

**REGISTRO DE LAS
AUTORIDADES DE
CERTIFICADOS RAÍZ Y
SUBORDINADAS DEL
DNI-E EN EL SERVIDOR WEB
INTERNET INFORMATION
SERVER**

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

ÍNDICE

1.	INTRODUCCIÓN	3
2.	INSTALACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN RAÍZ Y SUBORDINADAS DEL DNIE	4
3.	CONFIGURACIÓN DEL INTERNET INFORMATION SERVER	10

1. INTRODUCCIÓN

Registro de las Autoridades de Certificación Raíz y Subordinadas del DNle en el Servidor Web Internet Information Server

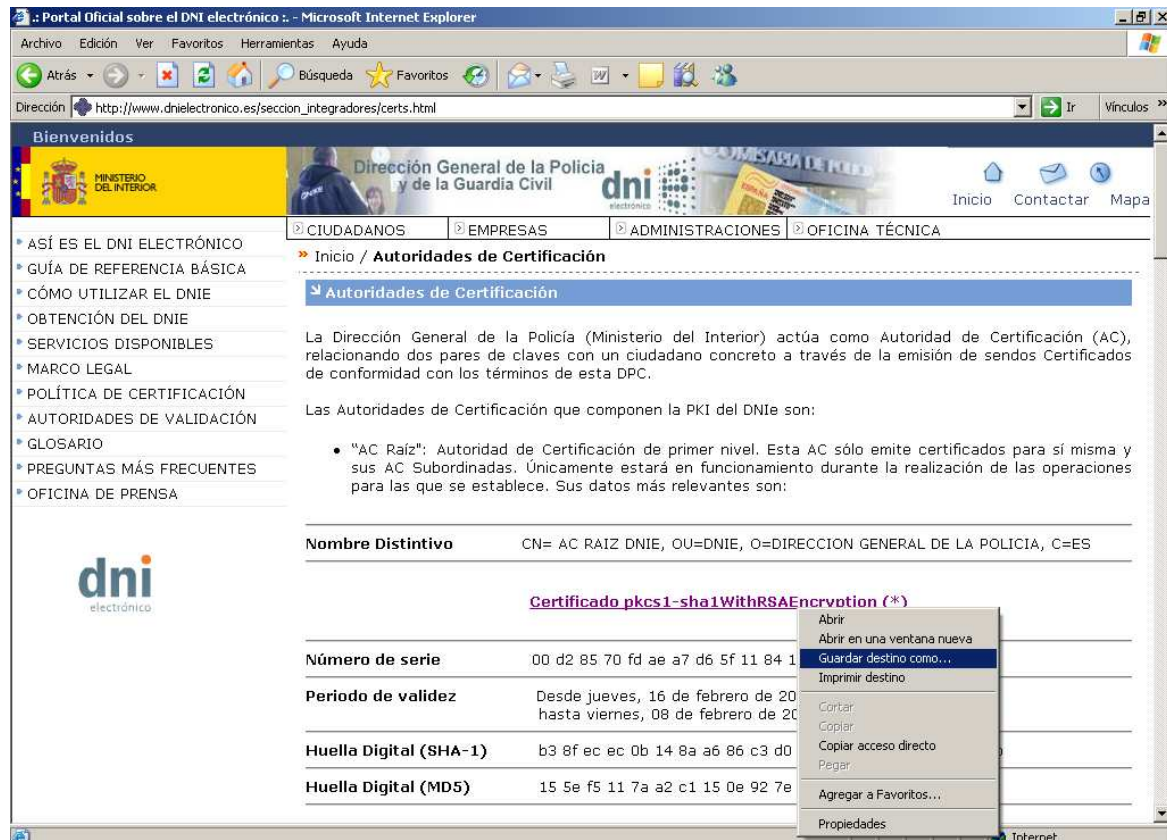
Este documento describe el procedimiento a seguir para configurar el servidor web IIS (Internet Information Server) para admitir transmisiones seguras de información por parte de un cliente con un DNle válido.

