



MANUAL DE USUARIO

# DNiERemote v1.2



24 de mayo de 2019

DNIEREMOTE v1.2

---

<b>Versión</b>	<b>Fecha</b>	<b>Autores</b>	<b>Descripción</b>
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.

# Índice

<b>1. Introducción</b>	<b>5</b>
<b>2. Componentes</b>	<b>5</b>
<b>3. Requisitos técnicos</b>	<b>6</b>
3.1. Software . . . . .	6
3.2. Hardware . . . . .	6
3.3. Conectividad . . . . .	6
<b>4. Instalación</b>	<b>6</b>
4.1. Windows . . . . .	6
4.2. Android . . . . .	7
<b>5. Uso</b>	<b>7</b>
5.1. Vinculación con el DNLe . . . . .	8
5.2. Integración con Mozilla Firefox . . . . .	16
<b>6. Preguntas frecuentes (FAQ)</b>	<b>19</b>

## 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. . . . .	8
5.	Acceso directo. . . . .	9
6.	Asistente de conexión: Introducción. . . . .	9
7.	Asistente de conexión: Pasos previos. . . . .	10
8.	Asistente de conexión: Información de uso. . . . .	10
9.	Android: Inicio de aplicación. . . . .	11
10.	Asistente: Fase de activación. . . . .	12
11.	Asistente: Selección de medio. . . . .	12
12.	Asistente: Medios de vinculación. . . . .	12
13.	Android: Medios de vinculación. . . . .	13
14.	Asistente de conexión: Fase de lectura . . . . .	13
15.	Android App: Lectura de certificados . . . . .	14
16.	Asistente de conexión: Fase de lectura, petición PIN . . . . .	14
17.	Asistente de conexión: Resultado . . . . .	15
18.	Opciones en Firefox . . . . .	16
19.	Privacidad y seguridad en Firefox . . . . .	16
20.	Nuevo dispositivo . . . . .	17
21.	Carga del módulo PKCS#11 . . . . .	17
22.	Dispositivo creado . . . . .	18

## 1. Introducción

En la actualidad se ha generalizado por completo el uso de los dispositivos móviles para el acceso a Internet. Esto permite a cualquier usuario estar siempre conectado y tener disponibles multitud de servicios telemáticos. En función del nivel de seguridad que requieran dichos servicios, éstos pueden necesitar de la autenticación del usuario, lo que hace que el Documento Nacional de Identidad (DNIe 3.0) pueda convertirse en una pieza clave.

La incorporación de la tecnología NFC (Near Field Communication, ver [1]) a los dispositivos móviles de última generación elimina las barreras del lector, drivers, etc. facilitando la conexión online y la autenticación del ciudadano. Por su parte, el DNIe 3.0 tiene un chip dual-interface que permite su utilización tanto con contactos como en modo contactless.



Figura 1: Reverso DNIe v3.0

La aplicación DNIERemote v1.2 aprovecha esta tecnología para convertir el dispositivo móvil en un lector del DNIe 3.0 conectado al PC, permitiendo así acceder a los servicios de la administración electrónica que requieren de autenticación con certificado digital, y realizar firmas digitales en documentos a través de las correspondientes aplicaciones.

## 2. Componentes

La aplicación DNIERemote v1.2 se compone de dos módulos: una aplicación de escritorio para sistemas operativos Windows y una App Android para el dispositivo móvil funcionando “en tándem”, es decir, ambos tienen que estar instalados y en ejecución para operar con el DNIe 3.0.

## 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 *Internet Explorer*, *Google Chrome*, *Opera* y *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, capacidad para conectarse a redes Wi-Fi<sup>®</sup>, y captura de imágenes con cámara trasera.

### 3.3. Conectividad

En caso de vinculación por WiFi, 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 v1.2 se puede obtener a través del 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 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.

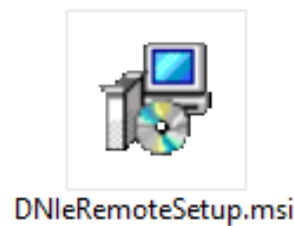


Figura 2: Paquete de instalación Windows.

