



OFICINA TÉCNICA DNI-E

# DOCUMENTO DE RECOMENDACIONES DE INSTALACIÓN

## ¿Cómo instalo el Módulo Criptográfico para el DNIe?

En la página Web encontrará el software con el ejecutable para la instalación del citado modulo criptográfico para sistemas Windows en el siguiente enlace http:

http://www.dnielectronico.es/descargas/win\_comp\_vista.html

Con solo ejecutar el fichero descargado se instalará el módulo *CSP* para el entorno Microsoft Windows y el módulo *PKCS#11* para navegadores Firefox Mozilla y Netscape sobre Windows.

Deberá reiniciar el PC para finalizar la instalación. En el reinicio se instalará el Certificado AC RAIZ DNIE en los navegadores que estén instalados previamente en el equipo. También se configuran los dispositivos de seguridad de los navegadores Firefox Mozilla y Netscape instalados.

En el directorio *C:* \*DNIe* se ubicará un archivo de log y los dos archivos siguientes para futuras configuraciones por parte del usuario:

## Certificado raíz de la DGP:

## ACRAIZ\_CERTIFICATE\_AND\_CRL\_SIGNING\_SHA1.crt

#### Módulo PKCS#11 para la instalación:

#### instalac.htm

Si se trata de la primera vez que instala el CSP del DNIe, al reiniciar el equipo le aparecerá la pantalla siguiente que indica que se va a proceder a instalar el certificado AC RAIZ DNIE.

Certificado	? 🗙
General Detalles Ruta de certificación	
Información del certificado	
Este certificado está destinado a los siguientes propósitos:	
•Todas las directivas de emisión •Todas las directivas de la aplicación	
* Más info. en declaración de entidades emisoras de certificados.	
Enviado a: AC RAIZ DNIE	
Emitido por AC RAIZ DNIE	
Válido desde 16/02/2006 hasta 09/02/2036	
Declaración del en	ni <u>s</u> or
	ceptar

Si ya había sido instalado anteriormente, esta ventana no será mostrada. Igualmente puede no aparecer esta ventana si el navegador Internet Explorer está suficientemente actualizado, ya que este certificado se instala automáticamente con un parche de actualización de Microsoft.





OFICINA TÉCNICA DNI-E

Le solicitará que confíe/instale el certificado raíz del DNIe, deberá **aceptar/instalar**. Este paso es necesario para el correcto funcionamiento del DNIe.

Asistente para importación de certificados	
Éste es el Asistente para importación de certificado Este asistente le ayuda a copiar certificado confianza de certificados y listas de revoca certificados desde su disco a un almacén de Un certificado, que se emite por una entida certificación, es una confirmación de su ide contiene información que se utiliza para pro para establecer conexiones de red seguras de certificados. Haga dic en Siguiente para continuar.	DS s, listas de ciones de e certificados. id emisora de ntidad y bteger datos o . Un almacén a se guardan Cancelar

## Pulsamos sobre "Siguiente"

Asistente para importación de certificados 🛛 🔀
Almacén de certificados Los almacenes de certificados son áreas del sistema donde se guardan los certificados.
Windows puede seleccionar automáticamente un almacén de certificados, o bien es posible especificar una ubicación para el certificado. Seleccionar automáticamente el almacén de certificados en base al tipo de certificado Colocar todos los certificados en el siguiente almacén Almacén de certificados:
Examinar
< <u>A</u> trás Siguien <u>t</u> e > Cancelar

#### Pulsamos sobre "Examinar"

Seleccionamos el Almacén de certificados: "Entidades Emisoras Raíz de Confianza"

		an de cercini	ados que q	ulere us	ar.
	Personal				$\sim$
····	Entidades	emisoras rai	iz de confiai	nza	
	Confianza	empresarial			
Com	Entidades	emisoras de	cert. interr	medias	
	Editores de	e confianza			
<b>_</b>	Certificado	s en los que	no se conf	ía 📑	~
<		IIII		>	
Mostr	ar almacen	es <u>f</u> ísicos			





