Agencia de Tecnología y Certificación Electrónica

Petición de certificados de servidor con IIS

Tabla de Contenido

1. Introducción

1.1. Objeto

Descripción de los pasos a seguir para la generación de una petición de certificado de servidor Web e instalación de la respuesta utilizando el software Internet Information Server (en adelante IIS) de Microsoft.

1.2. Ámbito y deber de lectura

El ámbito de este documento es la generación de una petición de certificado de servidor Web e instalación de la respuesta utilizando el software IIS de Microsoft.

Todos los administradores que deseen obtener un certificado de servidor acorde a la Política de Certificación para Servidores con soporte SSL, disponible en http://www.accv.es/administracion-publica/certificados/servidor-con-soporte-ssl/.

1.3. Clasificación

La información contenida en este documento se ha clasificado como: **PUBLICO**

1.4. Referencias

- Internet Information Services (IIS)
    - http://technet.microsoft.com/es-es/library/cc753433%28WS.10%29.aspx

1.5. Definiciones

No aplicable.

1.6. Listado de apéndices

No aplicable.

2. Desarrollo

2.1. Descripción General

A continuación se detallan los pasos necesarios para la generación de una petición de certificado a partir de IIS (aunque las capturas de pantalla se han efectuado con la versión 5.0, para la 4.0 o 6.0, el proceso es igual), así como a la posterior inserción de la respuesta firmada por la Autoridad de Certificación en el servidor.

Se considera que el administrador tiene conocimientos de IIS, y que el servidor tiene el servidor web configurado correctamente.

2.2. Generación de la petición

PASO 1: Abrir el Administrador de Servicios Internet

Se encuentra en “Inicio -> Programas -> Herramientas Administrativas -> Administrador de Servicios Internet”.

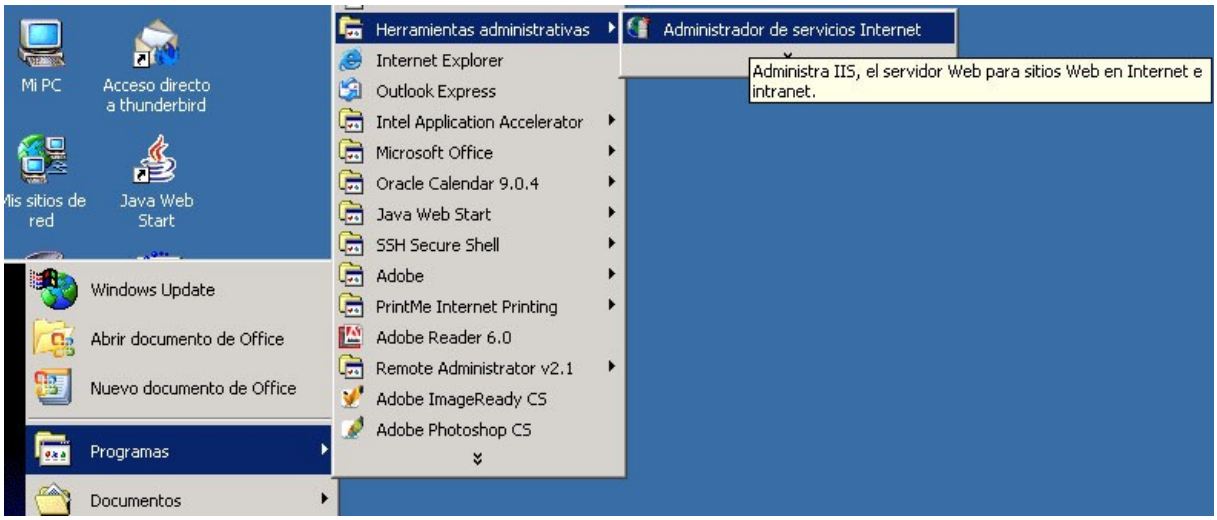

Ilustración 1

PASO2: Abrir las propiedades del sitio web al que queremos generar el certificado.

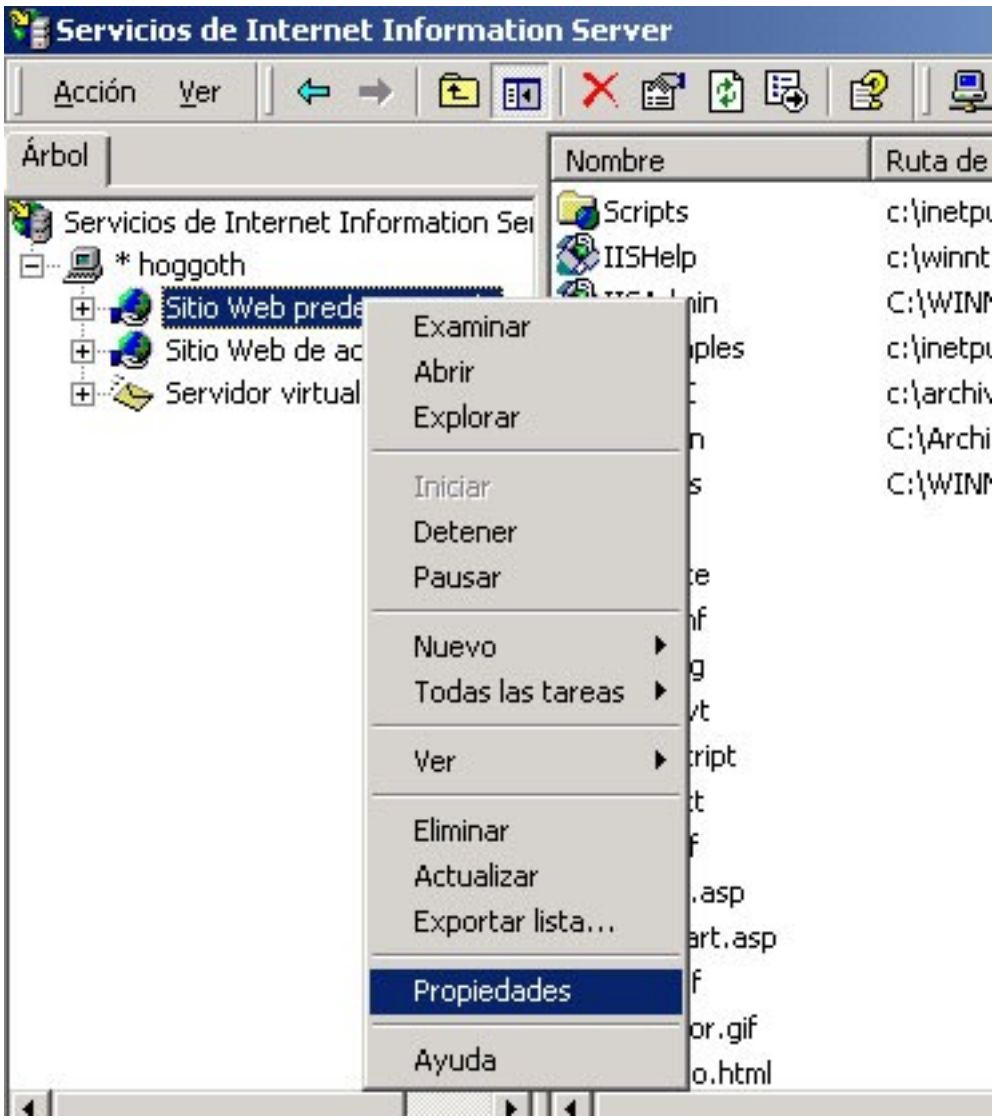

Ilustración 2

PASO 3: Seleccionar la pestaña “Seguridad de Directorios”.

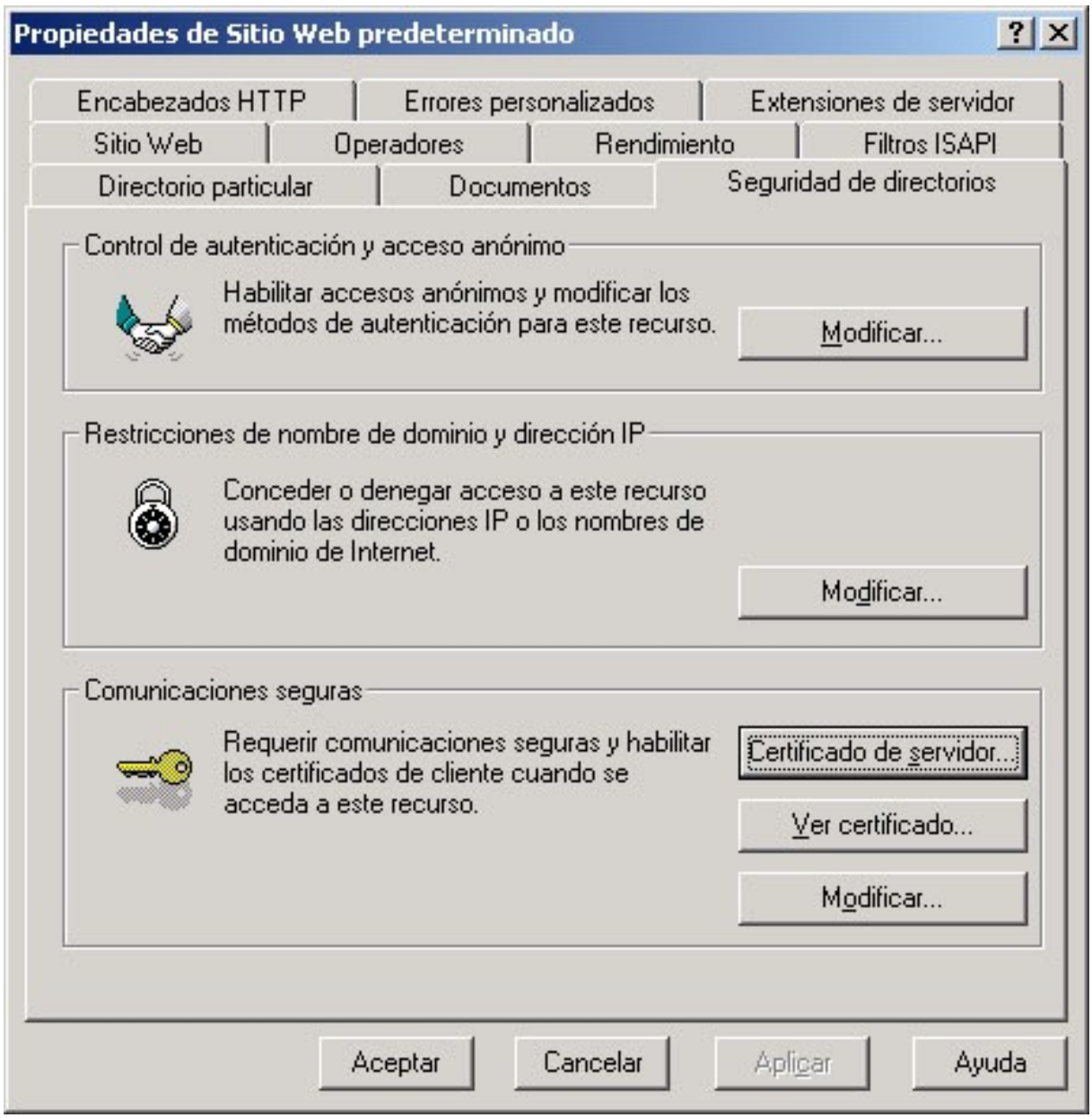

Ilustración 3

PASO 4: Seleccionar “Certificado de Servidor”.

Esto iniciara el “Asistente de certificado de servidor Web”, que debemos completar de la forma que se detalla a continuación:

PASO 4.1: Pantalla informativa. Nos informa si tenemos instalado un certificado, y a partir de ahí que opciones tomar. Si ya hay un certificado instalado, las siguientes pantallas nos dan opciones para gestionarlo, si no hay certificado pero se ha efectuado una petición previa, nos da opciones para instalar la respuesta y si no hay certificado ni petición, nos da opciones para generar una petición nueva. En este punto vamos a considerar la última opción, en la que vamos a efectuar la generación de la petición.

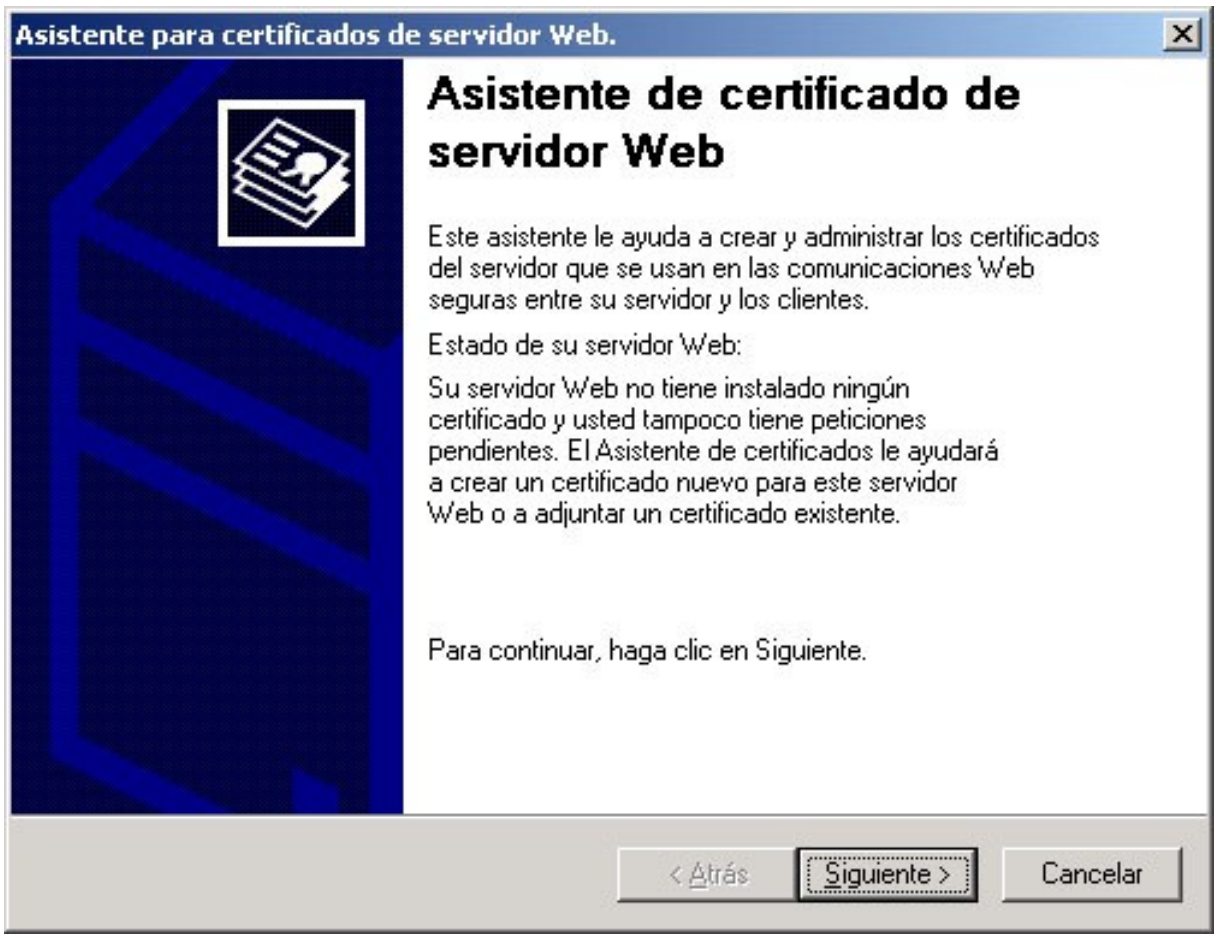

Ilustración 4

PASO 4.2: Seleccionamos “Crear un certificado nuevo”

