

**REGISTRO DE LAS  
AUTORIDADES DE  
CERTIFICADOS RAÍZ Y  
SUBORDINADAS DEL  
DNI-E EN  
INTERNET EXPLORER**

**CENTRO DE RESPUESTA A INCIDENTES DE  
SEGURIDAD (INTECO-CERT)**

## 1. INTRODUCCIÓN

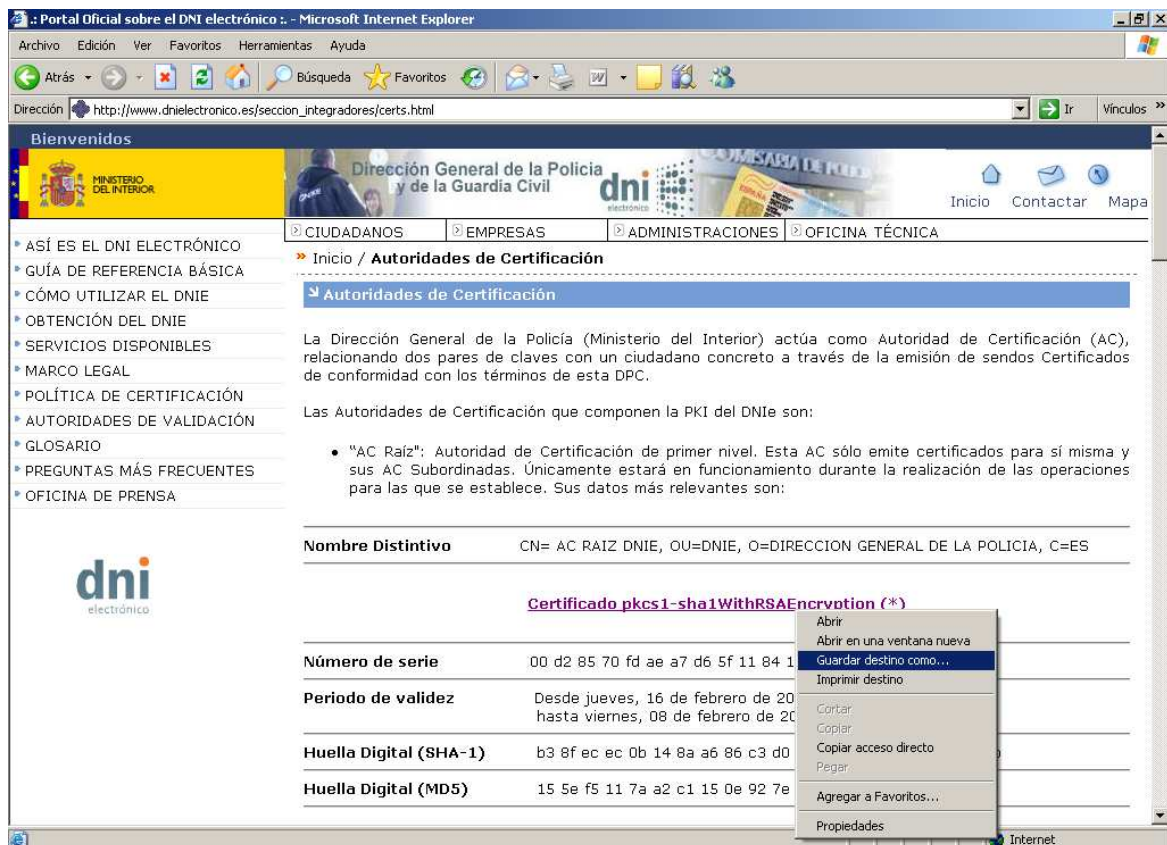
### Registro de las Autoridades de Certificación Raíz y Subordinadas del DNIE en Internet Explorer

Esta guía es válida si se dispone de un Sistema Operativo Microsoft (98, ME, 2000, XP, o posterior).

Para utilizar las aplicaciones que requieren firma electrónica se debe registrar en el navegador el Certificado Raíz de la Dirección General de la Policía:

- 1) Para ello se deberá descargar el Certificado desde la página de la D.G. de la Policía:

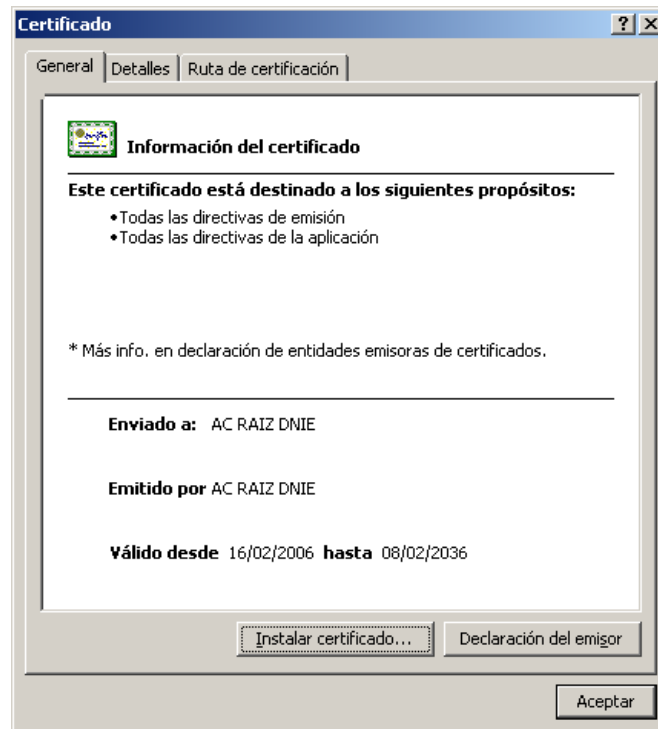
[http://www.dnielectronico.es/seccion\\_integradores/certs.html](http://www.dnielectronico.es/seccion_integradores/certs.html)



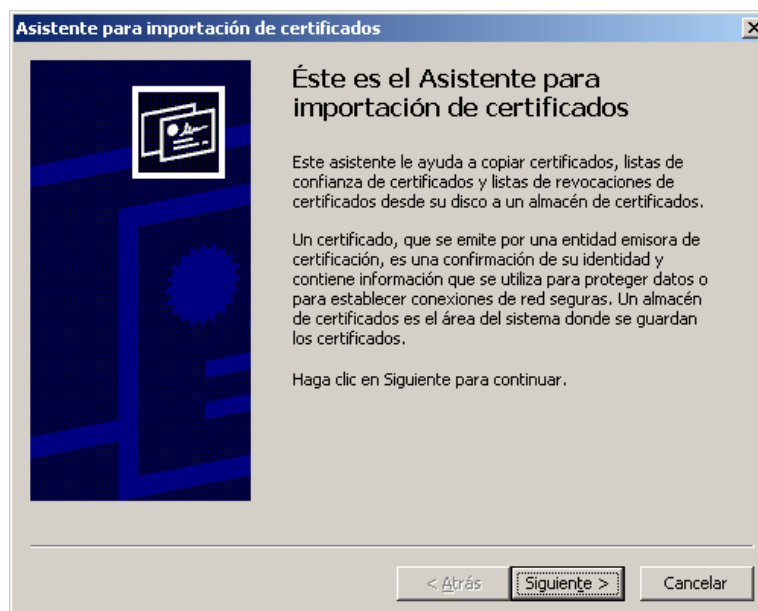
Se recomienda guardar el fichero con extensión ZIP que contiene Certificado Raíz de la D.G. de la Policía, para poder instalarlo posteriormente.

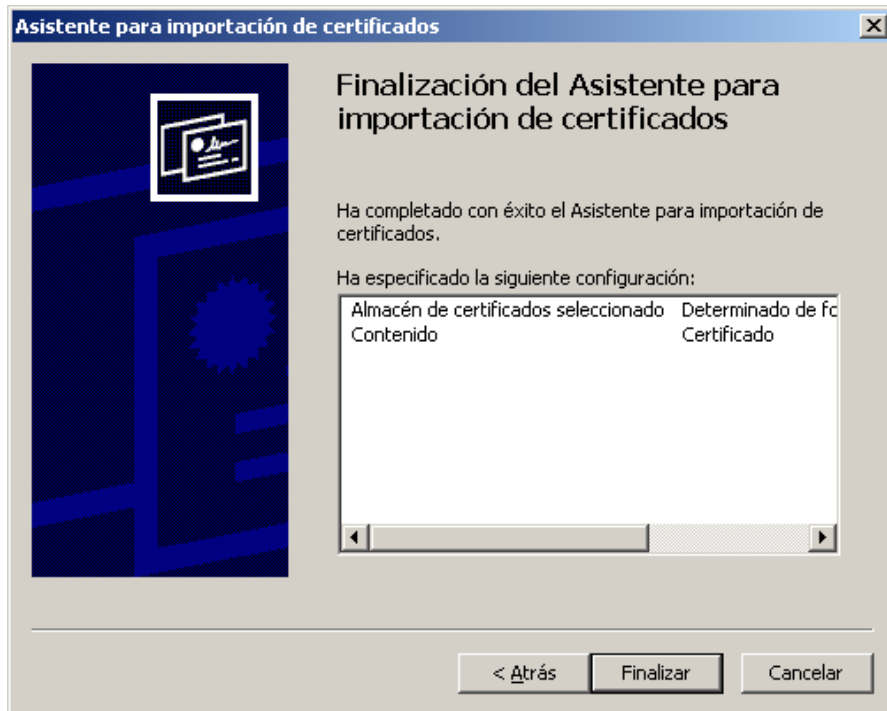
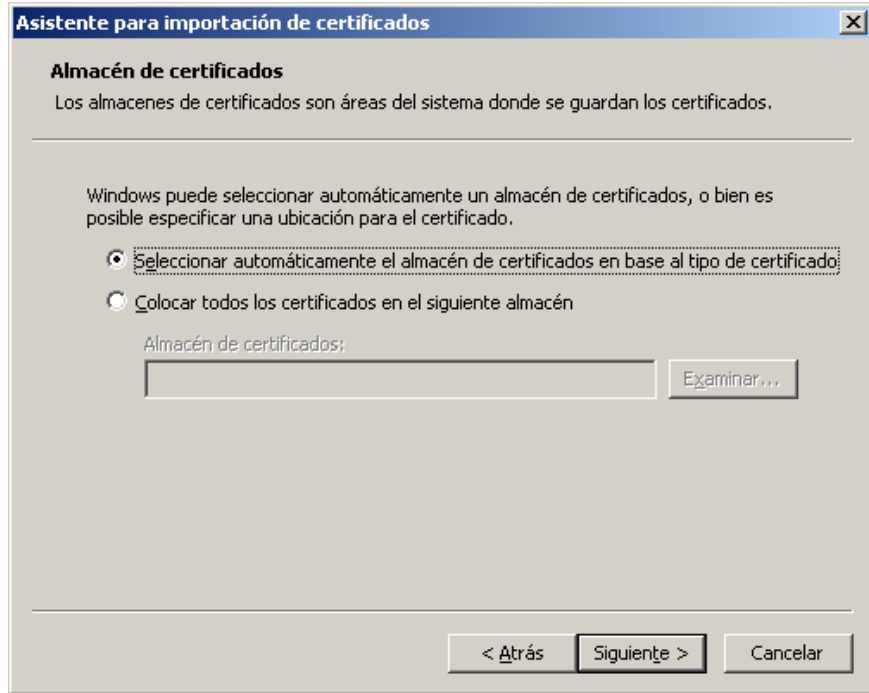
- 2) Seguidamente se descomprime el fichero y se ejecuta:

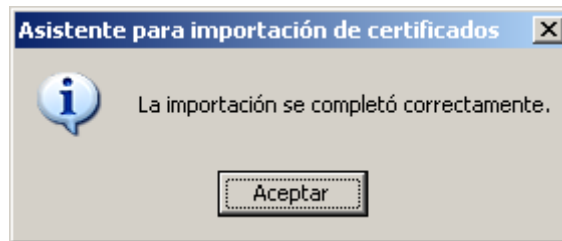
Automáticamente aparecerá la siguiente pantalla, donde se deberá pulsar la opción de "Instalar certificado..."



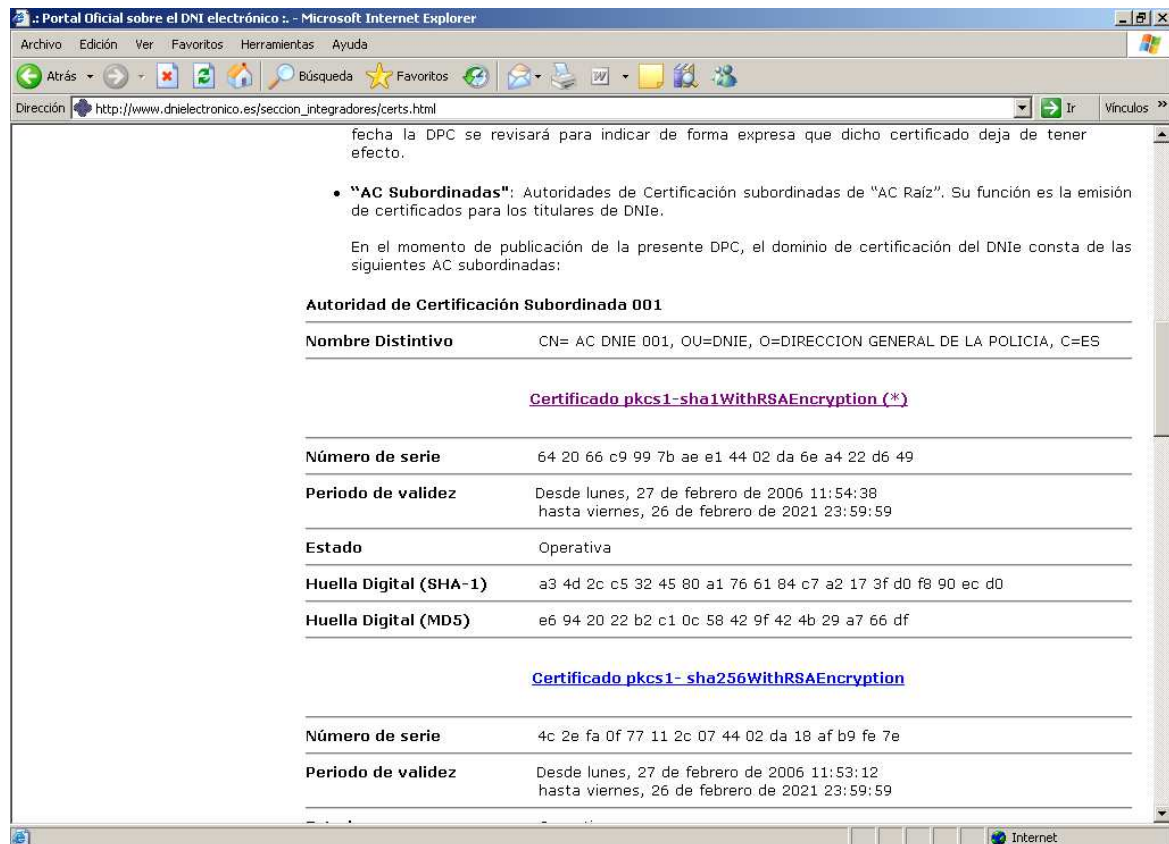
3) Seguidamente el Asistente para la Importación de Certificados guiará los diferentes pasos a seguir, y que se indican a continuación.







- 4) Será necesario repetir los pasos para las Autoridades de Certificación Subordinadas que aparecen en la página de la D.G. de la Policía, indicada en el paso 1:



- 5) Finalmente habrá que comprobar que los certificados se han registrado correctamente en el repositorio de Internet Explorer.

Para ello, desde Internet Explorer, seleccionando Herramientas, Opciones de Internet, Contenido, Certificados:

- En la pestaña de “Entidades emisoras de certificados de raíz de confianza” debe figurar: “AC RAIZ DNIE”
- En la pestaña de “Entidades emisoras de” debe figurar “AC RAIZ DNIE” con el número correspondiente a la Autoridad de Certificación Subordinada:

**Certificados** [?] [X]

Propósito planteado: <Todos>

Entidades emisoras de certificados intermedias | Entidades emisoras raíz de confianza | Edit [◀] [▶]

Emitido para	Emitido por	Fecha de...	Nombre descriptivo
ABA.ECOM Root CA	ABA.ECOM Root CA	09/07/2009	DST (ABA.ECOM...
AC RAIZ DNIE	AC RAIZ DNIE	08/02/2036	<ninguno>
Autoridad Certifica...	Autoridad Certificador...	28/06/2009	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	29/06/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	03/07/2009	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	21/01/2010	Belgacom E-Trus...
CBW HKT SecureN...	CBW HKT SecureNet ...	16/10/2009	CW HKT Secure...
CBW HKT SecureN...	CBW HKT SecureNet ...	16/10/2009	CW HKT Secure...
CBW HKT SecureN...	CBW HKT SecureNet ...	16/10/2010	CW HKT Secure...

[Importar...] [Exportar...] [Quitar] [Avanzadas...]

Propósitos planteados del certificado  
<Todos>

[Ver]

[Cerrar]

**Certificados** [?] [X]

Propósito planteado: <Todos>

Entidades emisoras de certificados intermedias | Entidades emisoras raíz de confianza | Edit [◀] [▶]

Emitido para	Emitido por	Fecha de...	Nombre descriptivo
AC DNIE 001	AC RAIZ DNIE	26/02/2021	<ninguno>
Epson Iberica, S.A.	Epson Iberica, S.A.	05/08/2005	<ninguno>
Epson Iberica, S.A.	Epson Iberica, S.A.	06/08/2013	<ninguno>
FWInternet	FWInternet	24/09/2005	<ninguno>
GlobalSign Root CA	Root SGC Authority	28/01/2014	<ninguno>
GTE CyberTrust Root	Root SGC Authority	23/02/2006	<ninguno>
Indra	Indra	09/06/2005	<ninguno>
INDRA AC Corpora...	INDRA AC Raiz	16/06/2019	<ninguno>
INDRA AC Raiz	INDRA AC Raiz	16/06/2034	<ninguno>

[Importar...] [Exportar...] [Quitar] [Avanzadas...]

Propósitos planteados del certificado  
<Todos>

[Ver]

[Cerrar]

**Nota:** El certificado con algoritmo de firma pkcs1-sha1WithRSAEncryption se publica por razones de interoperabilidad, para facilitar a aquellos sistemas y aplicaciones que no soporten pkcs1-sha256WithRSAEncryption, construir la cadena de confianza en los procesos de validación de certificados y firma. Estos sistemas y aplicaciones tienen un plazo máximo de dos años para realizar las adaptaciones que sean necesarias para soportar dicho algoritmo. A partir de esa fecha la Declaración de Prácticas de Certificación del DNle se revisará para indicar de forma expresa que dicho certificado deja de tener efecto.