El proceso consta de dos acciones a realizar sobre el servidor y la configuración del IIS. La primera consiste en la importación de los certificados raíz y subordinados en el servidor. La segunda, en la modificación de las políticas de acceso del IIS.

2. INSTALACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN RAÍZ Y SUBORDINADAS DEL DNIe

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



Bienvenidos

Dirección General de la Policía y de la Guardia Civil

Inicio / **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
Número de serie	00 d2 85 70 fd ae a7 d6 5f 11 84 1
Periodo de validez	Desde jueves, 16 de febrero de 20 hasta viernes, 08 de febrero de 20
Huella Digital (SHA-1)	b3 8f ec ec 0b 14 8a a6 86 c3 d0
Huella Digital (MD5)	15 5e f5 11 7a a2 c1 15 0e 92 7e

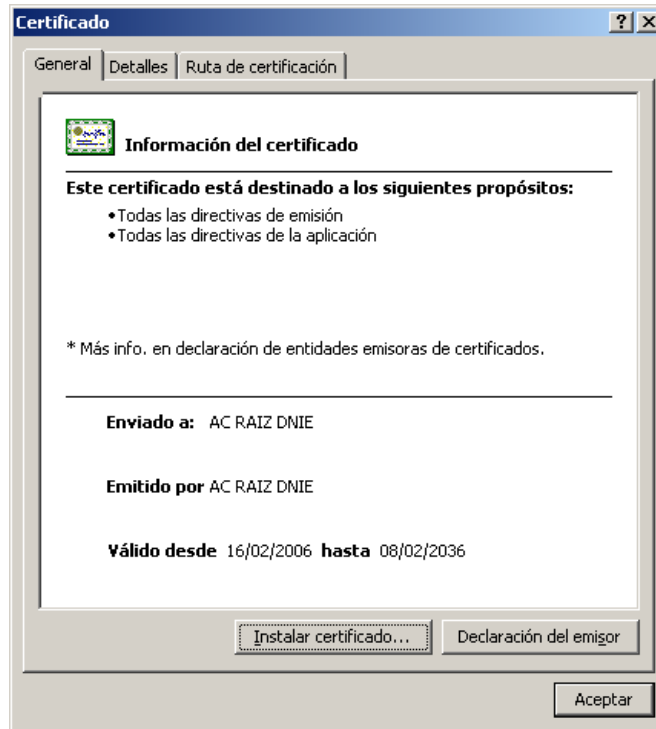
Certificado pkcs1-sha1WithRSAEncrvotn (*)

Guardar destino como...