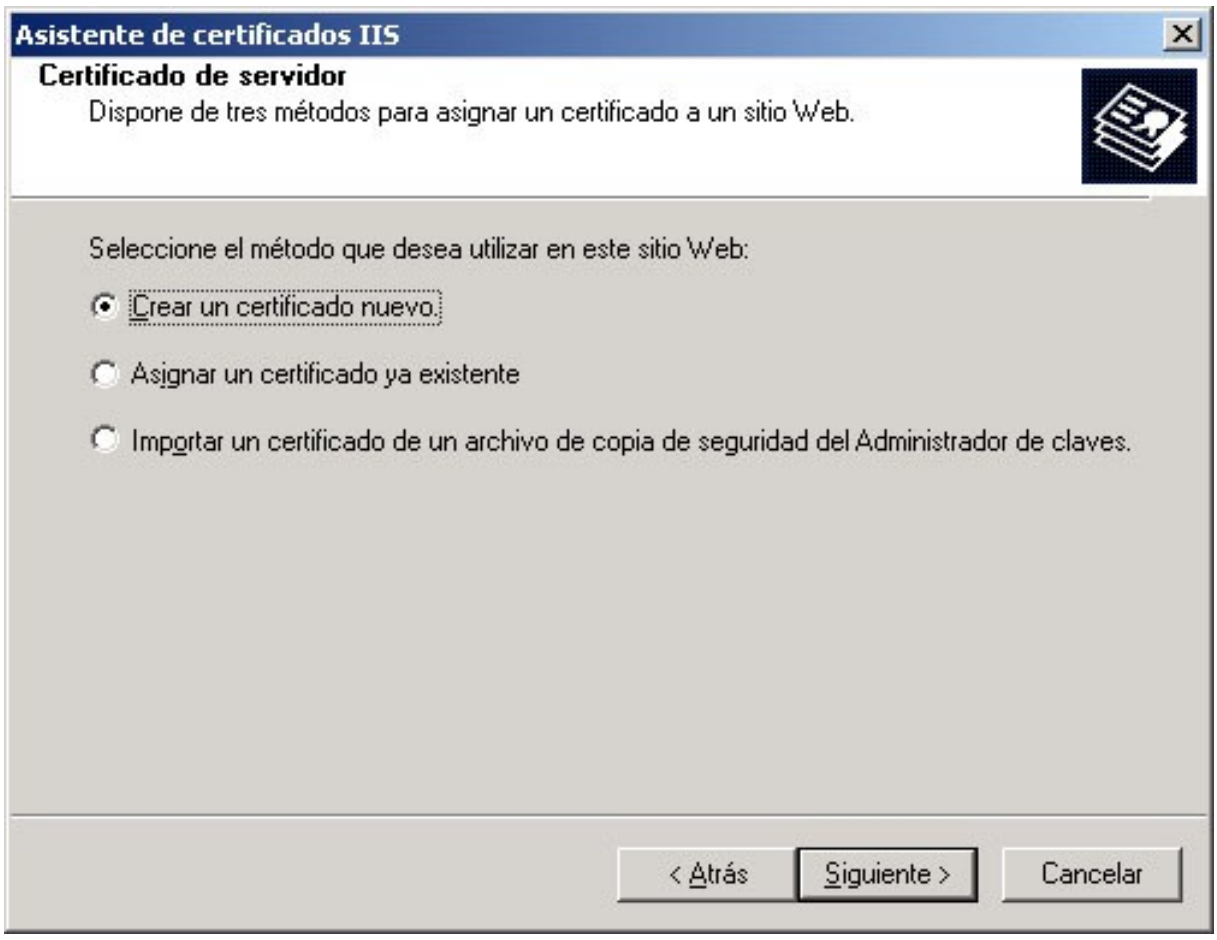

Ilustración 5

PASO 4.3: Seleccionamos “Preparar la petición ahora pero enviarla más tarde”

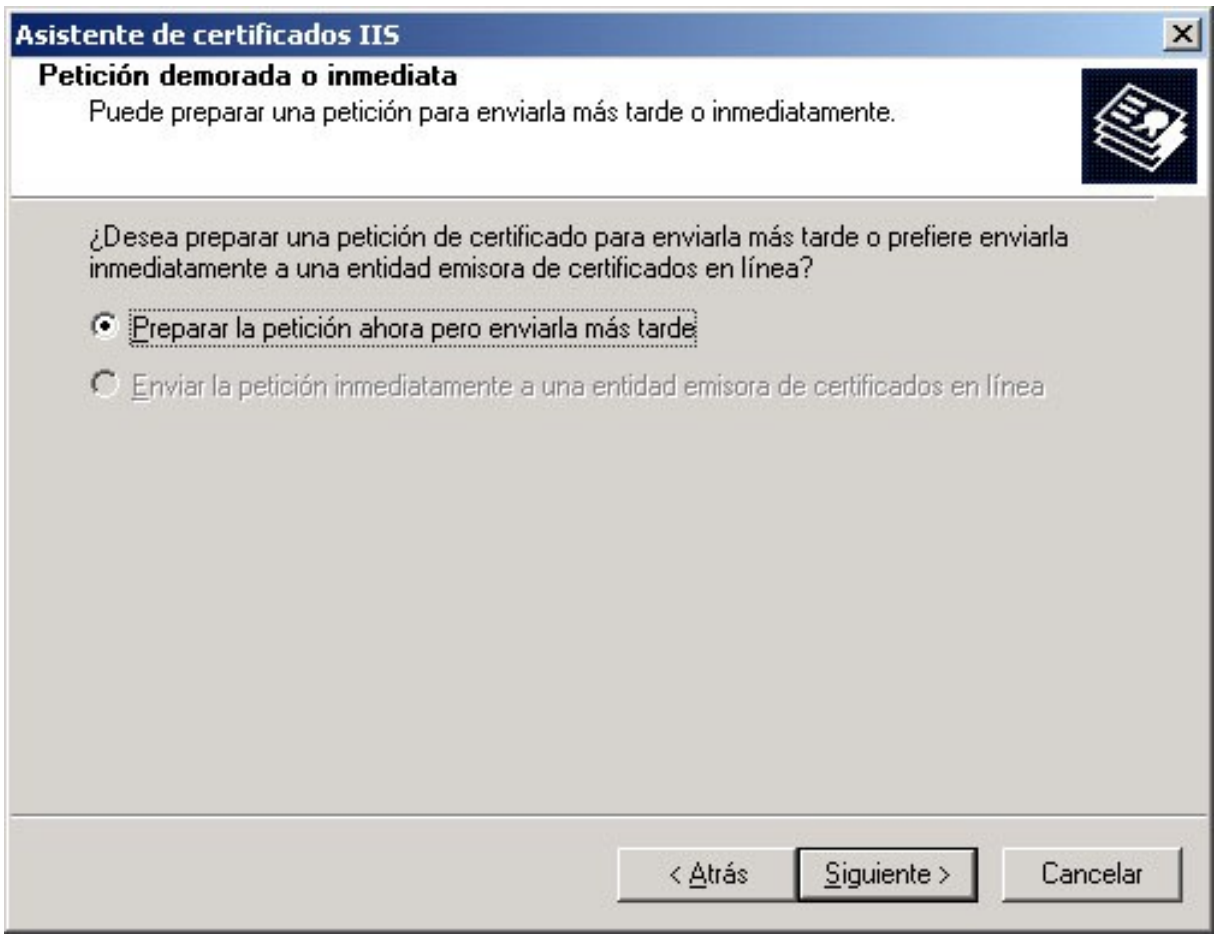

Ilustración 6

PASO 4.4: Nombre y configuración de seguridad

Asignamos un nombre representativo al certificado, siendo utilizado en este caso únicamente a nivel identificativo. Este nombre no se reflejara en los campos del certificado. En esta misma pantalla, seleccionamos el tamaño de la clave, eligiendo 1024 bits.

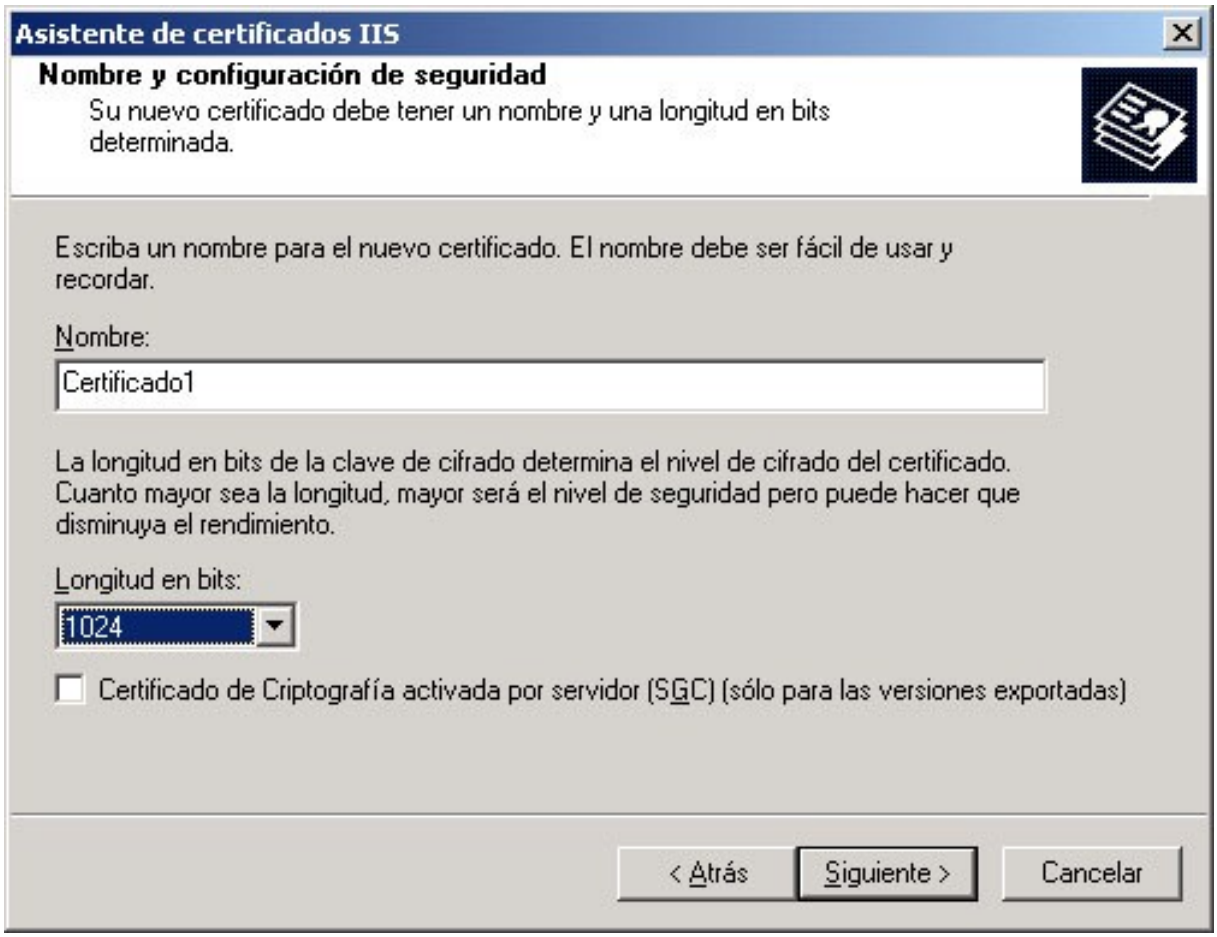

Ilustración 7

PASO 4.5: Información de la organización.

Se debe completar ***exactamente*** como aparece en la imagen de la Ilustración 8.

