muestra una localización aproximada de la antena NFC del dispositivo móvil, en función de la marca y el modelo. Principalmente se suelen localizar en el marco superior, en la zona media o un poco más abajo de la zona media.



(a) Windows



(b) Linux

Figura 14: Asistente de conexión: Fase de lectura.

Se recomienda tener conocimiento previo de la localización de la antena en el terminal, ya que debido a la fragilidad en la conexión NFC, se tendrán serios problemas si no se consigue estabilizarla. Cada marca e incluso modelo de dispositivo móvil tiene sus preferencias en la ubicación de la antena y en la asignación de potencia.



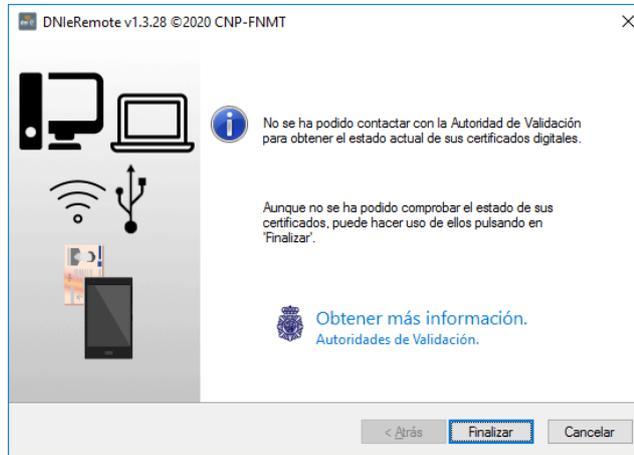
Figura 15: Android App: Lectura de certificados.

El último paso consiste en la comprobación del estado de los certificados, siendo necesaria conectividad a Internet en el dispositivo móvil. Si el estado es correcto, el asistente se cierra automáticamente y la vinculación habrá finalizado. Si no es correcto se muestra el resultado, si se encuentran revocados o expirados, y el procedimiento para su renovación a través de un vínculo directo al portal del **DNI electrónico** donde se informa del proceso.

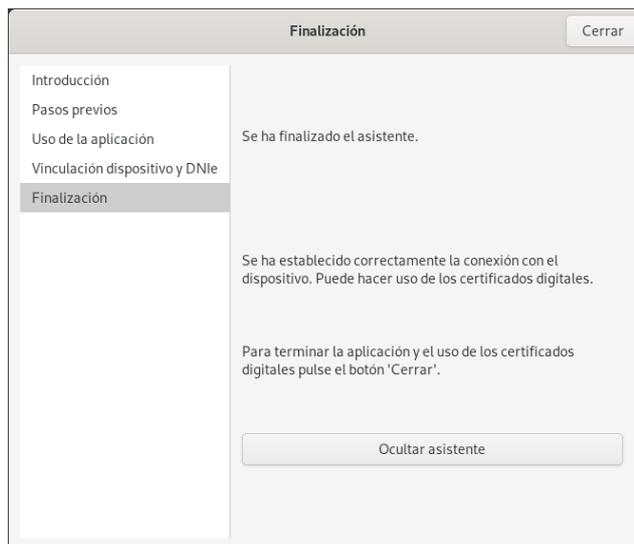
En caso de que no se pueda acceder al servicio de consulta de estado de los certificados, se muestra la advertencia pero permitiendo finalmente el uso de los certificados (fig. 16a y 16b) sin ninguna restricción.

Windows: Una vez finalizada la conexión, se informa al usuario de las diferentes operaciones que se realicen con el DNle mediante mensajes que aparecen en el área de notificaciones del sistema operativo Windows (esquina inferior derecha).

Linux: Para poder hacer uso de los certificados el asistente, aunque haya finalizado, ha de permanecer en ejecución en segundo plano para poder gestionar las peticiones de firma digital con el DNle 3.0 a través de la aplicación Android. Puede ocultar el asistente mediante el botón correspondiente. Si cierra el asistente se finalizará la conexión y no se tendrá acceso a la firma digital.



(a) Windows



(b) Linux

Figura 16: Asistente de conexión: Resultado.

5.2. Integración con Mozilla Firefox

El navegador Firefox requiere de configuración manual para hacer uso de los certificados digitales del DNIe 3.0. Firefox conecta con los dispositivos criptográficos a través de una interfaz estándar o *PKCS#11* (ver [4]) que es necesario indicar en el área de opciones del navegador (fig. 17). Accederemos

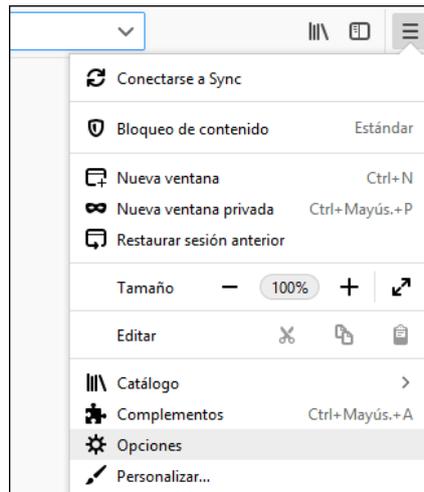


Figura 17: Opciones en Firefox.

al área de configuración (fig. 18) donde se selecciona la pestaña *Privacidad y Seguridad* para añadir el dispositivo de seguridad a través del botón disponible al final de la página.

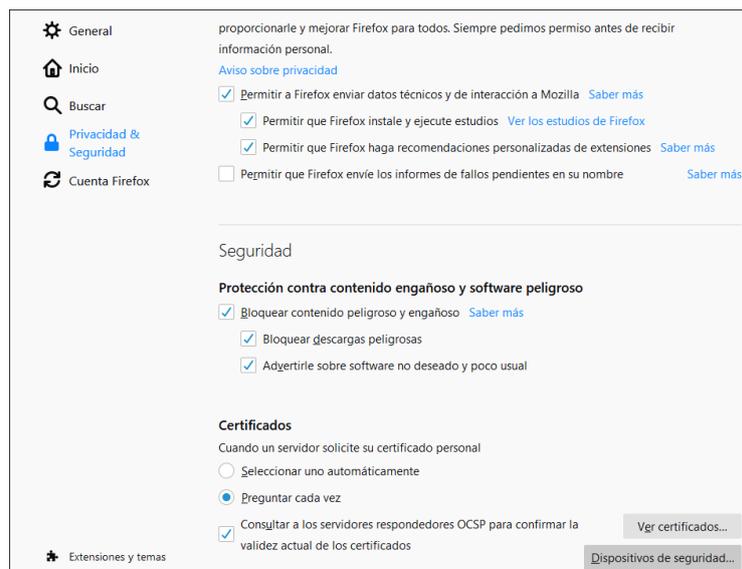


Figura 18: Privacidad y seguridad en Firefox.

Se abrirá un cuadro de diálogo para crear el dispositivo y seleccionar la librería necesaria (fig. 19 y 20):

Windows: el nombre de la librería es *DNiERemotePKCS11.dll* ubicada en */Windows/System32/*.

Linux: el nombre de la librería es *libdnieremotepkcs11.so* ubicada en */usr/local/lib/*.

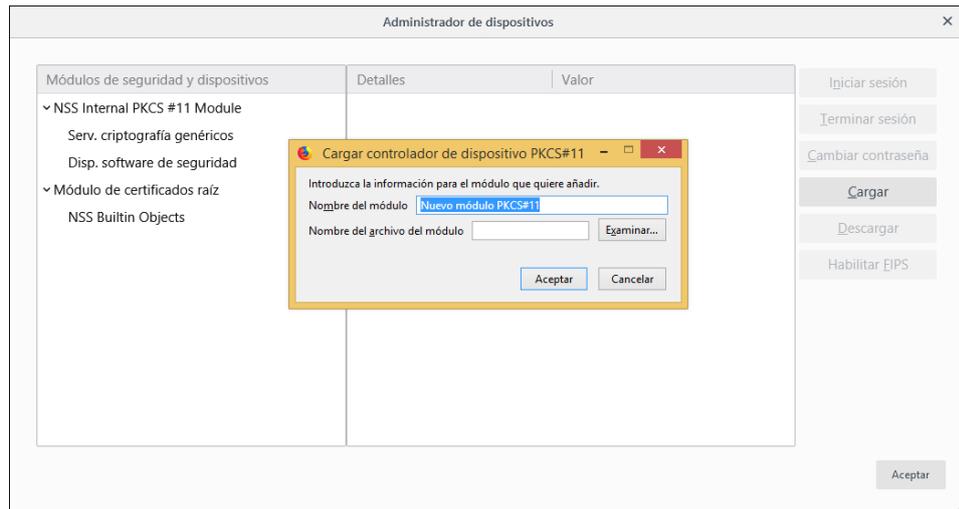


Figura 19: Nuevo dispositivo

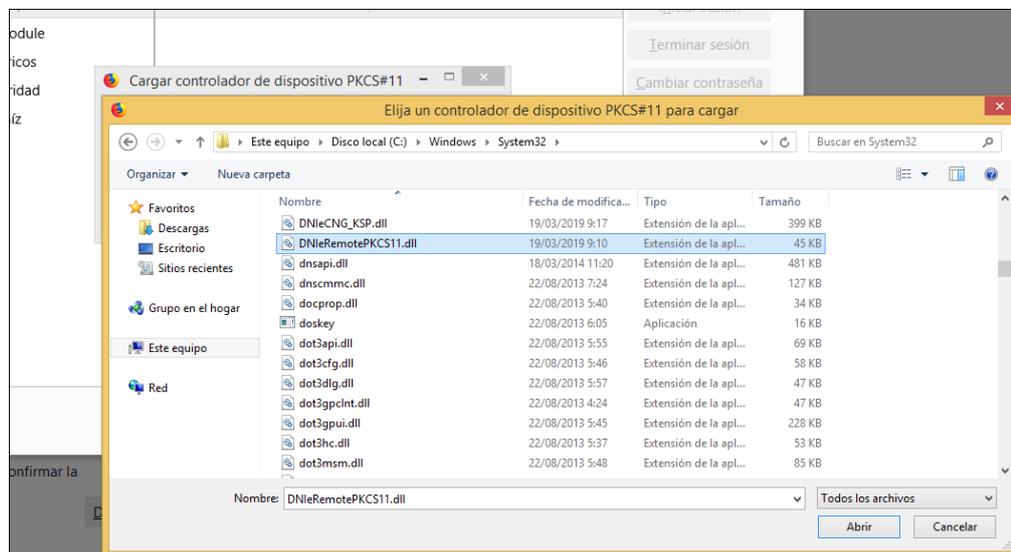


Figura 20: Carga del módulo PKCS#11

Una vez pulsemos ‘Aceptar’ aparecerá el nuevo dispositivo con la información del módulo (fig. 21), guardado para futuros accesos al navegador.

El inicio de sesión **sólo será posible cuando se haya finalizado con éxito el proceso de vinculación del DNIE 3.0** descrito al principio de este documento. Este inicio de sesión se realiza de forma automática cuando se accede a una página web que requiera de autenticación con el certificado del DNIE, por lo que no es necesario realizarlo en este momento.

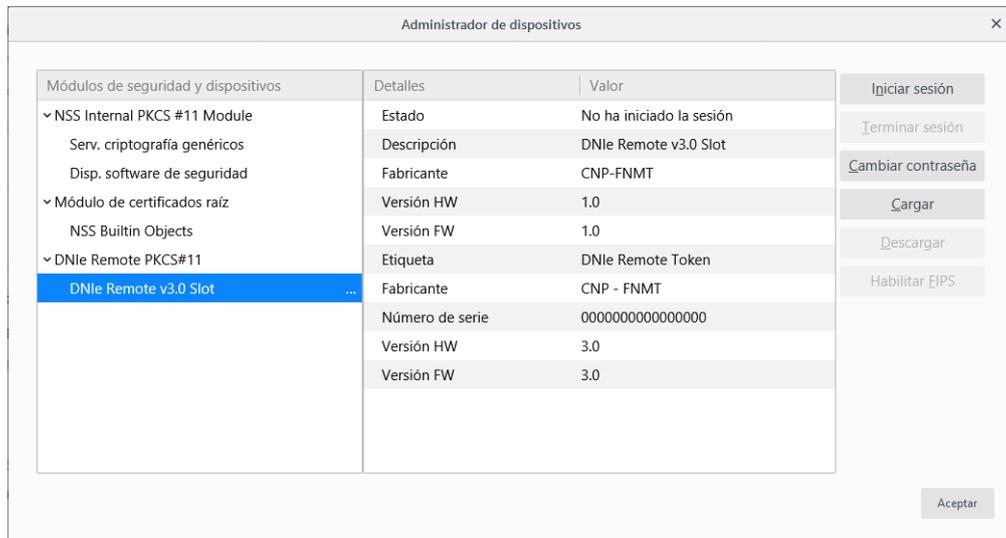


Figura 21: Dispositivo creado

5.3. Integración con Autofirm@

La aplicación Autofirm@ es una herramienta disponible en el [Portal de Administración electrónica](#) que permite realizar operaciones de firma de archivos en entorno de escritorio o por otras aplicaciones en las que se ha integrado, como las aplicaciones web.

Debido a la forma en que cada aplicación implementa la integración con los servicios criptográficos del sistema operativo, por ahora, DNIERemote no es 100 % compatible con Autofirm@. Así, sólo a través del contenedor de claves de Mozilla Firefox es posible directamente realizar operaciones de firma con los certificados que DNIERemote carga en su contenedor. Sin embargo y para usuarios avanzados, es posible hacer compatible Autofirm@ con un procedimiento que se explica más adelante.