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

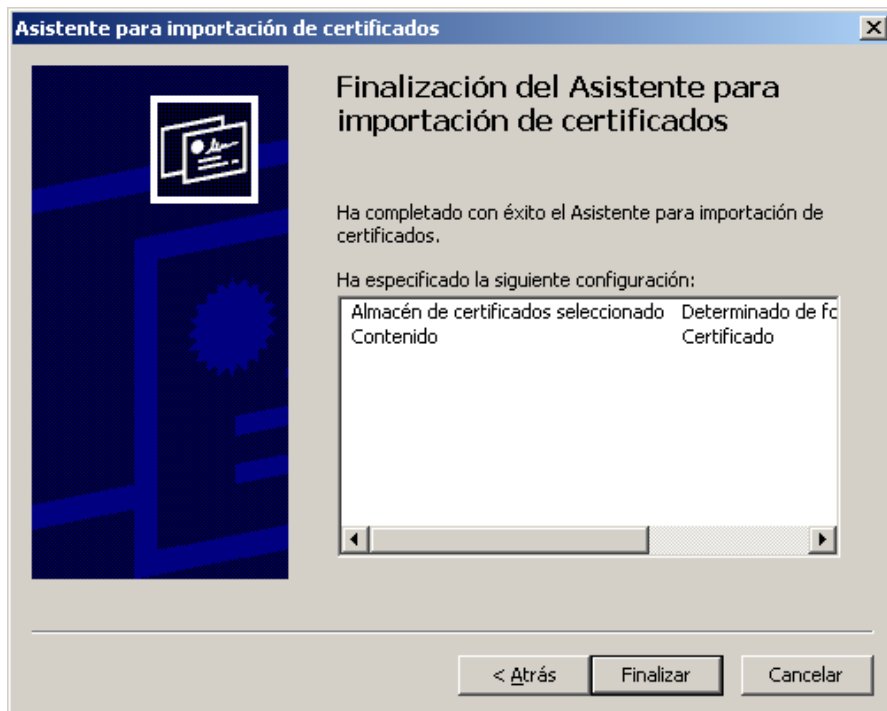
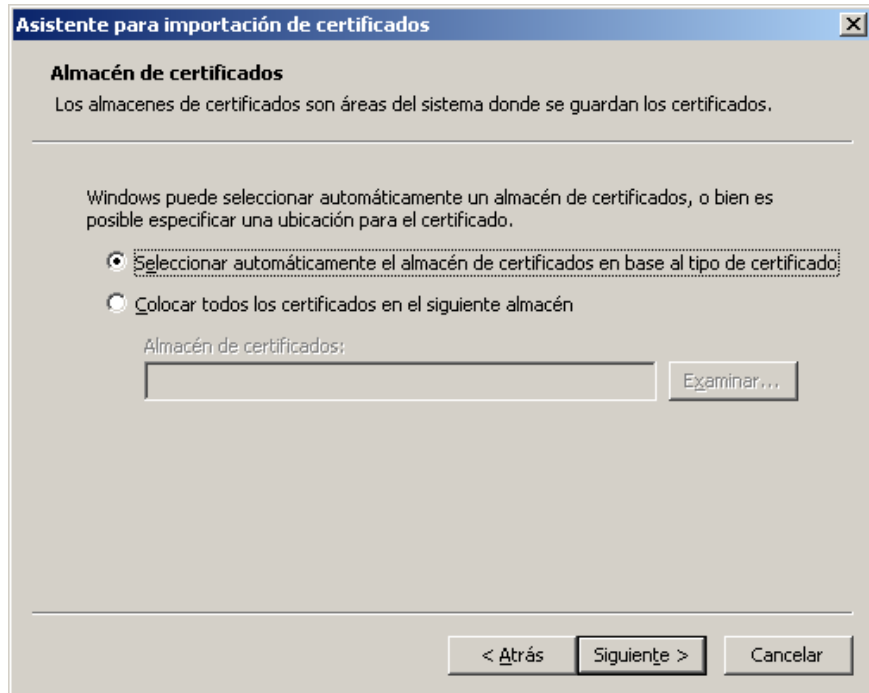
2) Seguidamente se descomprime el fichero y se ejecuta:

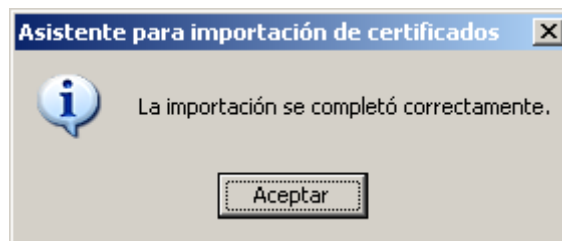
Automáticamente aparecerá la siguiente pantalla, donde se deberá pulsar la opción de "Instalar certificado..."