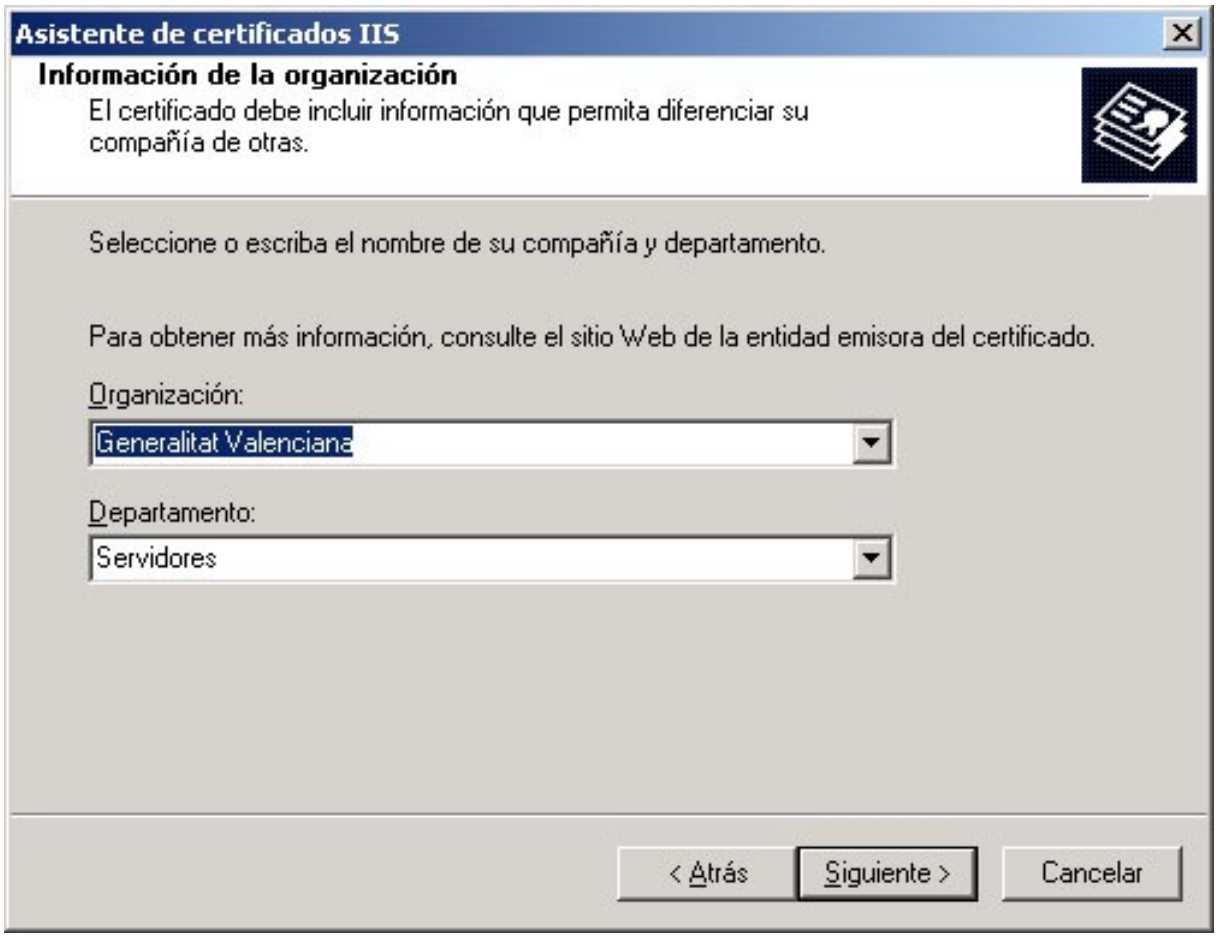

Ilustración 8

PASO 4.6: Nombre común de su sitio Web

IMPORTANTE: El nombre que se solicita en este apartado es el nombre completo (nombre o alias + dominio) con el que el servidor se publica en Internet. Este nombre es el que aparecerá en el certificado y para asegurar la confianza en el sitio debe coincidir con el nombre al que responde al servicio.

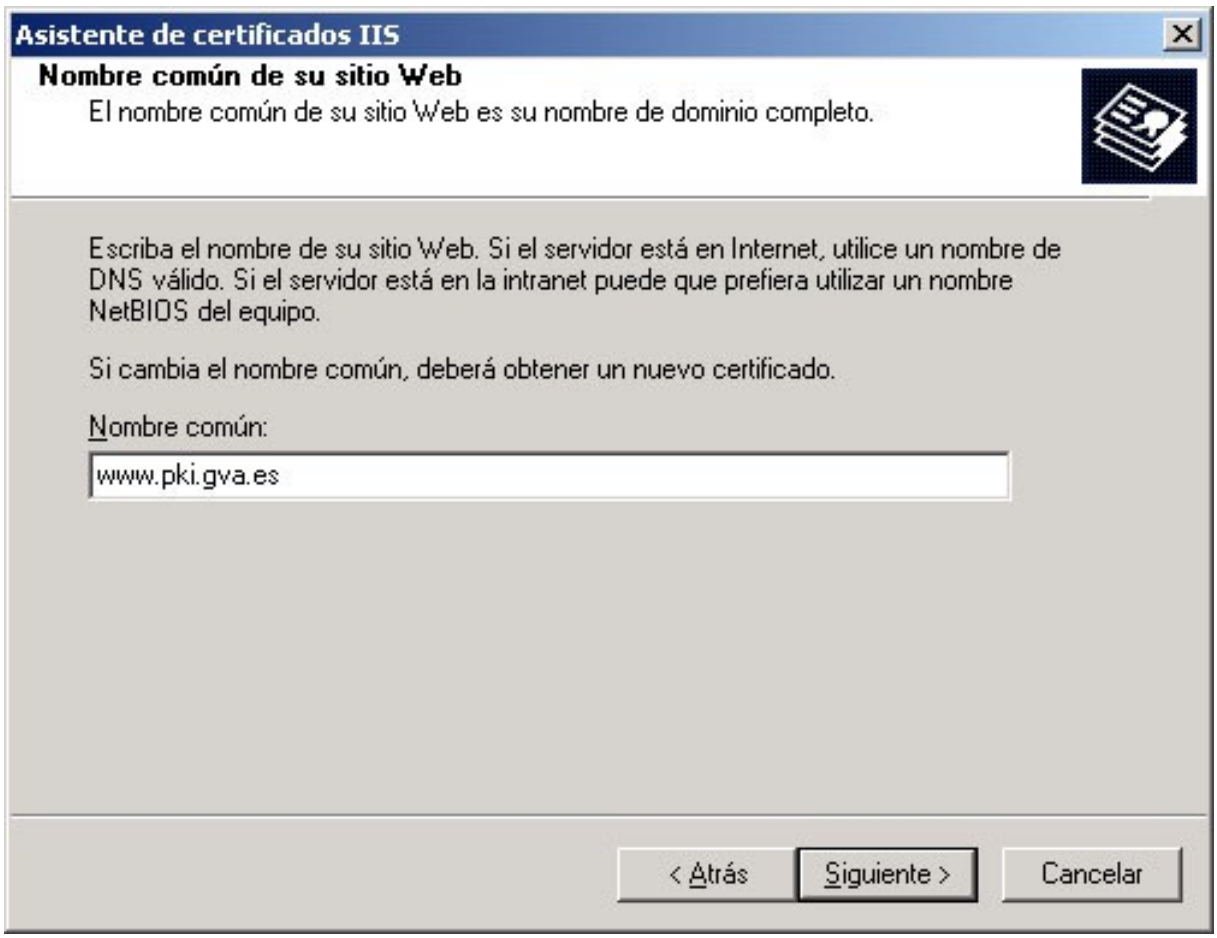

Ilustración 9

PASO 4.7: Información geográfica

De los campos que aparecen aquí, el “País o región” es fijo, y debe dejarse a “ES (España)”. Los otros dos campos (“Estado o provincia” y “Ciudad o localidad”) se rellenaran según corresponda.

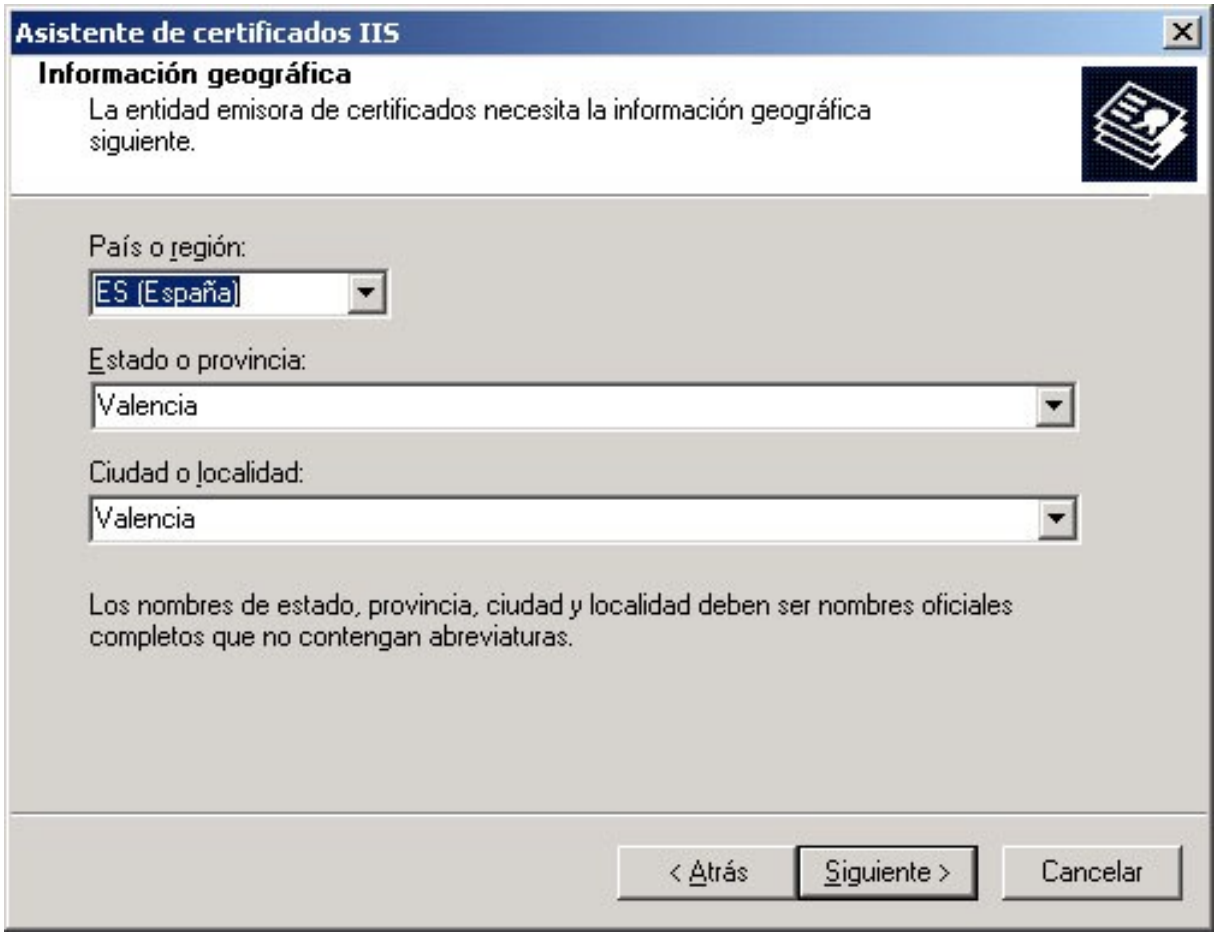

Ilustración 10

PASO 4.8: Nombre de archivo de la petición de certificado

En este paso se le asigna el nombre y la ubicación al fichero que almacena la petición generada con los datos suministrados a lo largo del proceso.

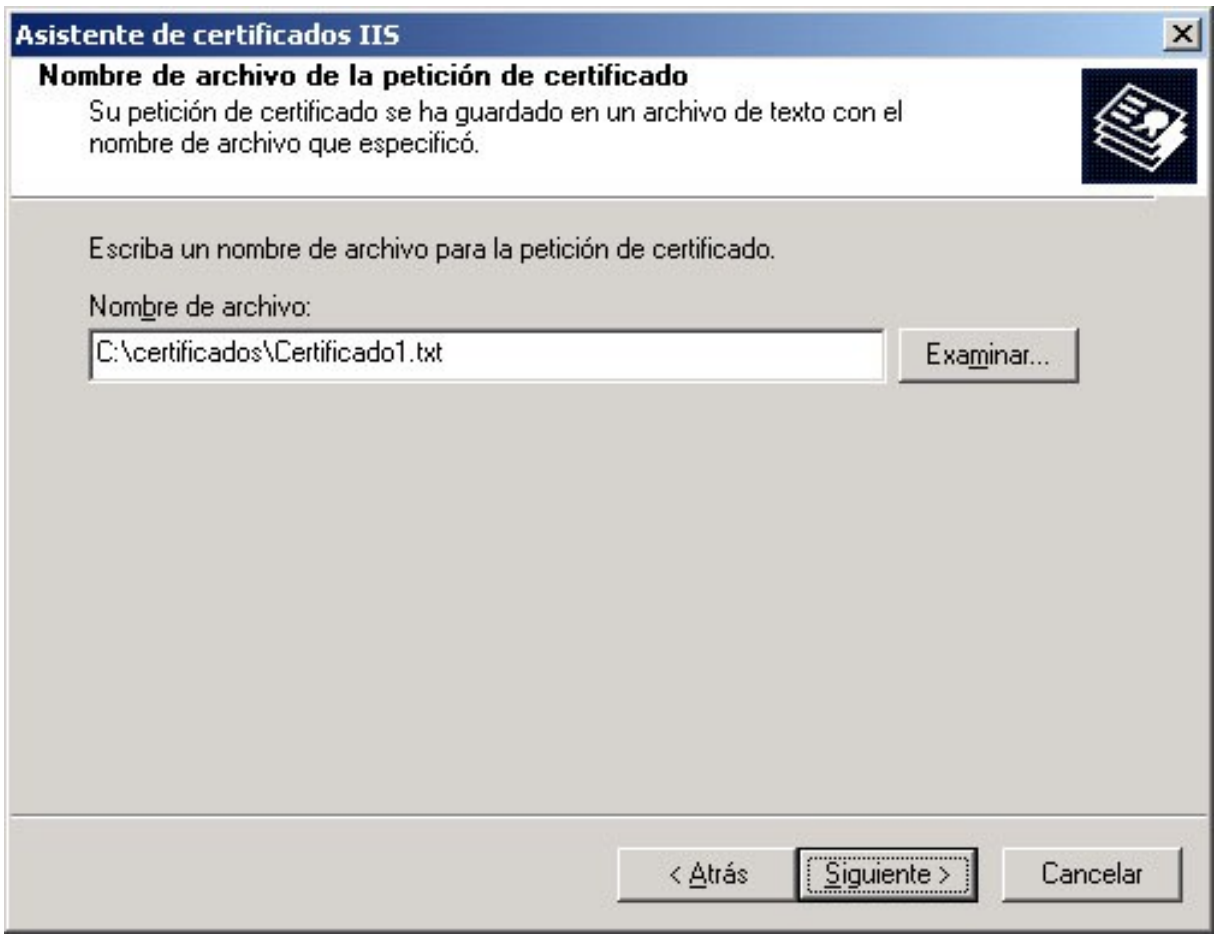

Ilustración 11

PASO 4.9: Resumen del archivo de petición

Pantalla informativa donde se muestran los datos que se incluirán en la petición. Si se detecta algún error en este punto, retrocederemos y corregiremos los datos erróneos.