OFICINA TÉCNICA DNI-E

Asistente para importación o	le certificados			
	Finalización del Asistente para importación de certificados Ha completado con éxito el Asistente para importación de certificados.			
	Ha especificado la siguiente configuraci	ón:		
	Almacén de certificados seleccionado Contenido	Determinado de fo Certificado		
	<	>		
	< <u>A</u> trás Finali:	zar Cancelar		

Pulsamos sobre "Finalizar"

Adverte	encia de seguridad 🛛 🕺
1	Está a punto de instalar un certificado desde una autoridad de certificados (CA) que afirma representar a: AC RAIZ DNIE Windows no puede validar que el certificado procede realmente de "AC RAIZ DNIE". Póngase en contacto con "AC RAIZ DNIE" para confirmar su origen. El siguiente número le ayudará en este proceso:
	Huella digital (sha 1): B38FECEC 0B 148AA6 86C3D00F 0 1ECC884 8E8085EB Advertencia: Si instala este certificado de raíz, Windows confiará automáticamente en cualquier certificado emitido por esta CA. La instalación de un certificado con una huella digital sin confirmar supone un riesgo para la seguridad. Al hacer dic en "Si", asume este riesgo. ¿Desea instalar este certificado?

En este punto pulsar sobre el botón "Sí" para permitir que la autoridad raíz del DNIe, AC RAIZ DNIE, se instale en el navegador y de esta forma se pueda establecer adecuadamente la cadena de confianza de certificación. (La desinstalación del CSP del DNIe no borra el certificado raíz del navegador, por lo que si realiza una segunda instalación, o actualiza la versión no volverá a mostrarse este mensaje)

Asistent	e para importación de certificados	×
(į)	La importación se completó correctamente.	





OFICINA TÉCNICA DNI-E

#### ¿Cómo sé que está bien instalado?

Para verificar que la instalación se ha realizado correctamente se puede hacer uso de cualquiera de los servicios disponibles como se indica en <u>http://www.dnielectronico.es/servicios\_disponibles/</u>.

También se puede verificar de modo manual como se indica a continuación. Dependiendo de los navegadores instalados en su PC:

#### 1. Internet Explorer

#### A través del menú Herramientas / Opciones de Internet / Contenido / Certificados...

Conexiones	Progr	amas	Opcio	nes avanzadas
General	Segurdad	Priva	cldad	Contenido
Inter	lasificaciones le a net que se puede	yudan a contr ver con este	equipo.	o de contenido de
Inter	lasificaciones le a net que se puede	yudan a contr e ver con este <u>H</u> abilitar	olar el tipo equipo.	o de contenido de Configuración
ertificados —	lasificaciones le a net que se puede	yudan a conti e ver con este <u>H</u> abilitar	equipo.	o de contenido de

Si está instalado correctamente el módulo CSP del DNIE (Proveedor de Servicios de Certificación) y tiene correctamente instalados los drivers del lector de tarjetas criptográficas e introducido éste en el citado lector, le pedirá el PIN del DNIe.

		Introduzca el PIN
dni		
ELECTRÓNICO	•••	

Una vez lo introduzca podrá ver los siguientes certificados:

- 1. Los certificados del DNIe en la pestaña Personal:
  - un certificado con propósito de Autenticación
  - y otro certificado con propósito de Firma.