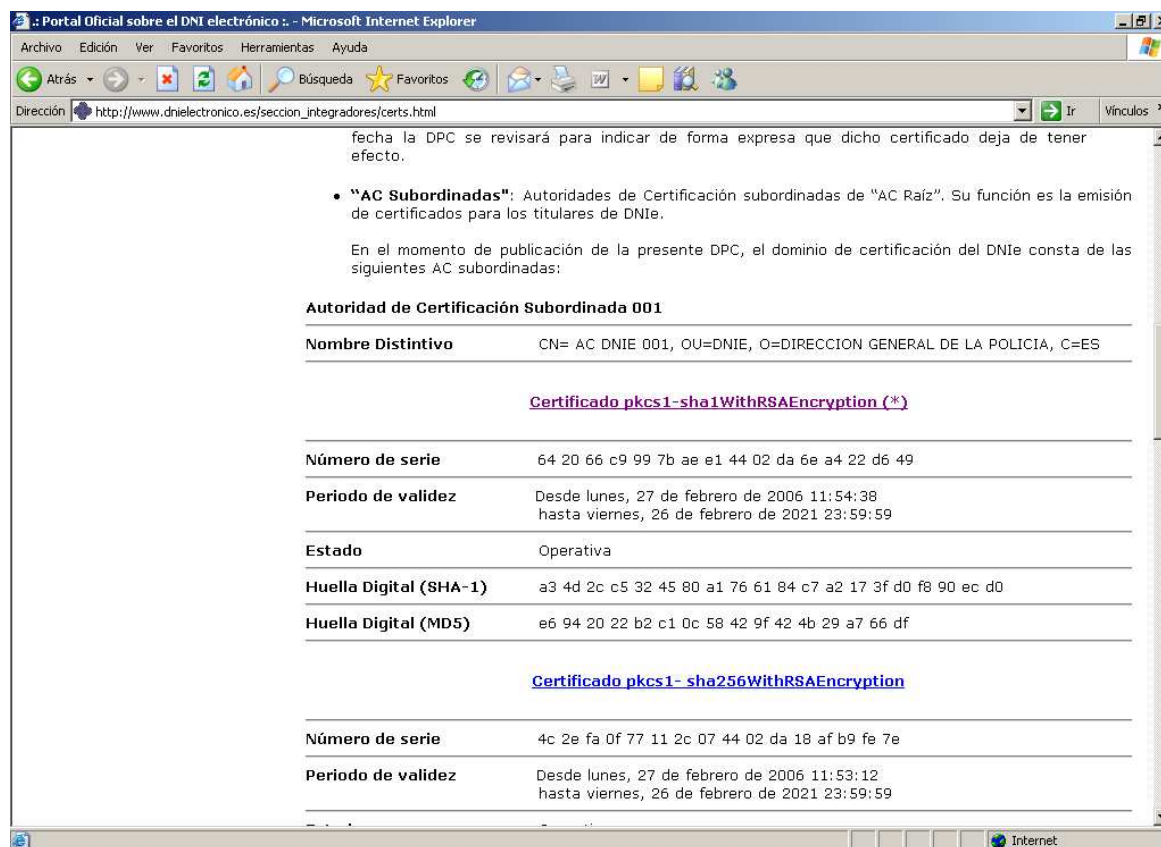
3) Seguidamente el Asistente para la Importación de Certificados guiará los diferentes pasos a seguir, y que se indican a continuación.







- 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
USA E-COM Root CA	USA E-COM Root CA	05/07/2009	DST (USA E-COM...
AC RAIZ DNIE	AC RAIZ DNIE	08/02/2006	<ninguno>
Autoridad Certific...	Autoridad Certificad...	29/06/2008	Autoridad Certifi...
Autoridad Certific...	Autoridad Certificad...	29/06/2008	Autoridad Certifi...
Baltimore E2 by DST	Baltimore E2 by DST	03/07/2009	DST (Baltimore E...
Belgacom E-Trust F...	Belgacom E-Trust Pres...	23/01/2010	Belgacom E-Trust...
CW HKT SecureNet...	CW HKT SecureNet ...	16/10/2009	CW HKT Secure...
CW HKT SecureNet...	CW HKT SecureNet ...	16/10/2009	CW HKT Secure...
CW HKT SecureNet...	CW 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 Densco, S.A.	Epson Densco, S.A.	05/07/2005	<ninguno>
Epson Densco, S.A.	Epson Densco, S.A.	05/08/2013	<ninguno>
FujiNetwork	FujiNetwork	24/04/2005	<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 Rac	14/06/2019	<ninguno>
INDRA AC Rac	INDRA AC Rac	14/06/2019	<ninguno>

Importar... | Exportar... | Quitar | Avanzadas...