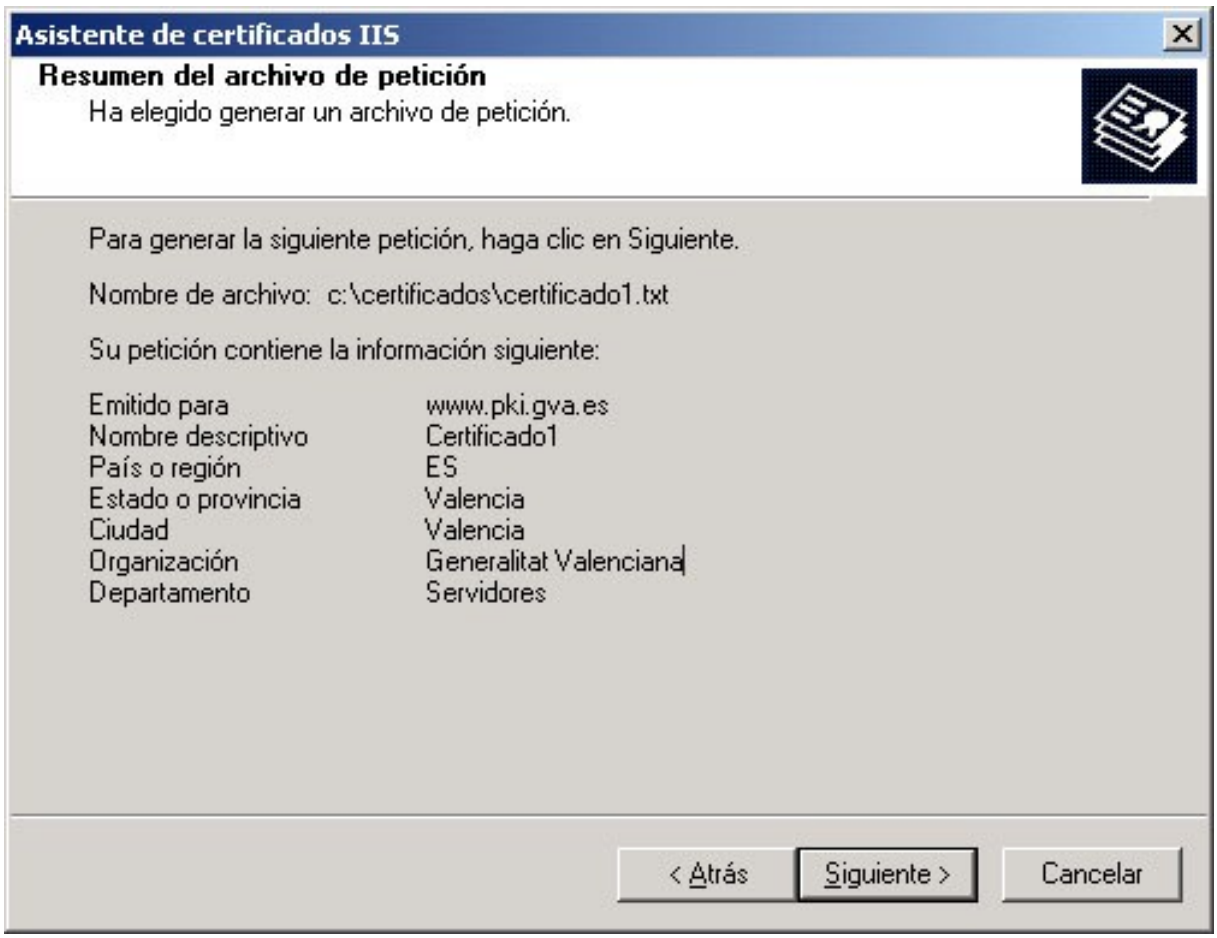

Ilustración 12

PASO 4.10: Completando el asistente para certificados de servidor Web.

En este paso se genera la petición y se almacena en el fichero que hemos indicado en el PASO 4.8. Pulsamos finalizar para salir del asistente.

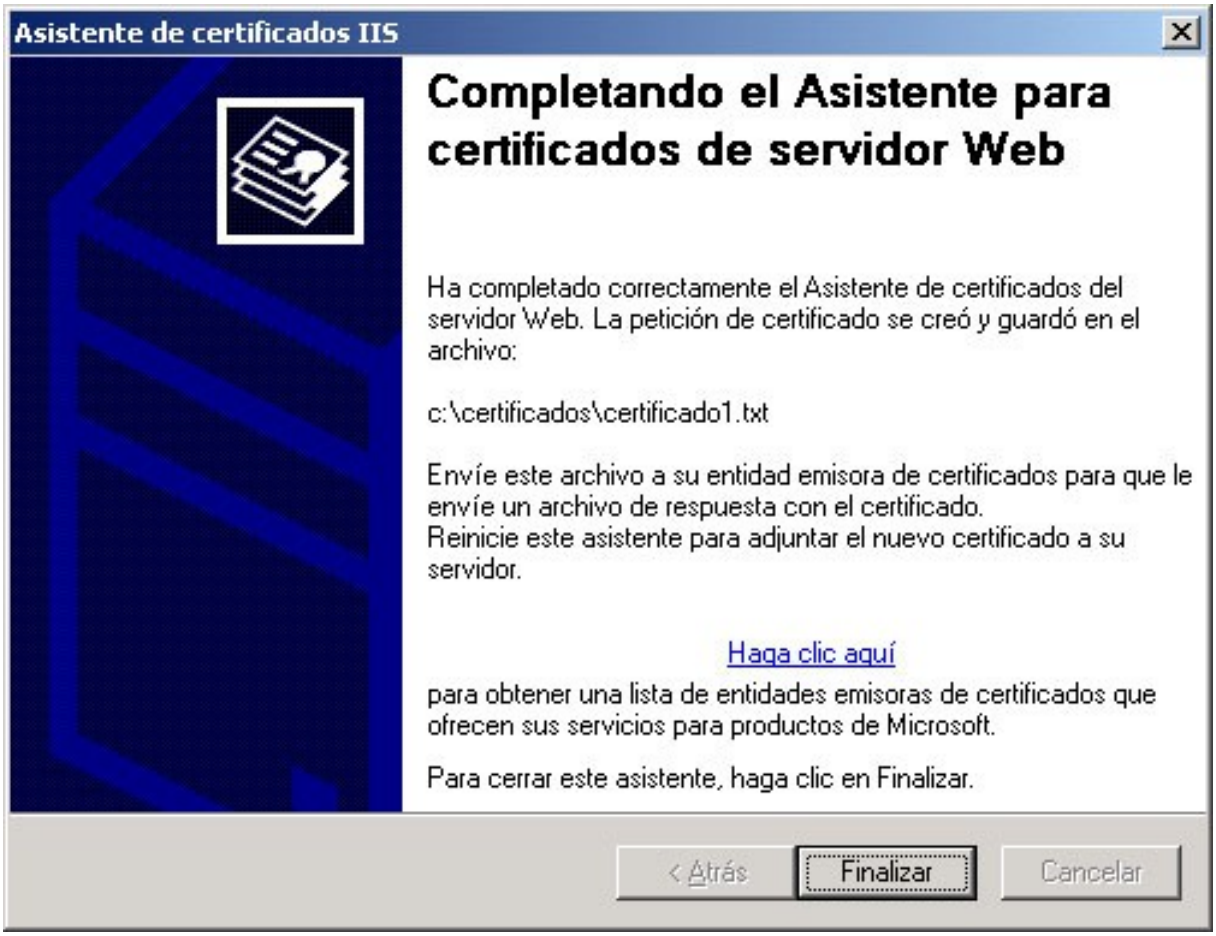

Ilustración 13

En este punto, tenemos generada la petición en el fichero indicado.

El contenido de ese fichero es el que debemos pegar en el campo “Petición generada (PKCS10)” del NPSC (https://npsc.accv.es:8450/npsc).

Una vez efectuada la petición y tal como se describe en la política de certificación para

Servidores con soporte SSL (http://www.accv.es/administracion-publica/certificados/servidor-consoporte-

ssl/), obtendremos el certificado firmado por la Autoridad de Certificación correspondiente a la

petición enviada.

Con este certificado, que guardaremos en lugar seguro, debemos efectuar los pasos siguientes.

Efectuar los pasos 1, 2 y 3, descritos anteriormente. Con esto abriremos el administrador de servicios Internet y nos posicionaremos en la pestaña de “Seguridad de directorios”.

PASO 5: Seleccionar “Certificado de Servidor”.

Esto iniciara de nuevo el “Asistente de certificado de servidor Web”, que debemos completar de la forma que se detalla a continuación

PASO 5.1: Pantalla informativa.

Si hemos seguido los pasos anteriores correctamente, nos mostrara que tenemos una petición de certificado pendiente, y el asistente se ejecutara ahora para procesar la petición.

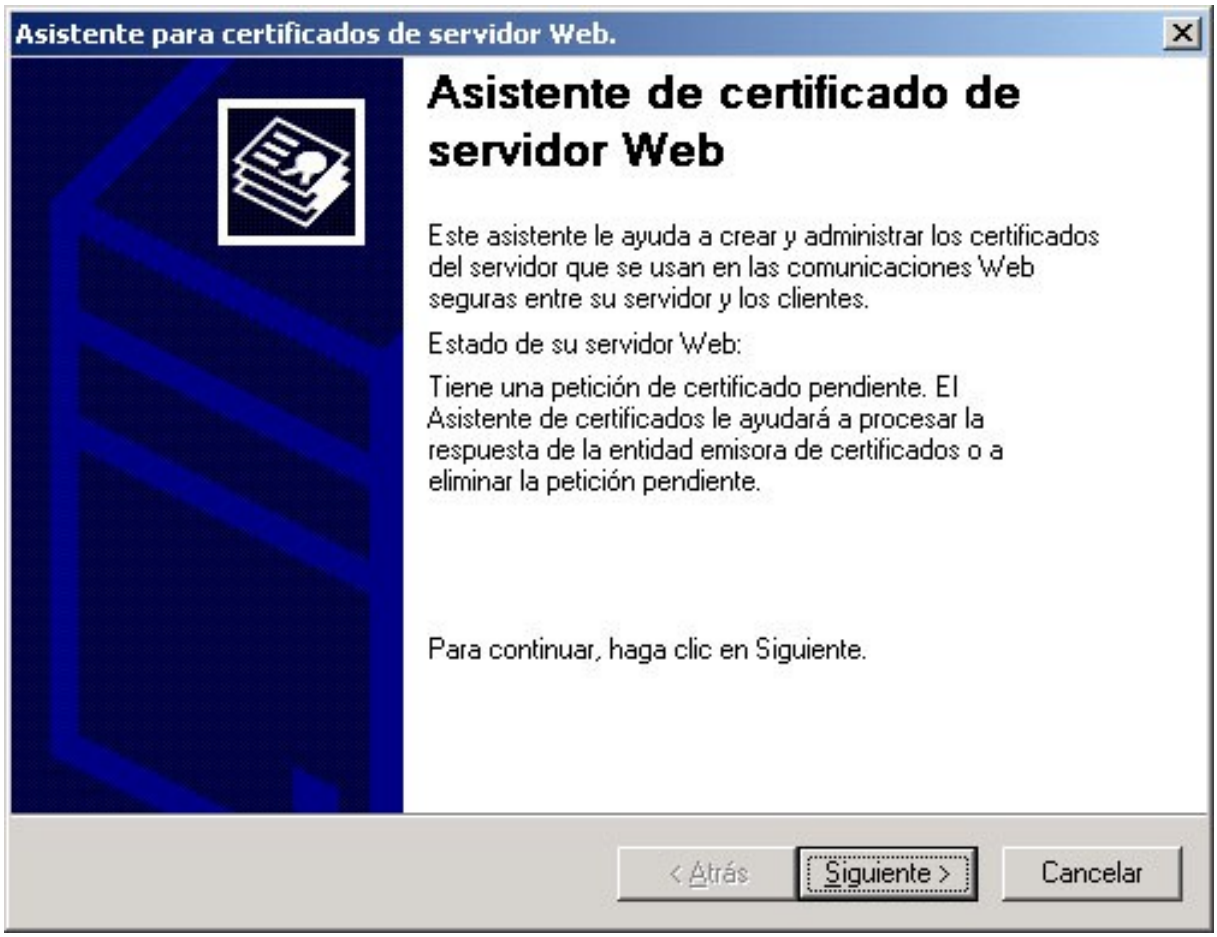

Ilustración 14

PASO 5.2: Petición de certificado pendiente

Dejamos marcado “Procesar la petición pendiente e instalar el certificado”

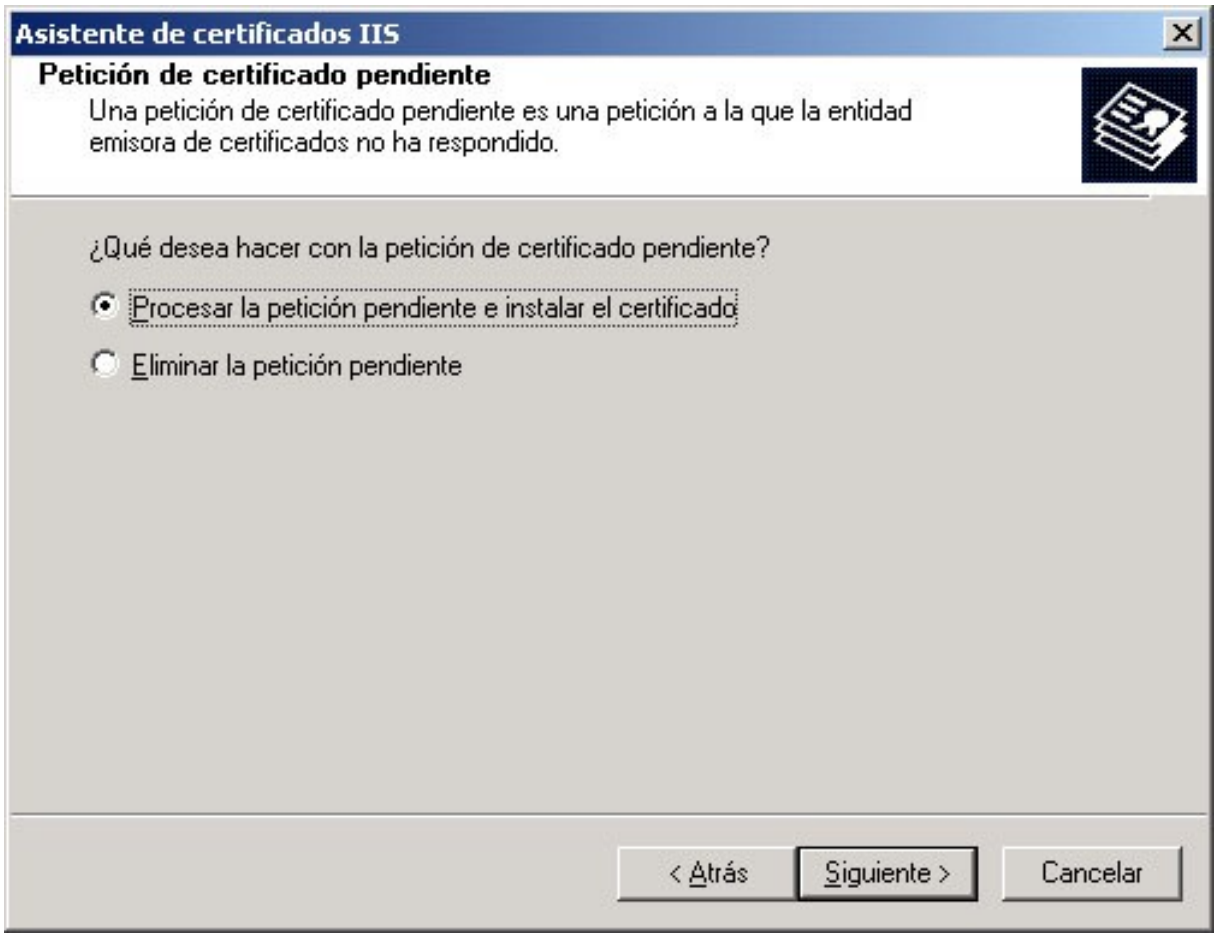

Ilustración 15

PASO 5.3: Procesar petición pendiente

Seleccionamos el archivo que nos ha devuelto la autoridad de certificación.

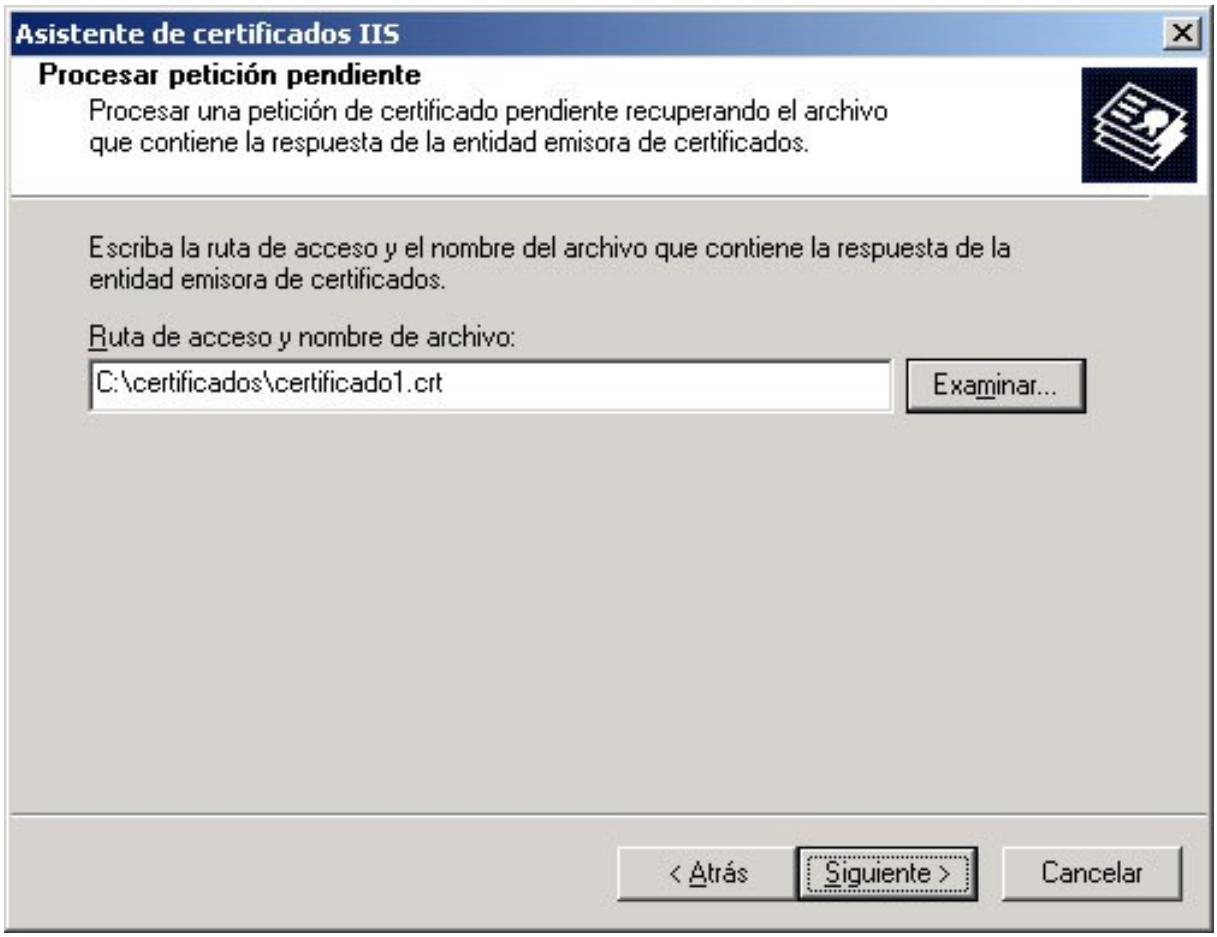

Ilustración 16

PASO 5.4: Resumen del certificado

En esta pantalla nos aparecen una serie de datos del propio certificado. Es importante comparar los datos que se suministran con los proporcionados al realizar la petición. Si hubiera algún problema con los elementos del certificado, cancele el proceso y póngase en contacto con los servicios de soporte de la Autoridad de Certificación, descritos en http://www.accv.es/

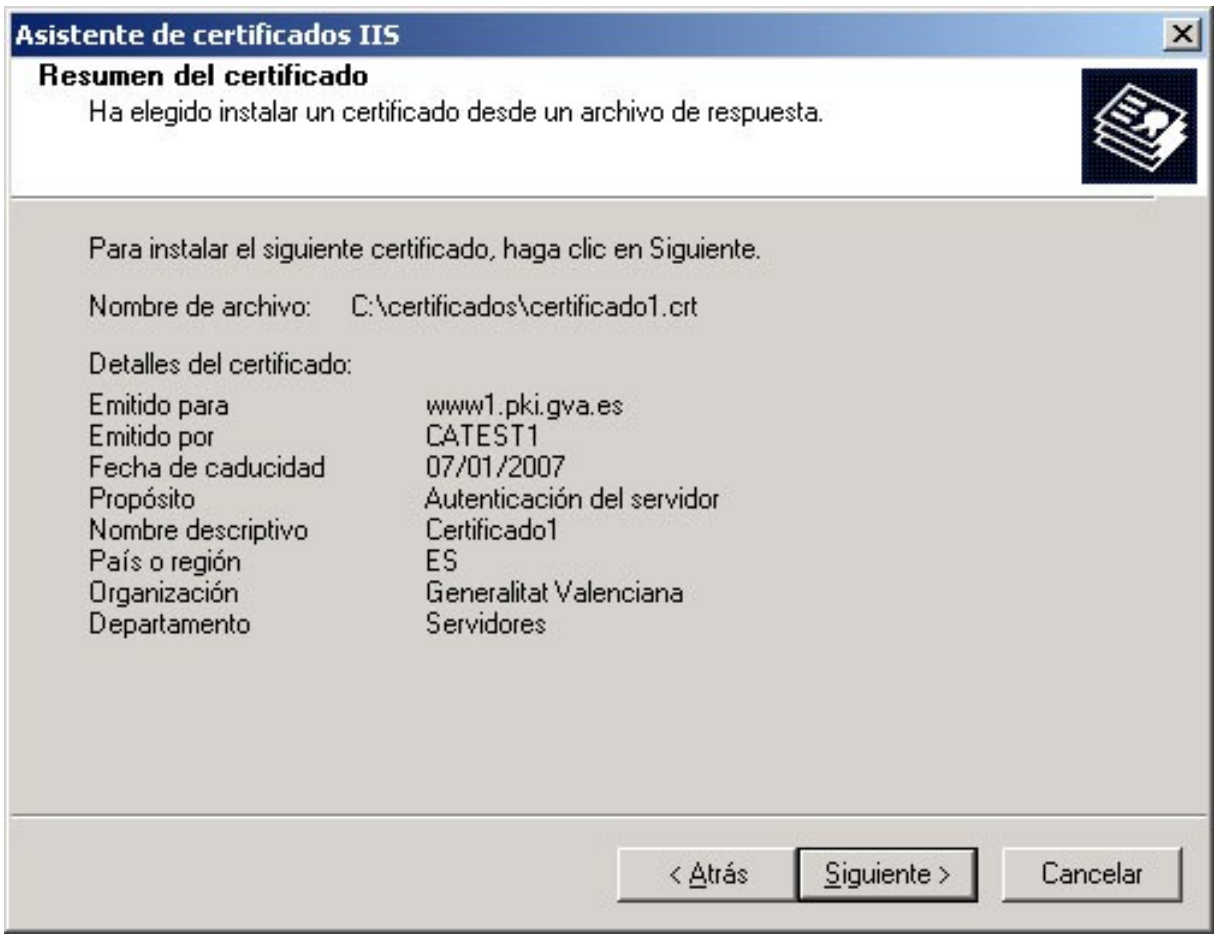

Ilustración 17

PASO 5.5: Completando el asistente para certificados de servidor Web

Si todos los pasos se han realizado correctamente, el asistente nos informara que se ha completado y que se ha instalado un certificado en este servidor.

Pulsamos finalizar para salir del asistente.

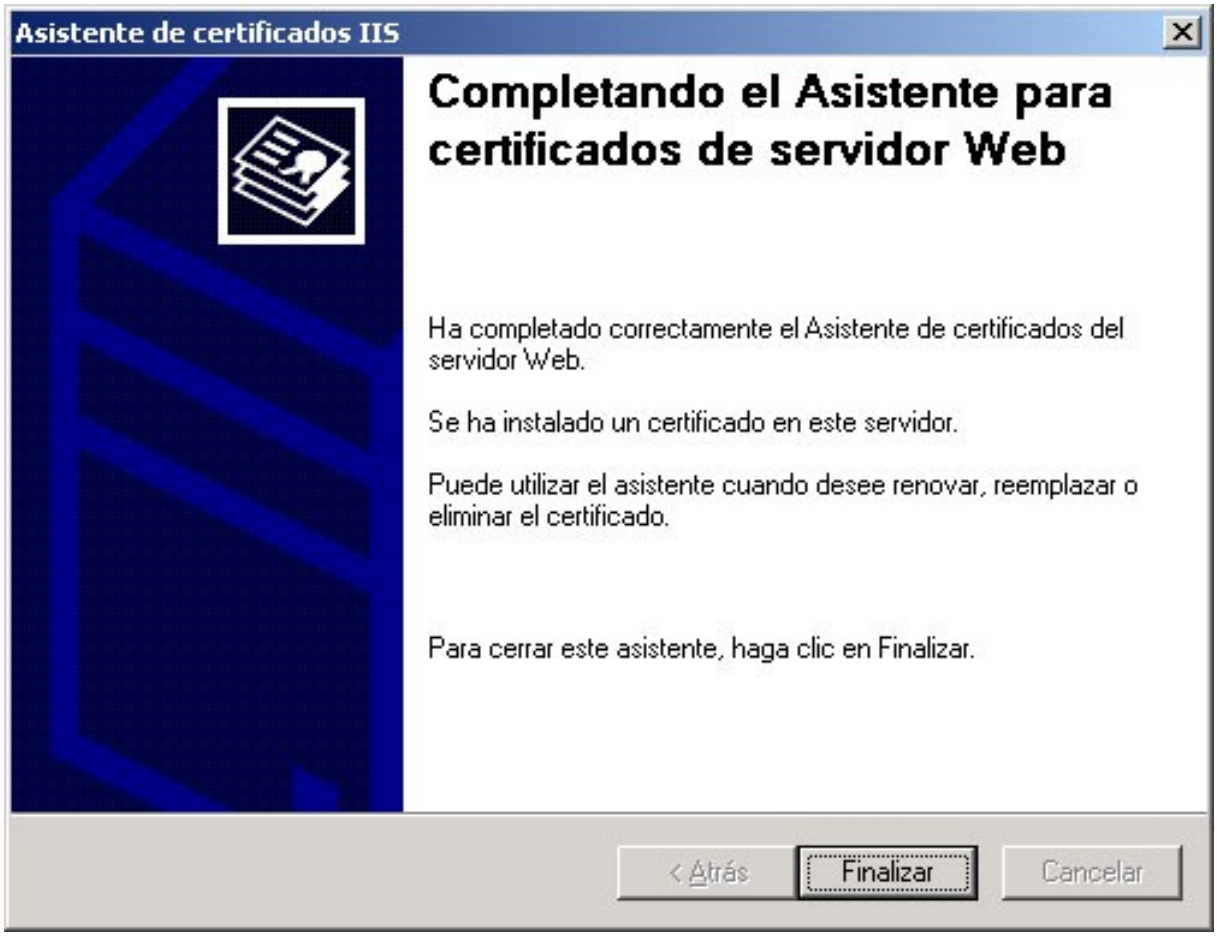

Ilustración 18

Una vez efectuado estos pasos, ya tendremos el certificado instalado en el sistema y podremos habilitar la respuesta de ese servicio por https.

Los siguientes pasos son necesarios para que el servidor Web acepte como certificados validos de cliente los emitidos por la Agencia de Tecnología y Certificación Electrónica.

PASO 6: Abrir la consola de gestión de certificados para el equipo local.

PASO 6.1: Abrir una consola genérica.

En la línea de comandos (ventana DOS) ejecutamos la orden

mmc

Ilustración 19

Este comando nos abre una consola vacía.

PASO 6.2: Seleccionar almacén de certificados del servidor

Desde el menú *Consola*, seleccionamos *Agregar o quitar complementos*

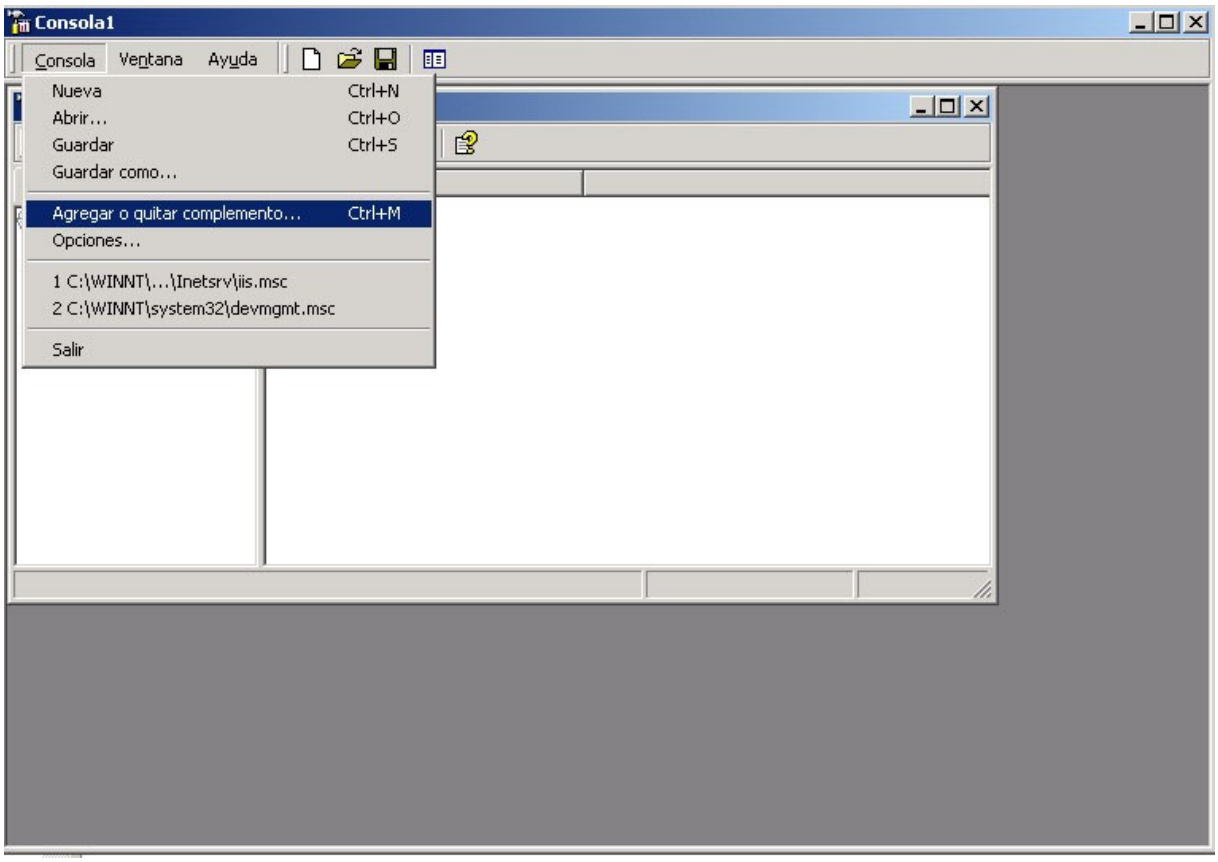

Ilustración 20

Desde la ventana de Agregar o quitar complementos, seleccionamos *Agregar*

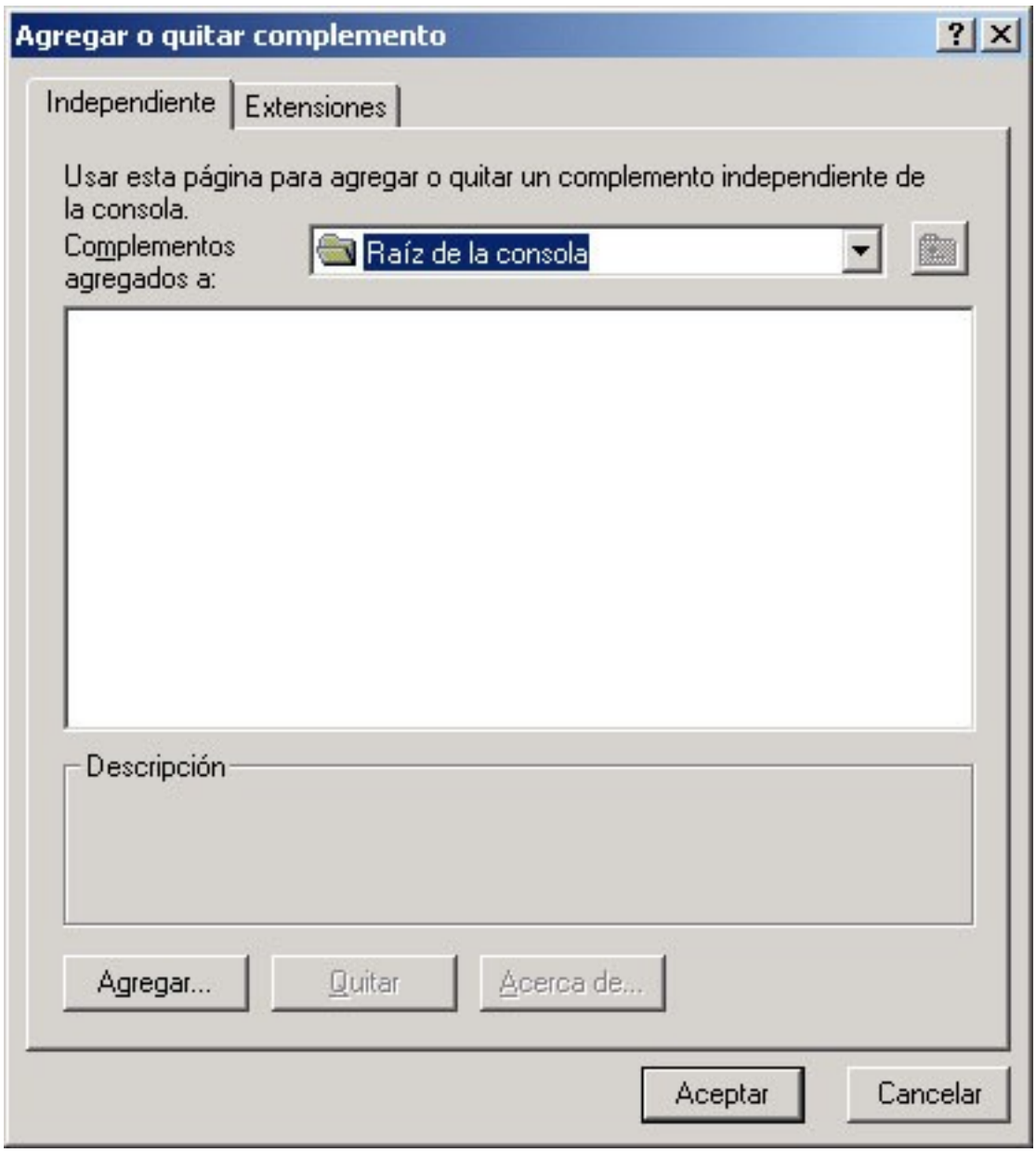

Ilustración 21

Desde la ventana Agregar un complemento independiente, seleccionamos *Certificados*, y pulsamos *Agregar*.

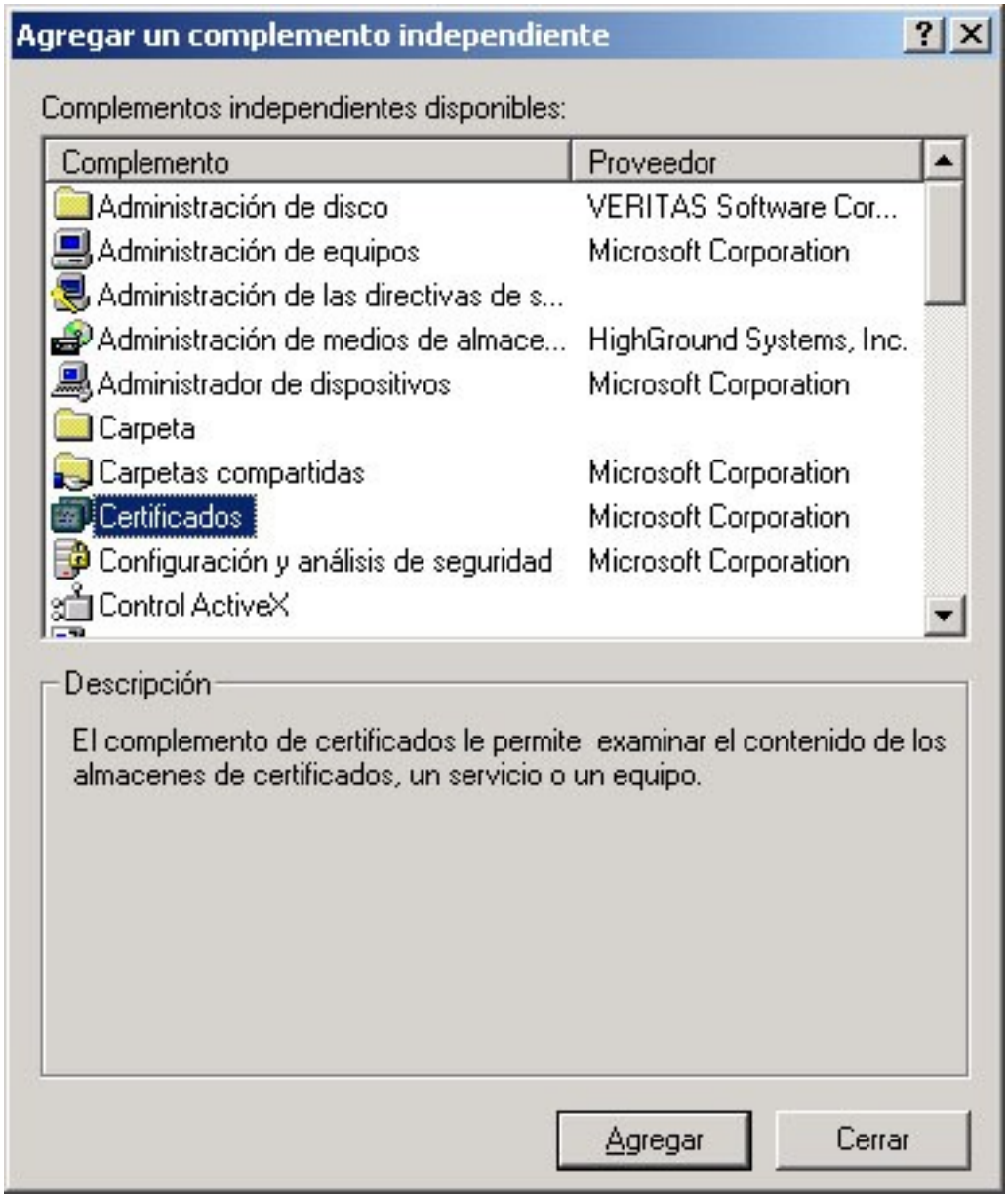

Ilustración 22

En la ventana Complemento de certificados, seleccionamos *Cuenta de equipo* y pulsamos *Siguiente*.

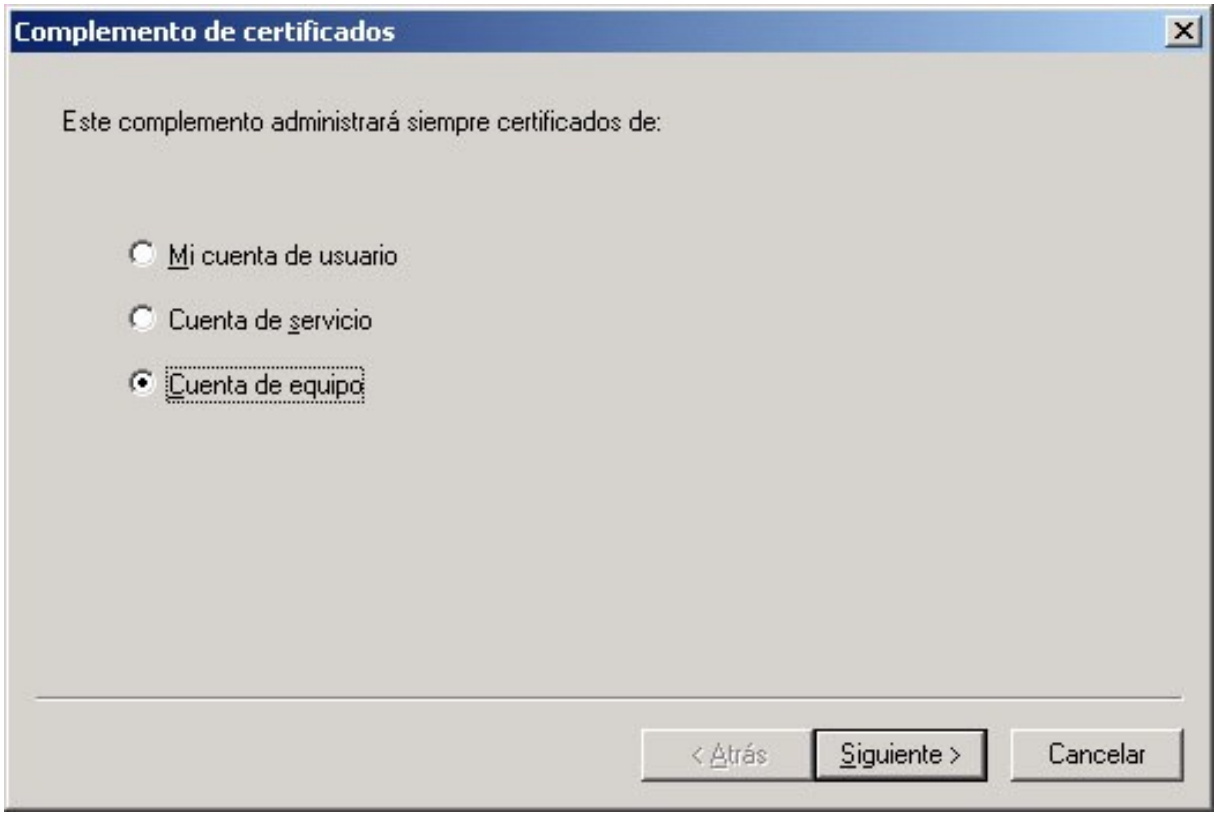

Ilustración 23

En la pantalla Seleccionar equipo, dejamos marcado *Equipo local (el equipo en el que se está ejecutando esta consola)*, y pulsamos *Finalizar*.

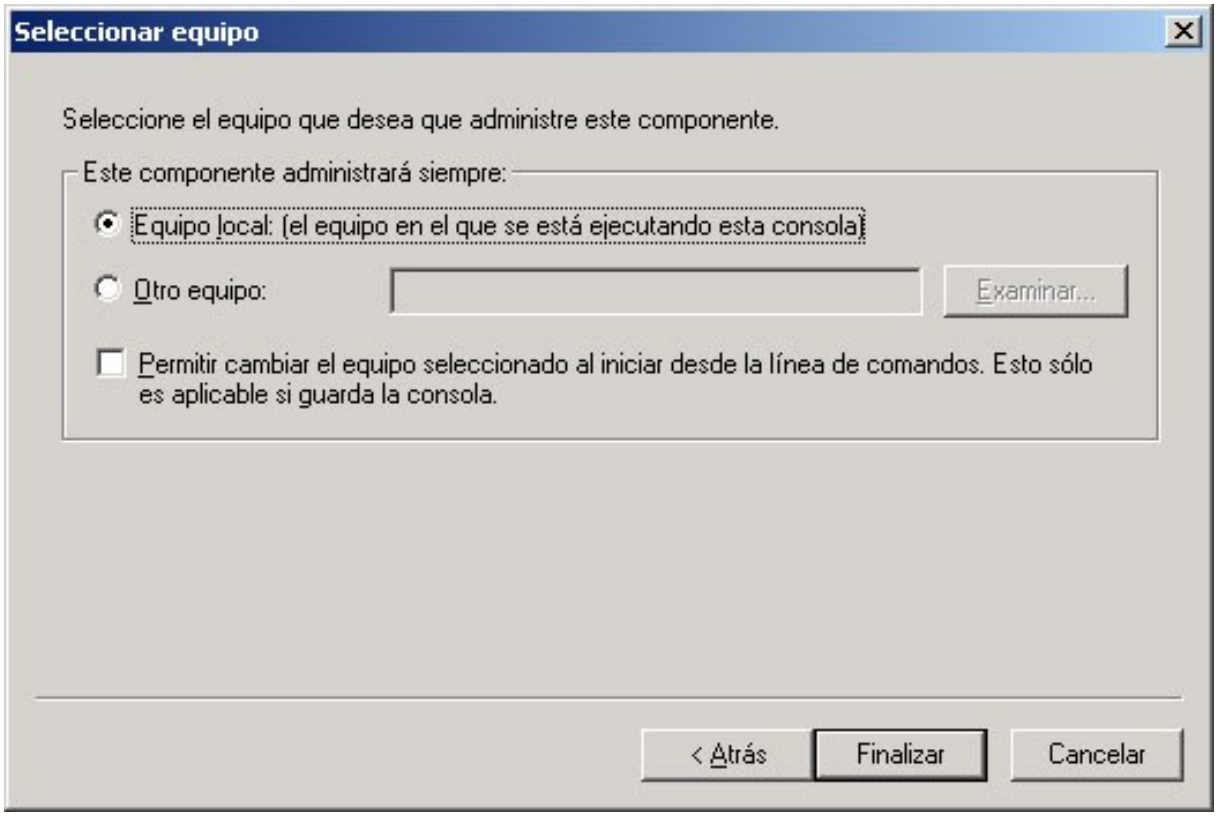

Ilustración 24

Cerramos la ventana Agregar un complemento independiente (Ilustración 22), y pulsamos Aceptar en Agregar o quitar complemento (Ilustración 21).

En este punto debemos tener una consola con el complemento de certificados en pantalla, tal y como se muestra en la siguiente ilustración.

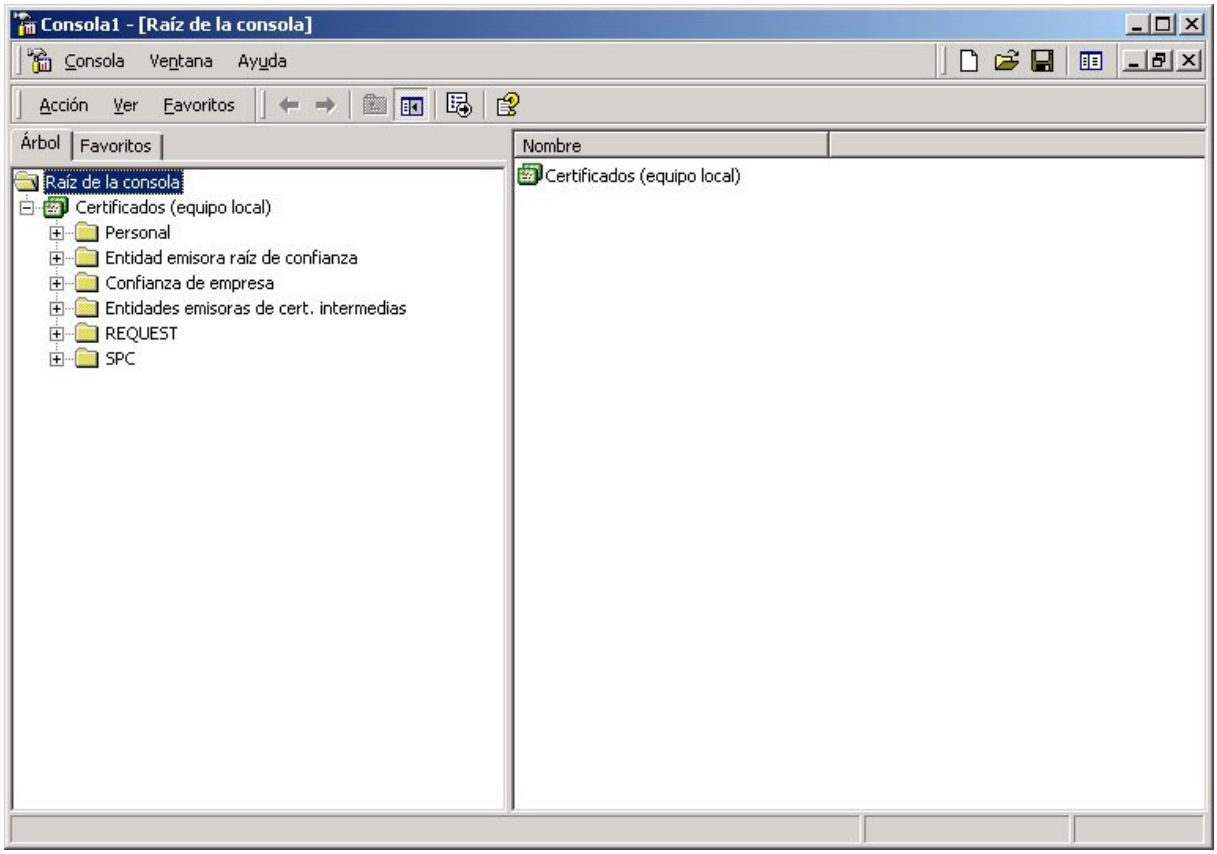

Ilustración 25

PASO 6.3 Importación del certificado de la RootCA

Descargamos el certificado de la Autoridad de certificación Raíz, que se encuentra en:

http://www.accv.es/ayuda/descargar-certificados-digitales/

guardándolo en disco, por ejemplo en C:\rootca.crt.

En la consola que tenemos abierta, desplegamos *Certificados (equipo local)*, *Entidad emisora raíz de confianza*, y pinchamos sobre *Certificados*.

Con el botón derecho del ratón, desplegamos el menú, seleccionando *Todas las tareas -> Importar*.

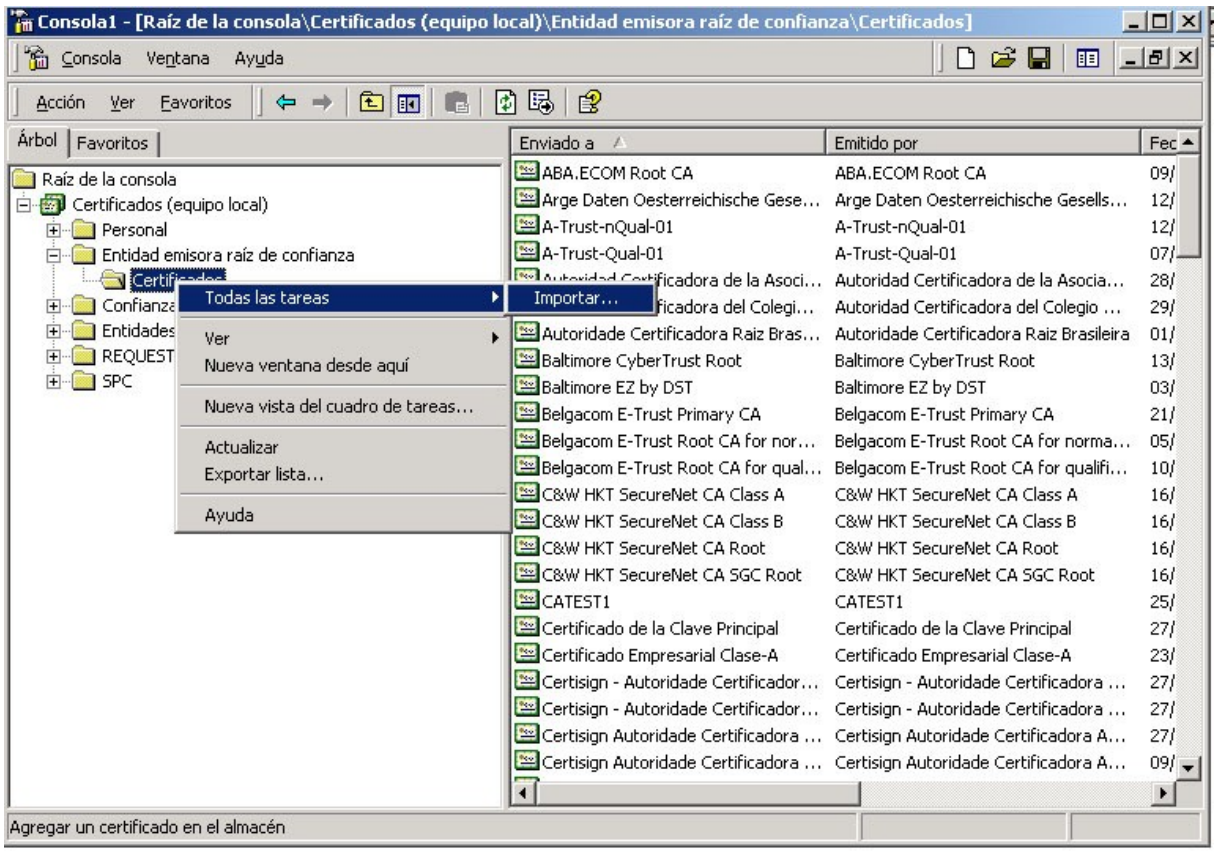

Ilustración 26

A continuación, nos aparece el Asistente para importación de certificados. La primera pantalla es informativa, seleccionando Siguiente:

Ilustración 27

El Asistente para importación de certificados nos solicita ahora el Archivo para importar, seleccionando el que habíamos guardado al principio de este paso, y pulsando Siguiente:

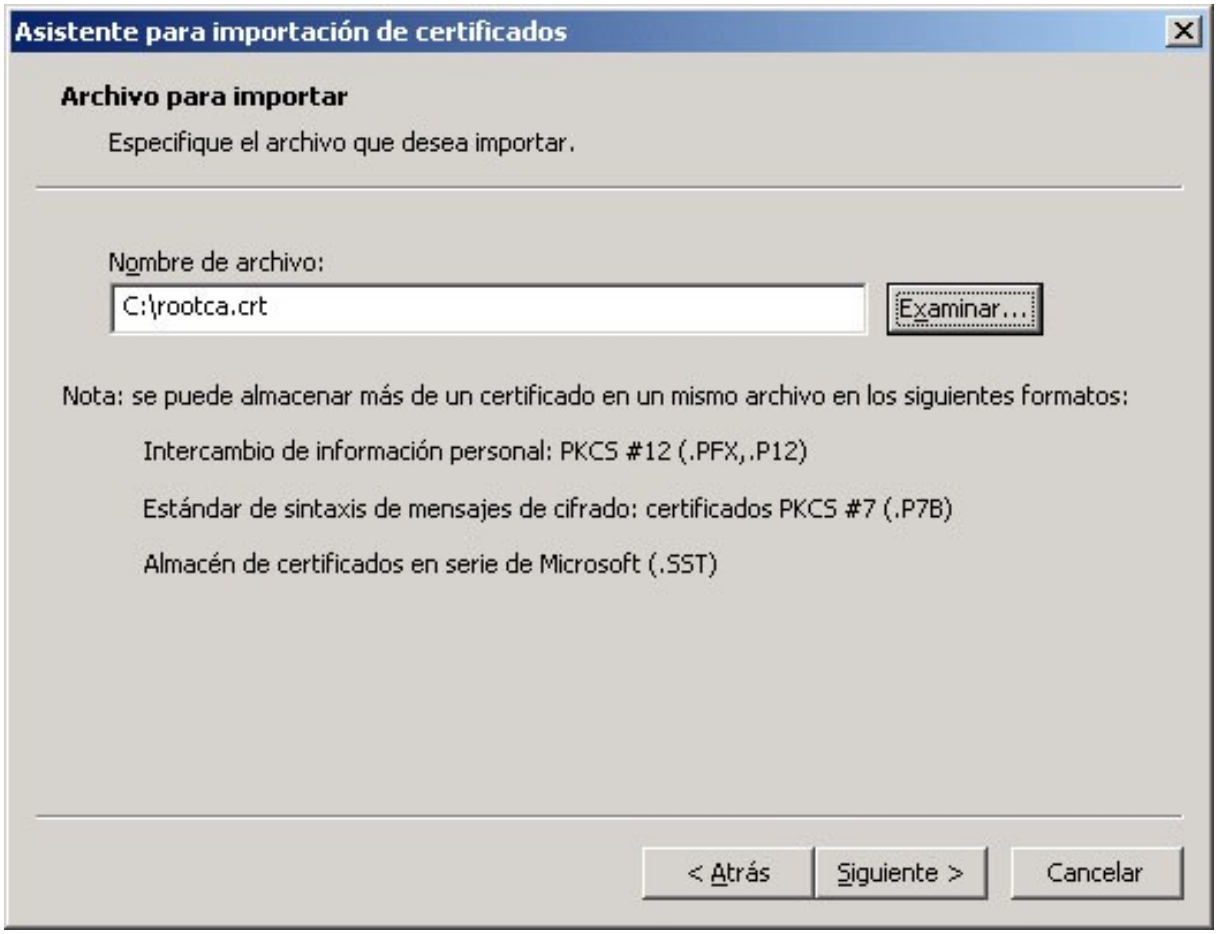

Ilustración 28

El Asistente para importación de certificados nos solicita el Almacén de certificados. Dejamos la opción por defecto que el sistema haya elegido.

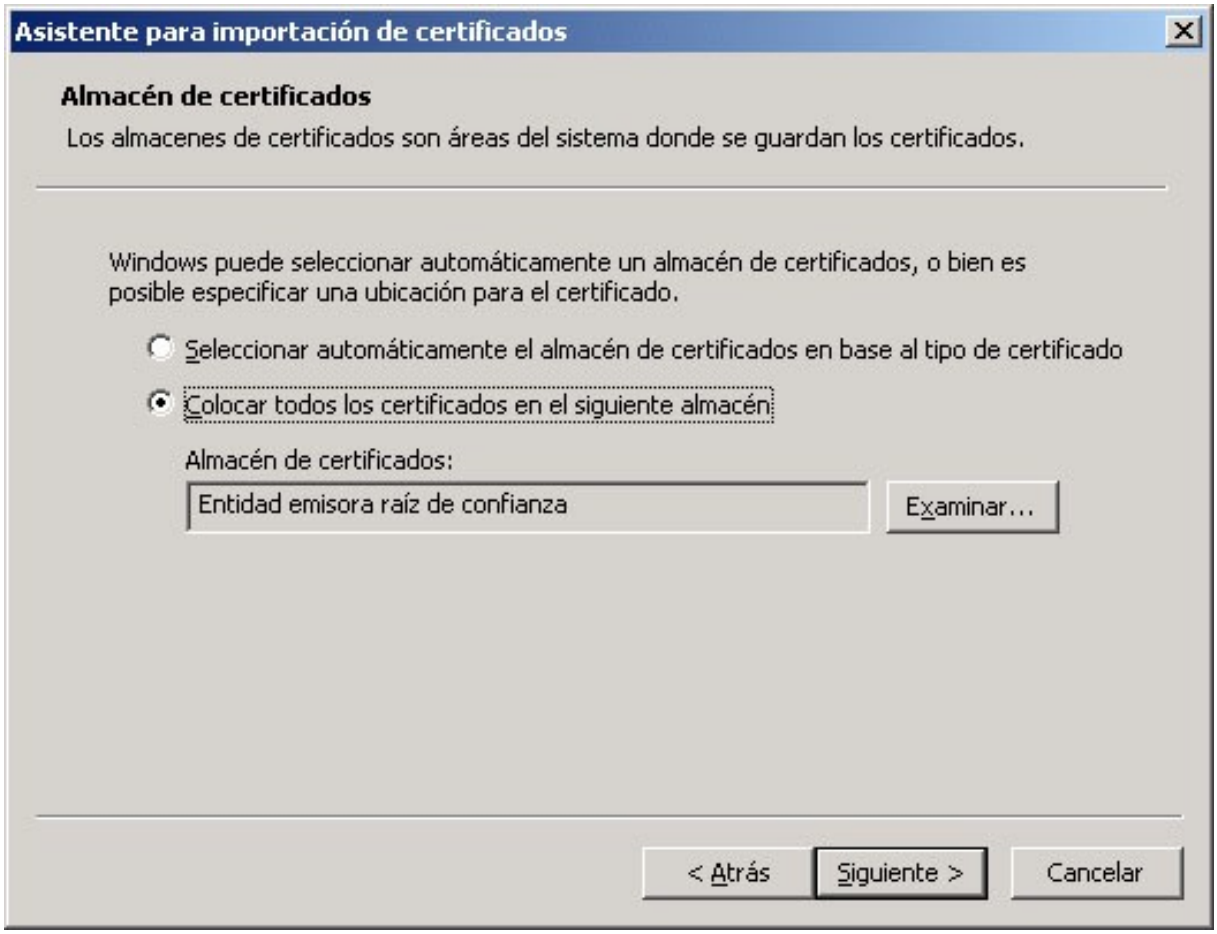

Ilustración 29

La última pantalla es informativa, terminando el proceso pulsando *Finalizar*.

El sistema nos informara si la importación se ha realizado correctamente.

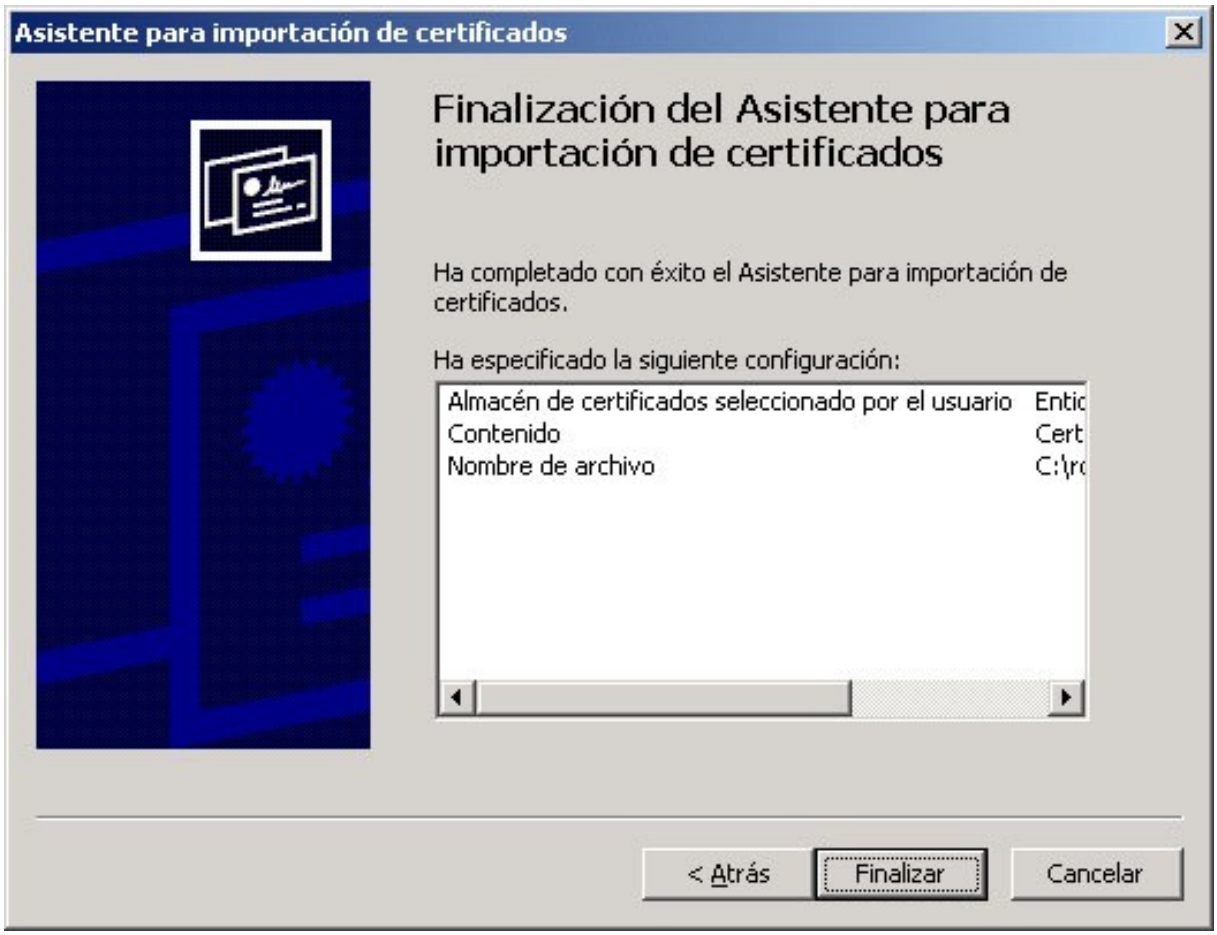

Ilustración 30

PASO 6.4: Importación de los certificados intermedios

Se va a describir el proceso para ACCV-CA2 (se realizaría igual para todas las intermedias).

Descargamos los certificados de la Autoridad de certificación intermedia, ACCV-CA2, que se encuentra en:

http://www.accv.es/ayuda/descargar-certificados-digitales/

guardándolo en disco, por ejemplo en C:\accv-ca2.crt.

Volvemos a la consola que habíamos abierto en el Paso 6.2, desplegamos *Certificados (equipo local)*, *Entidades emisoras de cert. intermedias*, y pinchamos sobre *Certificados*.

Con el botón derecho del ratón, desplegamos el menú, seleccionando *Todas las tareas -> Importar*.

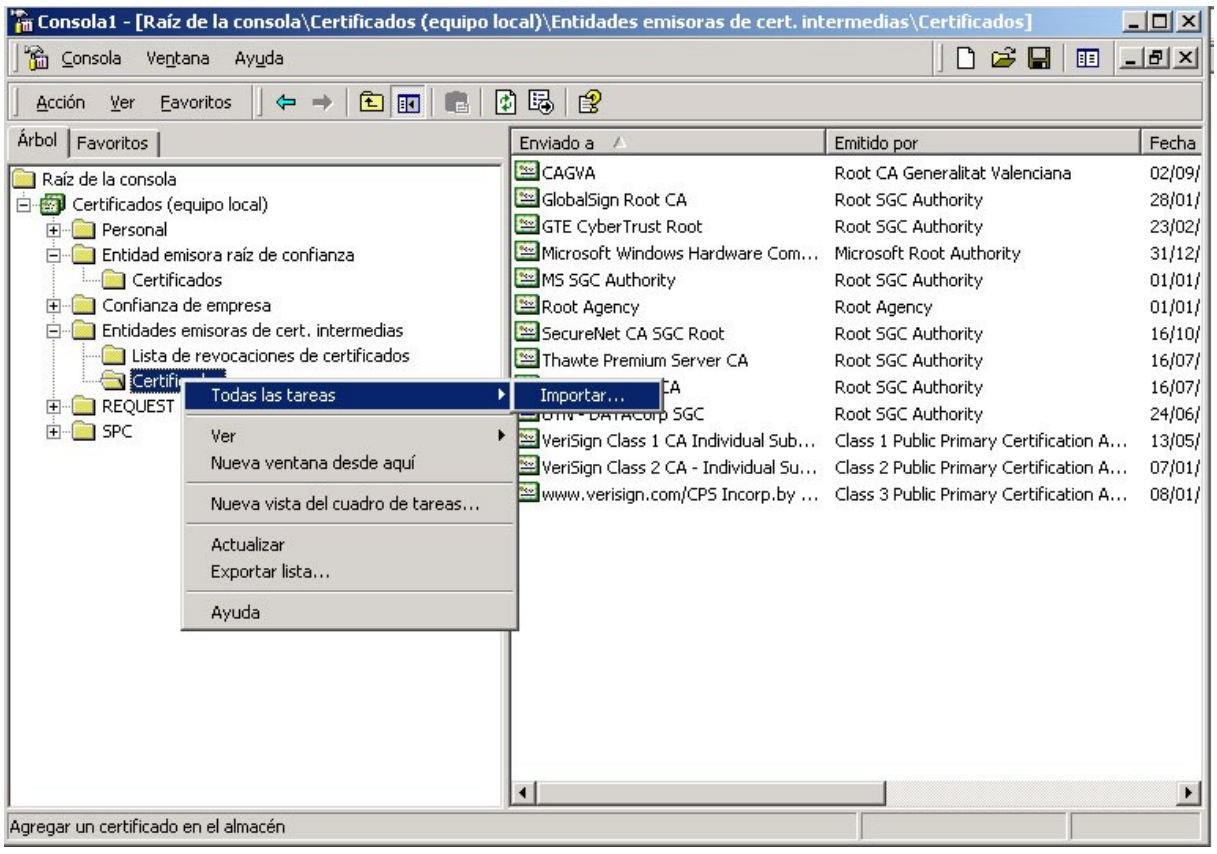

Ilustración 31

Realizamos el proceso de importación del certificado con el asistente, proporcionándole esta vez el certificado que hemos guardado al principio de este paso.

Una vez finalizado, ya se encuentran importados en el repositorio del sistema los certificados de la Agencia de Tecnología y Certificación Electrónica, de tal manera que si se habilita la autenticación de cliente, aparecerán en los certificados a elegir.

3. Apéndices

No aplicable.