Para realizar con éxito la firma del documento será requisito previo configurar correctamente Mozilla Firefox para utilizar los certificados digitales a través de DNIERemote, tal como se explica en el apartado [5.2](#).

Se presentan dos escenarios en los que se podrá hacer uso de Autofirm@ con DNIERemote:

Aplicación de escritorio: A través del modo por línea de comandos que ofrece Autofirm@, se puede indicar el almacén de claves que se utilizará para realizar la firma. Así, para poder firmar con DNIERemote, se establece el comando `-store mozilla` para habilitar la compatibilidad. Un ejemplo de comando de firma sería:

```
C:\Program Files\AutoFirma\AutoFirma>AutoFirma.exe sign -i \Users\john
\Desktop\Sample.pdf -o \Users\john\Desktop\Sample_signed.pdf -store
mozilla -certgui
```

En la documentación de Autofirm@ se pueden encontrar todas las opciones de comandos que ofrece este modo de ejecución.

Navegador web: En las sedes electrónicas de la Administración es común encontrar trámites que requieren de integración con Autofirm@ para completar el proceso. Al utilizar DNIERemote, **sólo con el navegador Mozilla Firefox** se consigue compatibilidad directa con Autofirm@, ya que comparten el mismo contenedor de claves.

Modificación de Autofirm@ para tener compatibilidad con el resto de navegadores (sólo para usuarios avanzados):

En Windows, Autofirm@ se instala con el entorno de ejecución de Java™ o JRE embebido. Hasta la fecha, la versión que incluye no es compatible con el tipo de contenedor para Windows que utiliza DNIERemote, pero

a partir de la versión 13 del JRE ya está solucionado este problema.

Por tanto, el procedimiento sería simplemente descargar la versión 13 o posterior del JRE en **ORACLE Java Software** o en **OpenJDK** y sustituirla (no sobrescribir) por la instalada en el directorio de instalación de Autofirm@ (carpeta jre). Al iniciar posteriormente Autofirm@, ésta advierte de posibles problemas por la versión de Java detectada, pero por ahora las pruebas realizadas con versiones de JRE 13.0.2 y posteriores han sido satisfactorias.

En caso de producirse algún problema, la solución es restaurar la versión original del JRE que venía en el instalador de Autofirma.

6. Preguntas frecuentes (FAQ)

La fase de vinculación del móvil con el PC a través de USB no finaliza.

Respuesta: Verifique que dispositivo móvil tenga el modo de depuración activo y que el modo de transferencia de archivos (MTP) esté también habilitado.

Cuando capturo el código QR en la fase de conexión mediante Wi-Fi siempre aparece el mensaje “La información recuperada no es válida.”.

Respuesta: Compruebe que tanto el PC como el móvil se encuentran conectados a la misma red.

La fase de vinculación del móvil con el PC a través de WiFi tarda varios segundos.

Respuesta: Es un comportamiento normal que el tiempo de vinculación varíe significativamente, llegando a ser inmediata o tardar varios segundos, hasta un máximo de 10, momento en el se considera que hay un problema de comunicaciones, probablemente debido al firewall de Windows. Como posible causa, se tendrá que verificar que existe una entrada en el firewall de Windows para *DNIERemote*.

Aparece el mensaje “Error de comunicación. Se ha perdido la conexión con el DNIe.” al aproximar el DNIe 3.0 al móvil para la carga de certificados.

Respuesta: La conexión mediante NFC es frágil, de muy corto alcance y requiere colocación precisa del DNIe 3.0. Averigüe la ubicación de la antena en su dispositivo móvil y, una vez detecte el DNIe, procure no moverlo.

Los certificados digitales no aparecen cuando utilizo aplicaciones Java™.

Respuesta: La aplicación provee de las interfaces actualmente soportadas por el sistema operativo para que las aplicaciones de terceros reconozcan los certificados del DNIe. Es responsabilidad del desarrollador de la aplicación adaptar ésta de acuerdo a las recomendaciones del proveedor en la integración con el sistema operativo.

Autofirm@ no muestra los certificados del DNIe.

Respuesta: En la sección [5.3](#) puede encontrar más información a cerca de la compatibilidad de DNIERemote con Autofirm@.

Referencias

- [1] NFC FORUM, NXP SEMICONDUCTORS, *NFC Forum Type Tags White Paper V1.0*, 2009.
- [2] ANDROID DEVELOPERS, ANDROID DOCUMENTATION, *App Widgets Overview*, 2018.
- [3] DPTO. DOCUMENTOS DE IDENTIFICACIÓN Y TARJETAS, FNMT, *Guía de referencia del DNIe con NFC*, 2017.
- [4] OASIS PKCS 11 TC, *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40*, 2017.