**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. 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.

## 5. Uso

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

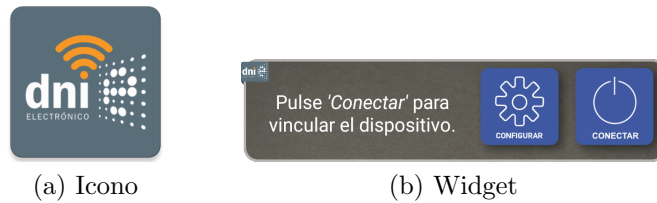


Figura 3: Accesos a la aplicación.

A continuación se describe con detalle el proceso de carga y vinculación del DNIE con el sistema operativo Windows 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).

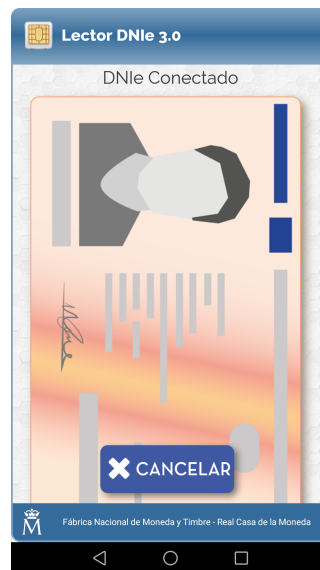


Figura 4: Android App: DNIE conectado.

### 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).



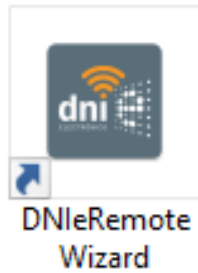


Figura 5: Acceso directo.

Una vez iniciado el asistente, éste informa en las primeras páginas de los requisitos y la funcionalidad de la aplicación (fig. 6). Se puede ir seleccionando *siguiente* (fig. 7 y 8) 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 Windows de nuestro PC (fig. 10).

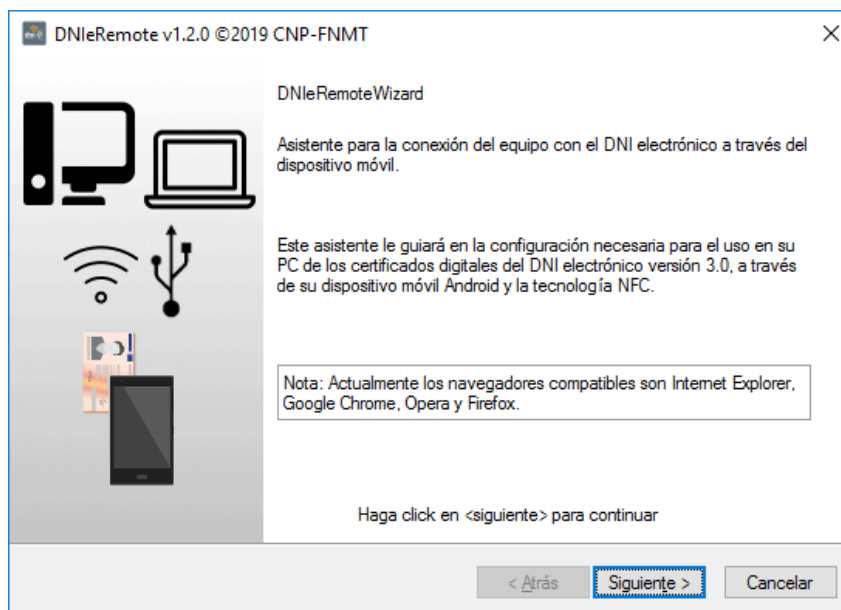


Figura 6: Asistente de conexión: Introducción.



Figura 7: Asistente de conexión: Pasos previos.

