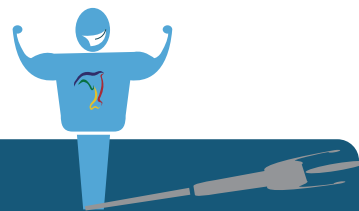


¿Qué ofrece Autentia Real Business Solutions S.L?

Somos su empresa de **Soporte a Desarrollo Informático**.
 Ese apoyo que siempre quiso tener...

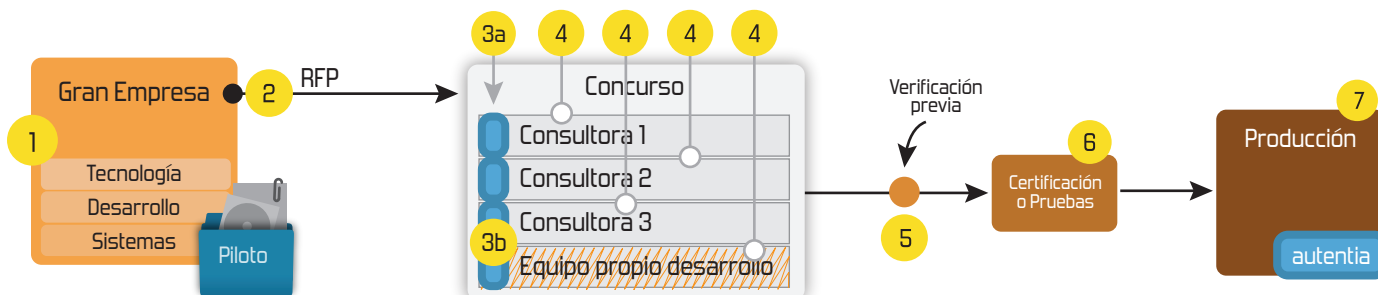
1. Desarrollo de componentes y proyectos a medida



2. Auditoría de código y recomendaciones de mejora

3. Arranque de proyectos basados en nuevas tecnologías

1. Definición de frameworks corporativos.
2. Transferencia de conocimiento de nuevas arquitecturas.
3. Soporte al arranque de proyectos.
4. Auditoría preventiva periódica de calidad.
5. Revisión previa a la certificación de proyectos.
6. Extensión de capacidad de equipos de calidad.
7. Identificación de problemas en producción.



4. Cursos de formación (impartidos por desarrolladores en activo)

Spring MVC, JSF-PrimeFaces /RichFaces,
 HTML5, CSS3, JavaScript-jQuery

Gestor portales (Liferay)
 Gestor de contenidos (Alfresco)
 Aplicaciones híbridas

Tareas programadas (Quartz)
 Gestor documental (Alfresco)
 Inversión de control (Spring)

Control de autenticación y
 acceso (Spring Security)
 UDDI
 Web Services
 Rest Services
 Social SSO
 SSO (Cas)

JPA-Hibernate, MyBatis
 Motor de búsqueda empresarial (Solr)
 ETL (Talend)

Dirección de Proyectos Informáticos.
 Metodologías ágiles
 Patrones de diseño
 TDD

BPM (jBPM o Bonita)
 Generación de informes (JasperReport)
 ESB (Open ESB)



[Home](#) | [Quienes Somos](#) | [Empleo](#) | [Foros](#) | [Tutoriales](#) | [Servicios Gratuitos](#) | [Contacte](#)

	<p>Tutorial desarrollado por: Roberto Canales Mora 2003-2005 Creador de AdictosAlTrabajo.com y</p> <p>Director General de Autentia S.L.</p> <p>Recuerda que me puedes contratar para echarte una mano:</p> <p>Desarrollo y arquitectura Java/J2EE Asesoramiento tecnológico Web Formación / consultoría integrados en tu proyecto</p> <p>No te cortes y contacta: 655 99 11 72 rcanales@autentia.com.</p>	
---	---	---

Descargar este documento en formato PDF [iissl.pdf](#)

[Free SSL Certificates](#)

Issued in mins installed in seconds Low price single root 128/256 bit
www.rapidssl.com

[SPW S.L.](#)

Soluciones en SSL-VPN Watchguard y Enkoo
www.spw.es

[Anuncios Goooooogle](#)

[Anunciarse en este sitio](#)

Activar el soporte SSL a Microsoft IIS

Cuando navegamos por páginas Web, estamos siempre expuestos a que los datos que transmitimos sean interceptados

Para evitar este problema, los servidores pueden activar la seguridad, de tal modo que se encripta la comunicación, asegurándonos que nadie puede leer lo que estamos enviando. Para algunos tipos de servicios, donde se intercambian datos personales ... esto es vital.

Os sonará que se utilizas **https** en vez de **http...** es decir http con soporte seguro **SSL**

No vamos a profundizar en el proceso ... ya que hay muchos libros que explican la teoría. Vamos a mostraros de un modo práctico los pasos necesarios para asegurar las comunicaciones entre cliente y servidor.

(No vamos a ser demasiado puristas en la explicación la idea es que todo el mundo lo entienda)

Muchos sistemas de seguridad se basan en el denominado "tercero de confianza", es decir, un organismo o entidad que proporcione algo y que reconozcan como válido las otras dos partes involucradas (vamos, como cuando vas a la policía a que te compulsen un documento).

Para realizar comunicaciones seguras, hay que encriptar los mensajes enviados. Se utiliza una técnica denominada clave asimétrica. