

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

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

1. INTRODUCCIÓN

Registro de las Autoridades de Certificación Raíz y Subordinadas del DNIE en Firefox

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



Portal Oficial sobre el DNI electrónico : Autoridades de Certificación - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://www.dnielectronico.es/seccion_integradores/certs.html

Personalizar vínculos

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Bienvenidos

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR CUERPO NACIONAL DE POLICÍA dni DNI ELECTRÓNICO Inicio Contactar Mapa

CIUDADANOS EMPRESAS ADMINISTRACIONES OFICINA TÉCNICA

Inicio / Oficina Técnica / Autoridades de Certificación

Autoridades de Certificación

La Dirección General de la Policía (Ministerio del Interior) actúa como Autoridad de Certificación (AC), relacionando dos pares de claves con un ciudadano concreto a través de la emisión de sendos Certificados de conformidad con los términos de esta DPC.

Las Autoridades de Certificación que componen la PKI del DNIE son:

- "AC Raíz": Autoridad de Certificación de primer nivel. Esta AC sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece. Sus datos más relevantes son:

Nombre Distintivo CN= AC RAIZ DNIE, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES

Certificado pkcs1-sha1WithRSAEncryption (*)

Número de serie 00 d2 85 70 fd ae a7 d6 5f 11 84 15 c6 31 b5 cb

Periodo de validez Desde jueves, 16 de febrero de 2006 11:37:25 hasta viernes, 08 de febrero de 2036 23:59:59

Huella Digital (SHA-1) b3 8f ec ec 0b 14 8a a6 86 c3 d0 0f 01 ec c8 84 8e 80 85 eb

Huella Digital (MD5) 15 5e f5 11 7a a2 c1 15 0e 92 7e 66 fe 3b 84 c3

Certificado nkcs1-sha256WithRSAEncrvntion

Terminado

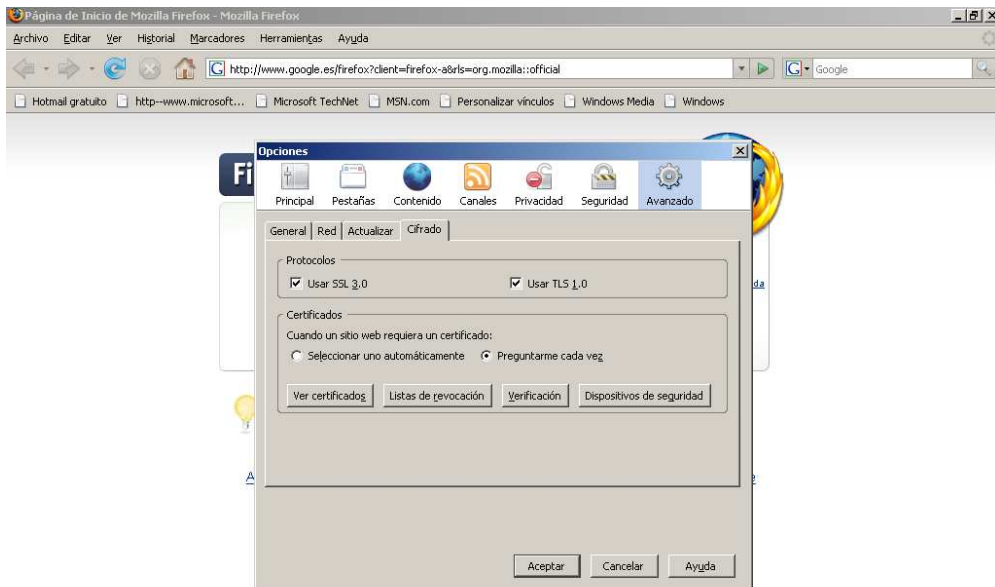
Se recomienda guardar el fichero que contiene Certificado Raíz de la D.G. de la Policía, para poder instalarlo posteriormente. El certificado está tanto con SHA-1 como con SHA-256 (ver nota al final del documento)

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

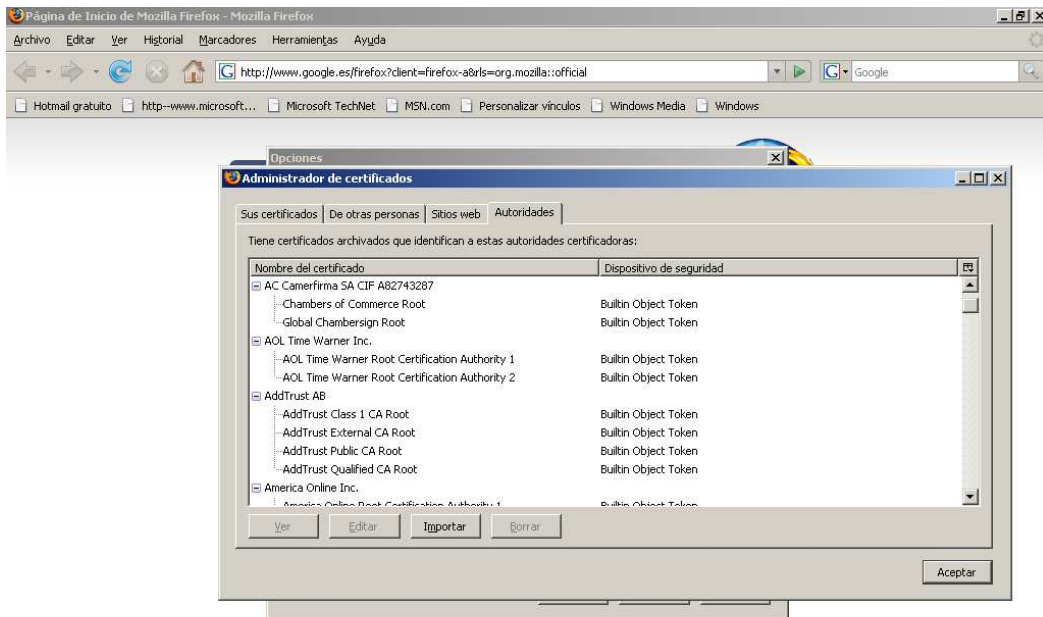
3) Se abre Firefox y se escoge en el Menú “Herramientas” el enlace “Opciones”.



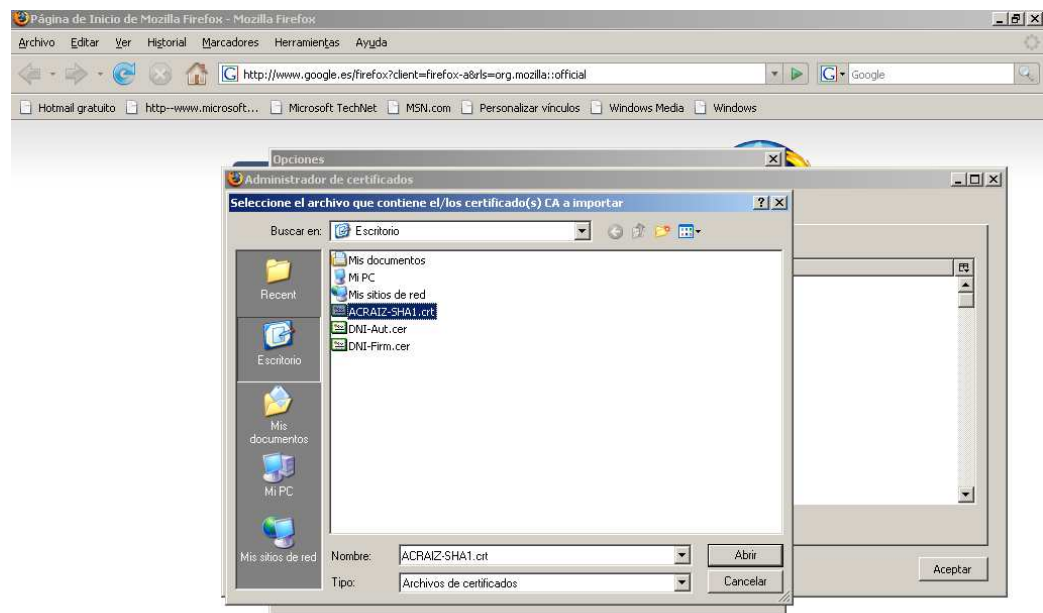
4) Dentro de “Opciones” se escoge la pestaña “Cifrado” y se pulsa el botón “Ver Certificados”.