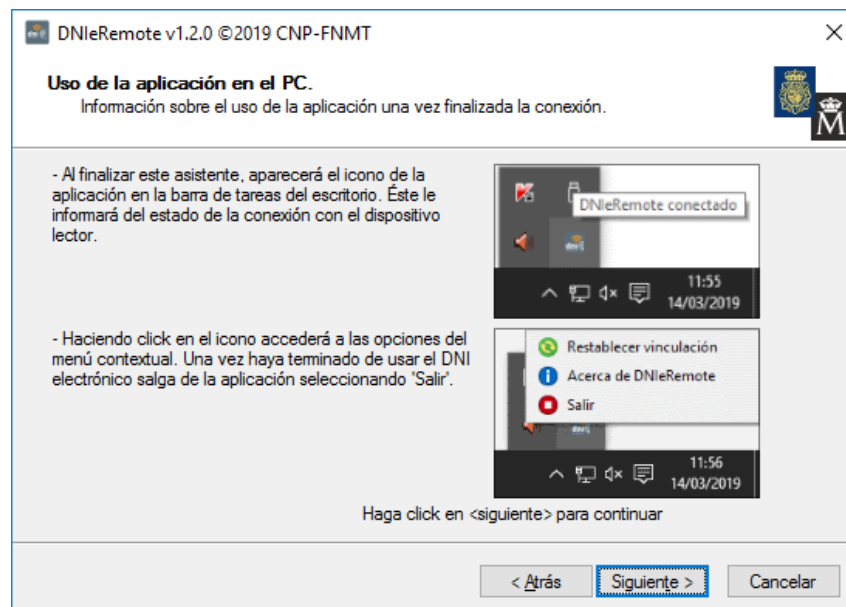


Figura 8: Asistente de conexión: Información de uso.

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 Windows (fig. 9a).



(a) Requisitos.

(b) Menú principal.

Figura 9: Android: Inicio de aplicación.

Una vez se pulse siguiente en la fase de activación, se requiere seleccionar el medio de vinculación, bien por USB o por conexión WiFi (fig. 11). A continuación se muestra el diálogo para la vinculación por USB (fig. 12a) o el diálogo para la captura del código QR que muestra el asistente (fig. 12b) con la cámara trasera del dispositivo móvil.

A su vez, también se deberá elegir el mismo medio de vinculación en la App del dispositivo móvil. Ambos medios pedirán permiso expreso para acceder al sistema de archivos del dispositivo móvil o a la cámara y mostrarán la interfaz correspondiente para completar la vinculación (fig. 13a y 13b).

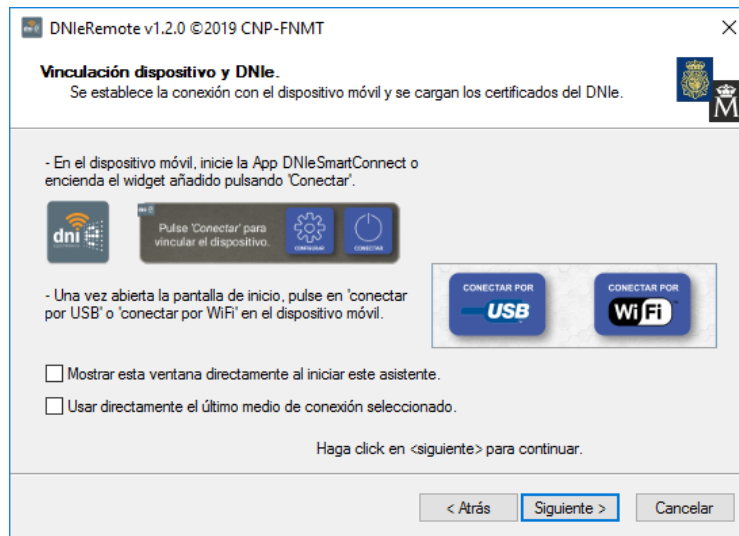


Figura 10: Asistente: Fase de activación.

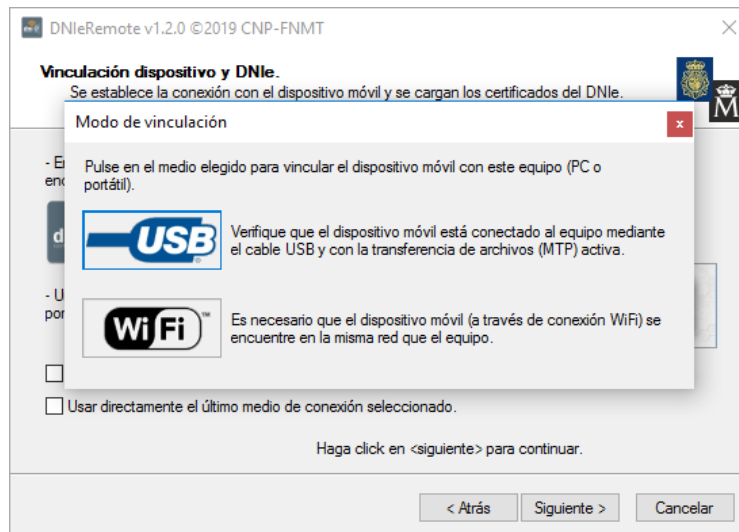
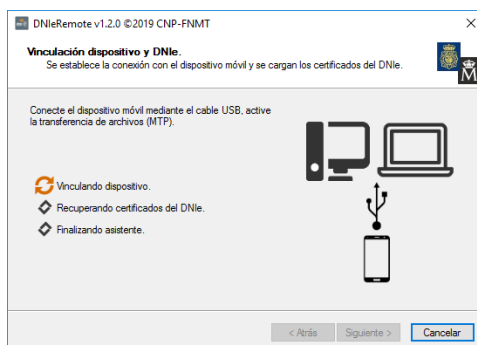


Figura 11: Asistente: Selección de medio.



(a) USB



(b) WiFi

Figura 12: Asistente: Medios de vinculación.

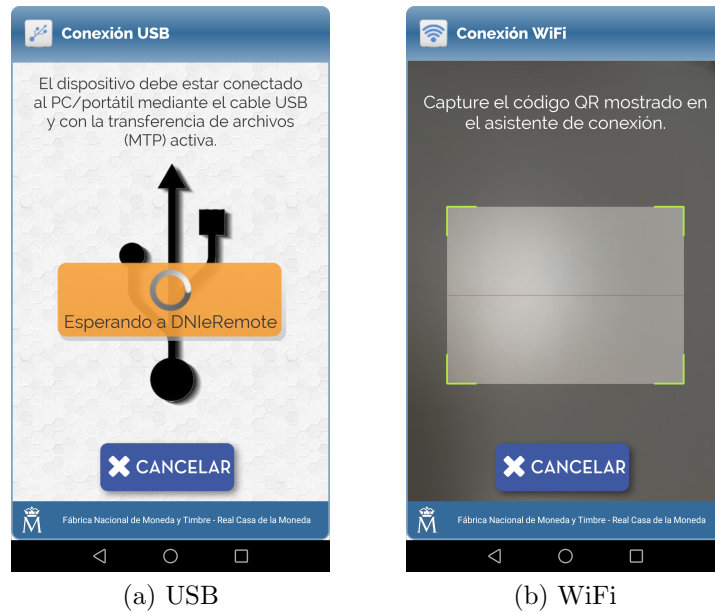


Figura 13: Android: Medios de vinculación.

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 DNIe 3.0 en el dispositivo móvil para iniciar la comunicación a través de NFC (fig. 14 y 15).

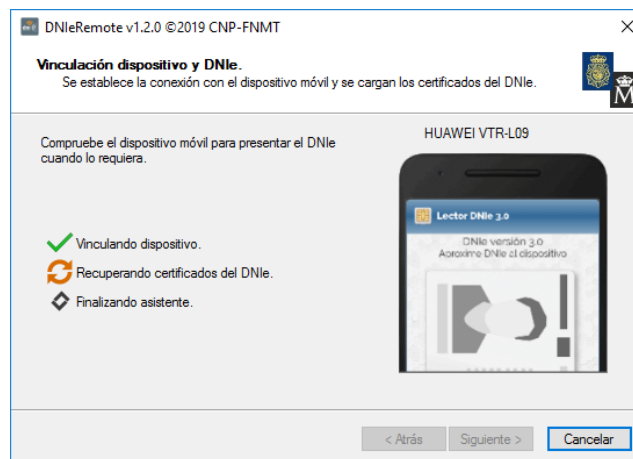


Figura 14: Asistente de conexión: Fase de lectura

Es importante 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 (zona media, extremo superior, etc.) y en la asignación de potencia.

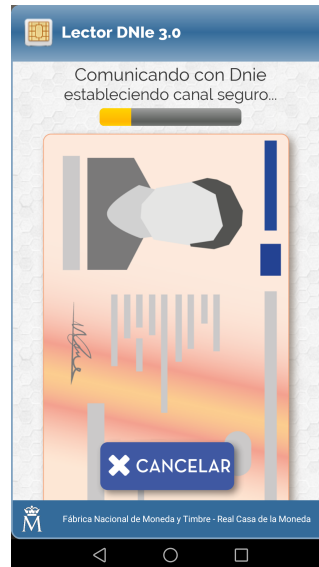


Figura 15: Android App: Lectura de certificados

Para cargar los certificados digitales el usuario debe indicar el PIN cuando se requiera (fig. 16).

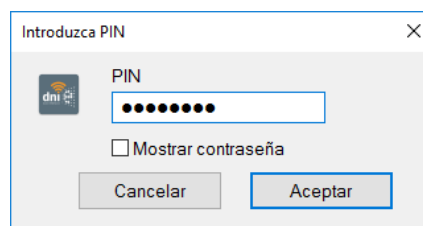


Figura 16: Asistente de conexión: Fase de lectura, petición PIN

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. De lo contrario, 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. 17) sin ninguna restricción.

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

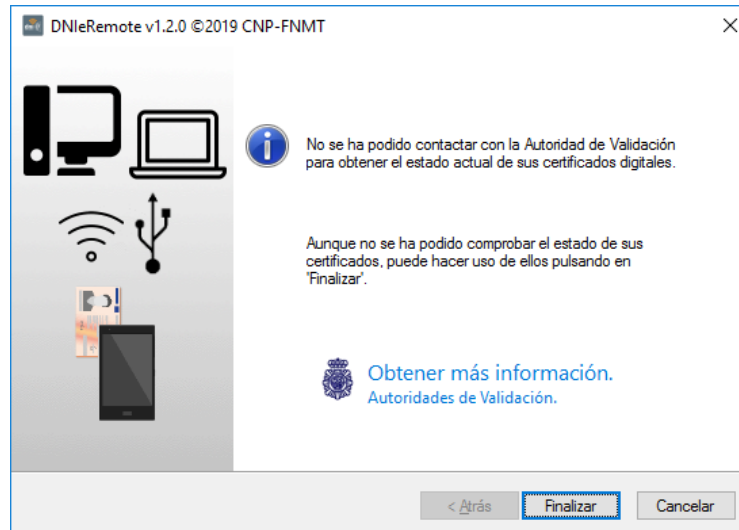


Figura 17: Asistente de conexión: Resultado



## 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. 18). Accederemos

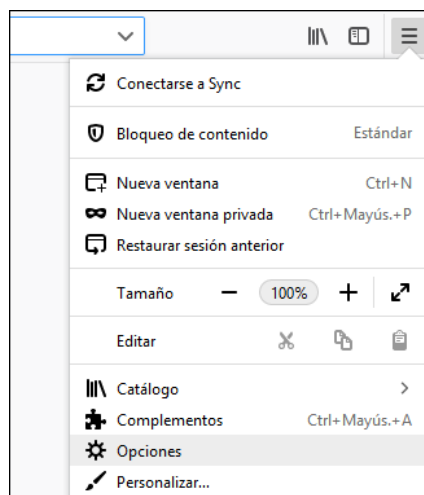


Figura 18: Opciones en Firefox

al área de configuración (fig. 19) donde se selecciona la pestaña *Privacidad y Seguridad* para añadir el dispositivo de seguridad a través del botón disponible al final de la página.

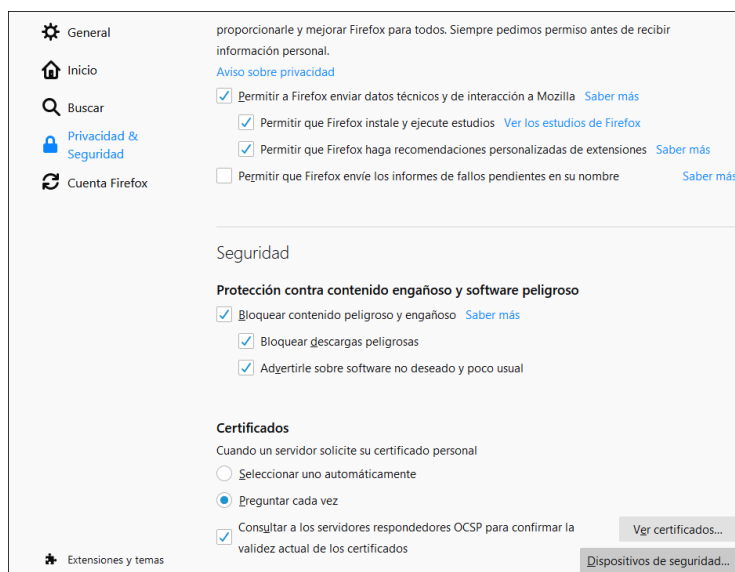


Figura 19: Privacidad y seguridad en Firefox

Se abrirá un cuadro de diálogo para crear el dispositivo y seleccionar la librería (fig. 20 y 21).