Propósitos planteados del certificado

<Todos>

Ver

Cerrar



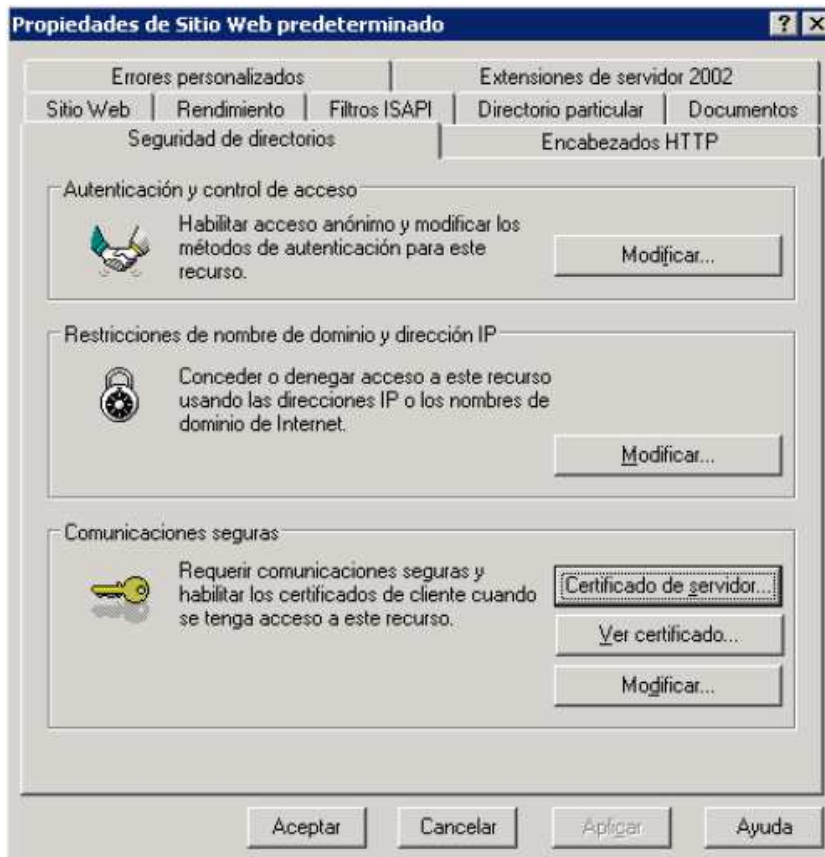
Instituto Nacional
de Tecnologías
de la Comunicación

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.

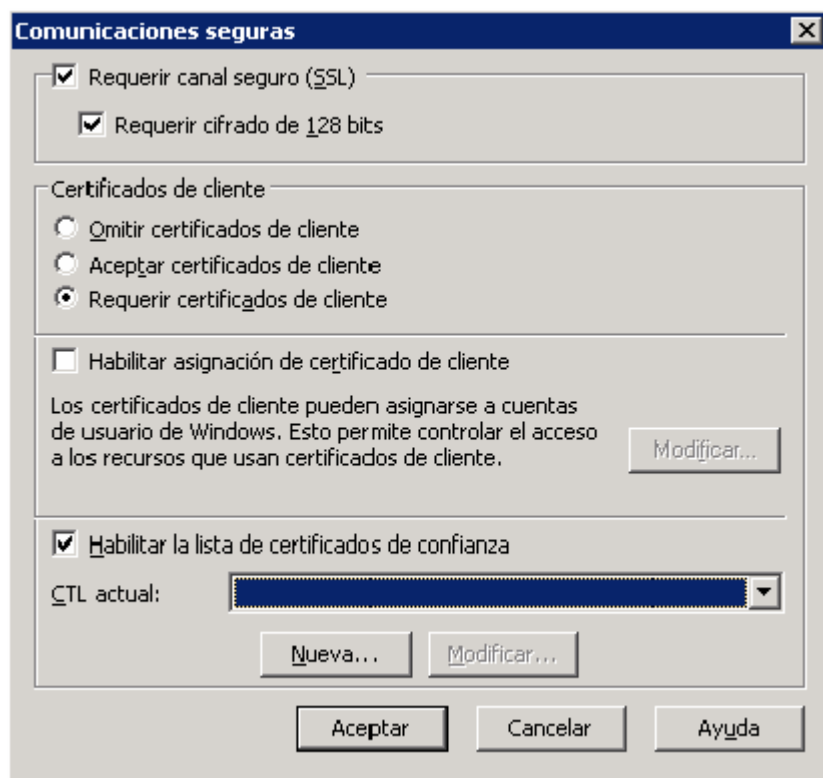
3. CONFIGURACIÓN DEL INTERNET INFORMATION SERVER

Una vez cargadas las claves públicas, habrá que configurar la instancia del servidor web en la que se quiere activar la autenticación del cliente utilizando el DNle.

- 1) Para conseguirlo habrá que entrar en las propiedades del “Sitio Web”, concretamente en la pestaña de “Seguridad de directorios”.




- 2) Si el certificado está bien instalado, dentro del apartado de “Comunicaciones seguras”, el botón “Modificar” estará activado. Pulsándolo podremos modificar los parámetros de configuración relativos a la autenticación de cliente, el canal seguro y los certificados de cliente que serán admitidos.



- 3) Dentro de la pantalla de configuración habrá que marcar las opciones tal y como aparecen en la imagen. Tienen que estar activadas las opciones de “Requerir canal seguro (SSL)” y que el cifrado sea de 128 bits. Dentro de los certificados de cliente, activar la opción “Requerir certificados de cliente”. Y por último, se ha de habilitar una lista de certificados de confianza. Esta lista únicamente contiene los certificados raíz de las Autoridades de Certificación en las que se confía. Es muy importante haber cargado las claves públicas, ya que el certificado de usuario cuelga de una Autoridad intermedia y el IIS al no ser capaz de reconstruir la cadena de confianza, la autenticación fallará.

Asistente para crear lista de certificados de confianza



Éste es el Asistente para lista de certificados de confianza

Este asistente le ayuda a crear una lista de certificados de confianza o a modificar una lista existente.

Una lista de certificados de confianza (CTL) es una lista firmada de certificados de entidades emisoras de certificación (CA) de raíz que han sido acreditados por un administrador.

Haga clic en Siguiente para continuar.

< Atrás **Siguiente >** Cancelar

Asistente para crear lista de certificados de confianza

Certificados en la lista de certificados de confianza (CTL)

Los certificados que se muestran en la siguiente tabla están actualmente en la CTL.

Certificados de la CTL actual:

Emitido para	Emitido por	Propósitos planteados

Agregar desde el almacén **Agregar desde archivo** Quitar Ver certificado

< Atrás **Siguiente >** Cancelar

Asistente para crear lista de certificados de confianza

Certificados en la lista de certificados de confianza (CTL)

Los certificados que se muestran en la siguiente tabla están actualmente en la CTL.

Certificados de la CTL actual:

Emitido para	Emitido por	Propósitos planteados
AC RAIZ DNIE	AC RAIZ DNIE	<Todos>

Agregar desde el almacén Agregar desde archivo Quitar Ver certificado

< Atrás **Siguiente >** Cancelar

Asistente para crear lista de certificados de confianza

Nombre y descripción

El nombre de CTL y la descripción le ayudan a distinguir dicha CTL de otras.


Escriba un nombre descriptivo y una descripción para la nueva CTL.

Nombre descriptivo:

Descripción:

< Atrás **Siguiente >** Cancelar

Asistente para crear lista de certificados de confianza



Finalización del Asistente para lista de confianza de certificados

Ha completado correctamente el Asistente para lista de confianza de certificados.

Ha seleccionado la siguiente configuración:

Propósito	Autenticación del cliente
Identificador	1.3.6.1.4.1.311.30.1
Validez	{46E03954-52FF-4802-B3C9-6B1}
Nombre descriptivo	<ninguno>
Descripción	Nueva CTL de IIS
	Esta CTL se va a usar como lista c

< Atrás **Finalizar** Cancelar