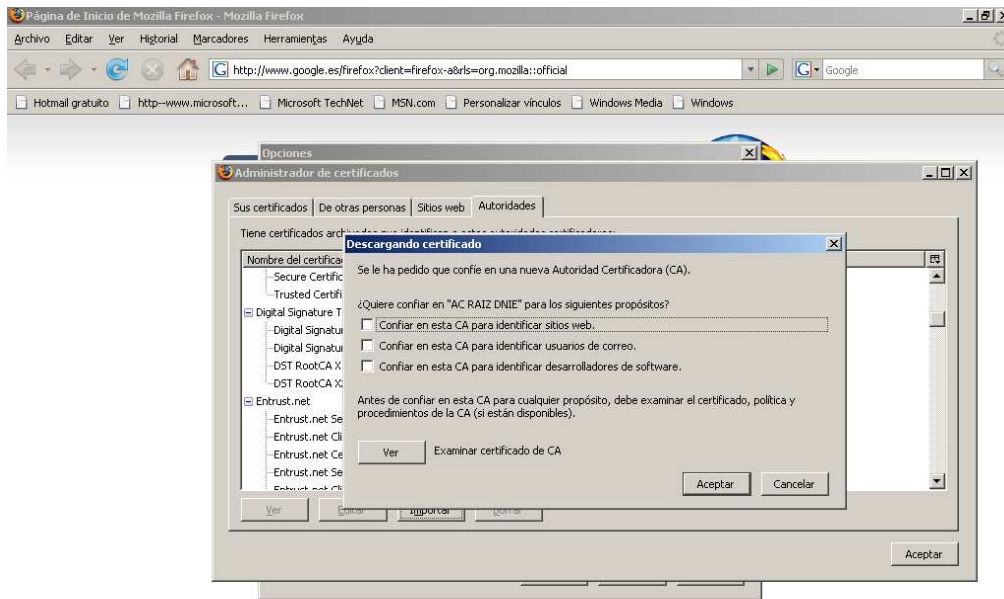
5) Se escoge la pestaña “Autoridades” y se pulsa el botón “Importar”.



6) Se selecciona el certificado raíz en la carpeta en que se haya guardado y se pulsa “Abrir”.

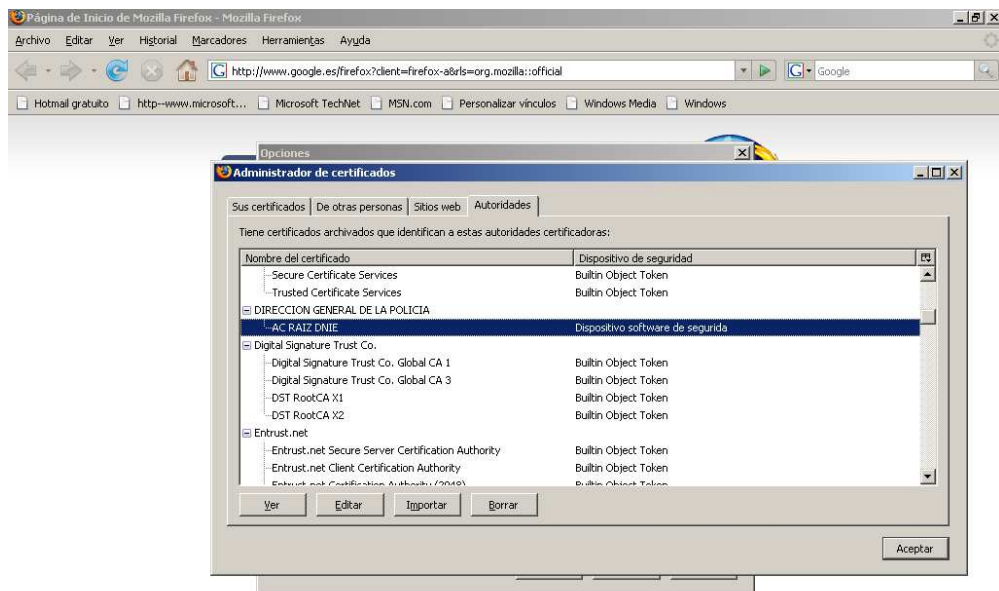


7) Se marca los propósitos para los que se confía, en principio pueden ser los tres, y se pulsa “Aceptar”.



Terminado

8) Se visualiza en la relación de Autoridades que se ha incorporado la “AC RAIZ DNIE” de la Dirección General de la Policía.



JavaScripts actualmente prohibidos [

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.