5 USO

DNIEREMOTE v1.2

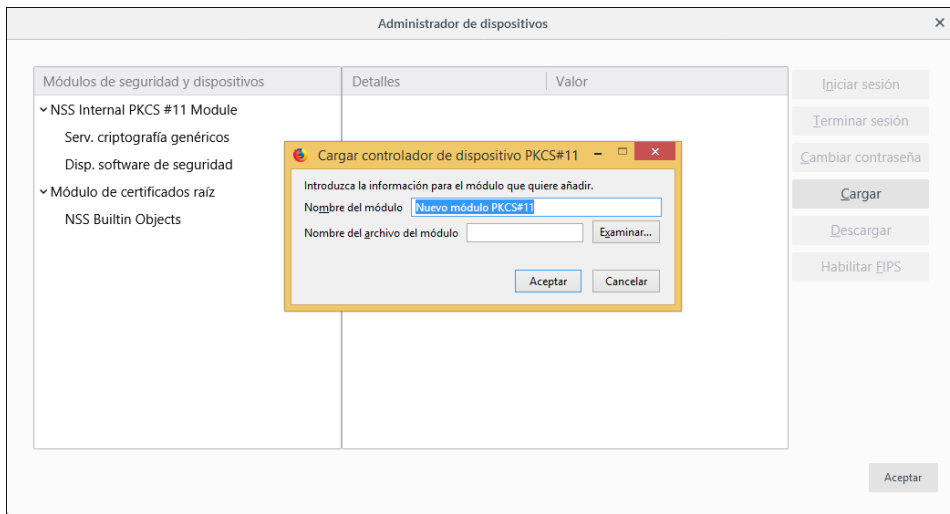


Figura 20: Nuevo dispositivo

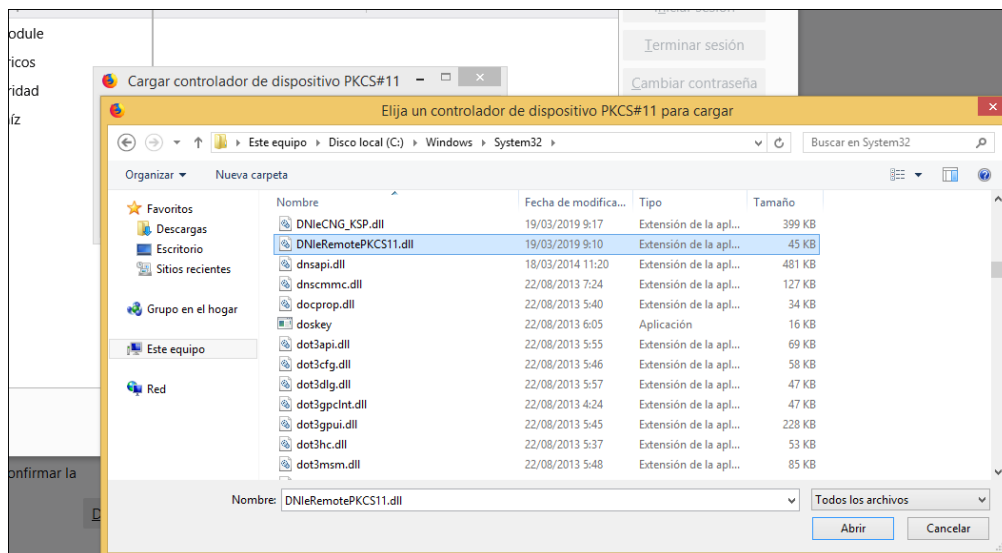


Figura 21: Carga del módulo PKCS#11

Una vez pulsemos ‘Aceptar’ aparecerá el nuevo dispositivo con la información del módulo (fig. 22), 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.

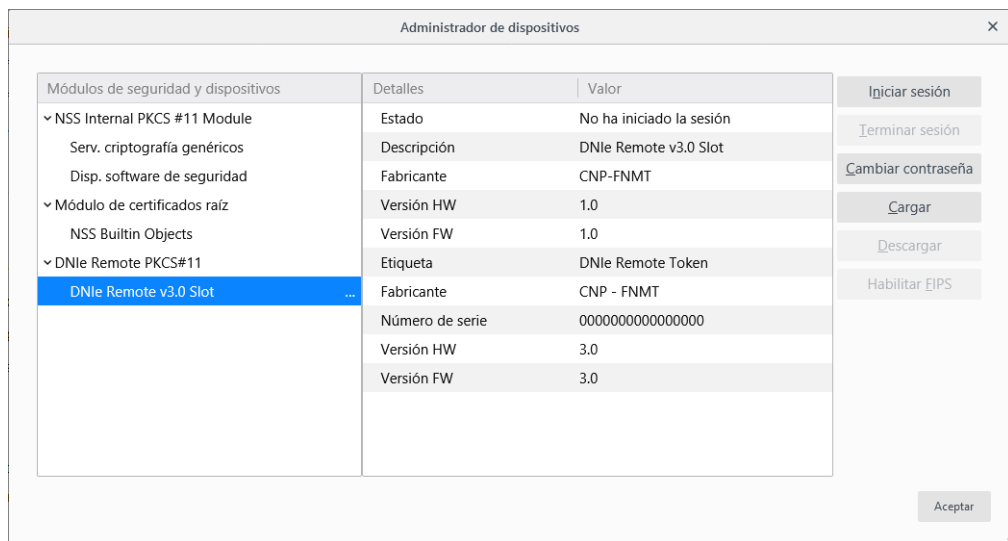


Figura 22: Dispositivo creado

## 6. Preguntas frecuentes (FAQ)

**La fase de vinculación del móvil con el PC a través de USB no finaliza o aparece el mensaje “Existe un problema en la sincronización de datos...”.**

Respuesta: Es posible que se haya perdido visibilidad del sistema de archivos del móvil. Desconecte y vuelva a conectar el cable USB al PC, activando siempre después el modo de transferencia de archivo vía USB (MTP).

**Cuando capturo el código QR en la fase de conexión mediante WiFi 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.

## 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.