OFICINA TÉCNICA DNI-E

Certificad	os				? 🛛
P <u>r</u> opósito p	lanteado:	dos>			✓
Personal	Otras personas	Entidades emis	oras de certifi	cados intermedias	Entidades emi < 🕨
Emitida	o para			Emitido por	Fecha d
🔛 AF	PELLIDOS, NON	1BRE (AUTER	NTICACIÓN)	AC DNIE 001	05/03/2011
	ELLIDOS, NOK	IDICE (FIRM)	4)	AC DIVIE 001	05/03/2011
<				]	>
<u>Importar</u>	<u>E</u> xportar	Quitar			<u>A</u> vanzadas
Propósito	s planteados del i	ertificado ——			
					Ver
					⊆errar

2. En la pestaña *Entidades emisoras raíz de confianza* podrá visualizar el certificado raíz AC RAIZ DNIE.

Certificados ?X	Certificado ?X
Propósito planteado: <todos></todos>	General Detalles Ruta de certificación
Entidades emisoras de certificados intermedias Entidades emisoras raíz de confianza Edit	Información del certificado
Emitido para     Emitido por     Fecha de caducidad     Nombre descript       AC RAIZ DNIE     AC RAIZ DNIE     09/02/2036 <ininguno></ininguno>	Este certificado está destinado a los siguientes propósitos: • Todas las directivas de emisión • Todas las directivas de la anliración
	* Más info. en declaración de entidades emisoras de certificados.
Importar Exportar Quitar Avanzadas	Enviado a: AC RAIZ DNIE
Propósitos planteados del certificado Autenticación del servidor, Autenticación del cliente, Firma de código, Correo	Emitido por AC RAIZ DNIE
seguro, Impresión de techa, 1.3.6.1.5.5.7.3.9, Sistema de archivos de cifrado, Seguridad IP del fin del túnel, Seguridad IP del usuario de seguridad,	Válido desde 16/02/2006 hasta 08/02/2036
Cerrar	Dedaración del emi <u>s</u> or
genu	Aceptar

Si ha podido seguir los pasos anteriores y ver los certificados esto indica que está correctamente instalado el módulo CSP y el certificado raíz para Microsoft.





OFICINA TÉCNICA DNI-E

2. <u>Netscape</u>

A través del menú Herramientas / Opciones / Avanzado / Dispositivos de Seguridad

Options							
Main	Tabs	Content	5 Feeds	0 Privacy	Security	Advanced	
General	Mini Browse	r Link Pad	Network	Update	Encryption		
Proto	ocols Use SSL <u>3</u> .0			V	] Use TLS <u>1</u> .(	)	
Certi When	ficates n a web site r	equires a ce	rtificate:				
•	Select one au	itomatica <mark>ll</mark> y	O Ask 1	me <mark>every t</mark>	ime		
Viev	w Certificates	Revoca	ation Lists	<u>V</u> erific	ation Se	curity Devices	
					ок	Cancel	ielp

Si está correctamente instalado el módulo PKCS#11 aparecerán en la lista de Dispositivos y módulos de seguridad instalados el módulo *DNI e Modulo PKCS#11*.

Security Modules and Devices		Details	Value	Log In
NSS Internal PKCS #11 Module	^	Module	DNIe Modulo PKCS # 11	
Generic Crypto Services		Path	USRPKCS11.dll	Log Out
Software Security Device				Change Password
Builtin Roots Module	=			
Builtin Object Token				Load
DNIe Modulo PKCS # 11				Unload

Con el módulo *DNI e Modulo PKCS#11* instalado, para ver los certificados del *DNI electrónico* hay que abrir el navegador netscape, y seguir el menú Herramientas / Opciones / Avanzado / Ver certificados , esto le pedirá el PIN del DNIe:

Contra	seña requerida 🛛 🚺
3	Por favor, introduzca la contraseña maestra para DNI electrónico.
	[
	Aceptar Cancelar





OFICINA TÉCNICA DNI-E

Después de introducir correctamente el PIN se abrirá una ventana del **Gestor de certificados** que mostrará en la pestaña **Sus certificados** los dos certificados que incorpora el documento:

- un certificado con propósito de Autenticación
- otro certificado con propósito de Firma.

En la pestaña "Autoridades" se podrá visualizar el certificado intermedio AC DNIE OOX (el valor de X será 1, 2 ó 3 ) y el certificado AC RAIZ DNIE.

uthorities ertificate authorities
curity Device
tin Object Token tin Object Token
electrónico
tware Security Devio
tin Object Token tin Object Token tin Object Token

Si ha podido seguir los pasos anteriores y ver los certificados, esto indica que está correctamente instalado el módulo PKCS#11 y el certificado raíz para Netscape.

## 3. Firefox

Siguiendo el menú Herramientas / Opciones / Avanzado, pestaña Seguridad botón "Dispositivos de Seguridad"

ciones						n (1865 - 1	
十			2	6		<u></u>	
Principal	Pestañas	Contenido	Canales	Privacidad	Seguridad	Avanzado	
eneral Re	ed Actualizar	Cifrado					
Durta	1						_
Protoco				<b>E</b> .			
Us Us	ar SSL <u>3</u> .0			Usar TLS	<u>1</u> .0		
Certific	ados						1
Cuando	o un sitio web	requiera un c	ertificado:				
C Se	leccionar uno	automáticame	ente 💿 F	Preguntarme ca	ada ve <u>z</u>		
_					(		
Ver ce	ertificados	Listas de <u>r</u> ev	ocación	Verificación	Dispositivo	s de seguridad	





OFICINA TÉCNICA DNI-E

Si está correctamente instalado el módulo PKCS#11 aparecerán en la lista de Módulos de seguridad y dispositivos instalados el módulo *DNI e Modulo PKCS#11*.

Administrador de dispositivos			
Módulos de seguridad y dispositivos	Detalles	Valor	
<ul> <li>NSS Internal PKCS #11 Module</li> <li>Servicios de criptografía gené</li> <li>Dispositivo software de segurida</li> </ul>		Módulo Ruta	DNIe Modulo PKCS # 11 USRPKCS11.dll
DNIe Modulo PKCS # 11			

Con el módulo *DNIe Modulo PKCS#11* instalado, para ver los certificados del *DNI electrónico* hay que abrir el navegador Firefox, y seguir el menú Herramientas / Opciones / Avanzado / Ver certificados, esto le pedirá el PIN del DNIe:

Contraseña requerida 🛛 🔀
Por favor, introduzca la contraseña maestra para DNI electrónico.
Aceptar Cancelar

Después de introducir correctamente el PIN y a través de la ventana Opciones, pulse el botón "Ver Certificados"

En la pestaña Sus Certificados podrá ver sus dos certificados:

- un certificado con propósito de Autenticación
- y otro certificado con propósito de Firma.

En la pestaña "Autoridades" podrá visualizar el certificado intermedio AC DNIE OOX (el valor de X será 1, 2 ó 3 ) y el certificado raíz AC RAIZ DNIE.

Sus certificados	Personas	Servidores	Autoridades	Otros		
Tiene certifica	dos archiva	ados que ider	ntifican a estas	s autoridade	s certificadoras:	
Nombre del certificado				Dispositi		
DIRECCIO	N GENERAL	DE LA POLI	CIA			^
AC DNIE 001				Disp. soft		
AC RAIZ DNIE				Disp. soft	~	
<u>V</u> er	Edita	r I <u>m</u>	portar	E <u>x</u> portar	Elimina <u>r</u>	
	6 - 22	10.05	10.00			

Si ha podido seguir los pasos anteriores y ver los certificados, esto indica que está correctamente instalado el módulo PKCS#11 y el certificado raíz para Firefox.





OFICINA TÉCNICA DNI-E

## SOLUCION DE PROBLEMAS

No puedo visualizar el certificado raíz AC RAIZ DNIE

Este problema puede aparecer en los navegadores Internet Explorer, Netscape y Firefox.

El programa de instalación deja el certificado raíz en el directorio c:\DNIe\ con el nombre ACRAIZ\_CERTIFICATE\_AND\_CRL\_SIGNING\_SHA1.crt.

Para solucionar este problema deberá abrir el navegador (Internet Explorer, Netscape y/o Firefox) y después arrastrar y soltar el certificado raíz sobre el navegador abierto y seguir los pasos que se indican.

Para verificar que se ha instalado el certificado raíz seguir los pasos indicados en el apartado *Cómo sé que está bien instalado.* 

## No puedo visualizar el módulo PKCS#11 para el DNI e

Este problema puede aparecer en los navegadores Firefox y Netscape. El programa de instalación deja el instalador del módulo criptográfico PKCS#11 en el directorio c:\DNIe\ con el nombre *instalac.htm* 

Para solucionar este problema deberá abrir el navegador (Netscape y/o FireFox) y después arrastrar y soltar el fichero *instalac.htm* sobre el navegador abierto y seguir los pasos que se indican.

Para verificar que se ha instalado el certificado raíz seguir los pasos indicados en el apartado *Cómo sé que está bien instalado*. Si tiene problemas intente realizar la instalación forzando la importación del certificado desde el navegador:

us certificados	Personas	Servidores	Autoridades	Otros			
Tiene certifica	dos archiva	dos que ider	tifican a esta:	s autoridades c	ertificadoras:		
Nombre del o	ertificado				Dispositiv	vo de seguri	₽.
E DIRECCIO	N GENERAL	DE LA POLIC	IIA				~
0C DG	0.001	2.2	14.2		Disp soft	wara da cadu	~
<u>V</u> er	Editar	I <u>m</u>	portar	Exportar	Elimina <u>r</u>		
	, <u> </u>						

Pulse sobre **"Importar"**, e incorpórelo desde la carpeta C:\DNIe haciendo doble clic sobre : ACRAIZ\_CERTIFICATE\_AND\_CRL\_SIGNING\_SHA1.crt





OFICINA TÉCNICA DNI-E

Descargando certificado	<
Se le ha pedido que corfíe en una nueva Autoridad Certificadora (CA).	
¿Quiere confiar en "AC RAIZ DNIE" para los siguientes propósitos?	
🗹 Confiar en esta CA para identificar sitios web.	
🗹 Confiar en esta CA para identificar usuarios de correo.	
🗹 Confiar en esta CA para identificar desarrolladores de software.	
Antes de confiar en esta CA para cualquier propósito, debe examinar el certificado, política y procedimientos de la CA (si están disponibles). Ver Examinar certificado de CA Caceptar Cancelar	

Establezca la confianza y pulse aceptar, el Certificado Raíz (AC RAIZ DNIE) se habrá incorporado al almacén de certificados de Firefox.

## Quiero usar el DNI e pero soy diferente usuario que el que instaló el módulo criptográfico

La instalación del módulo criptográfico del DNIe se estructura de la siguiente manera:

- Módulo CSP: para Microsoft
- Módulo PKCS#11: para Netscape y Firefox
- Certificado Raíz: para Microsoft, Netscape y Firefox

Cuando un nuevo usuario quiere usar el DNIe en un PC que ya tiene instalado el módulo criptográfico DNIe tendrá que configurar su(s) navegador(es):

#### **Internet Explorer**

El usuario únicamente tendrá que instalar el Certificado Raíz. Para instalarlo deberá seguir los pasos que se indican en el apartado *No puedo visualizar el certificado raíz AC RAIZ DNIE*.

#### Netscape y/o Firefox

El usuario tendrá que realizar dos tareas:

• tendrá que instalar el Certificado Raíz. Para instalarlo deberá seguir los pasos que se indican el apartado *No puedo visualizar el certificado raíz ACRAIZ DNIE.* 

• tendrá que configurar el Dispositivo de Seguridad. Para configurarlo deberá seguir los pasos que se indican en el apartado *No puedo visualizar el módulo PKCS#11 para el DNIe*.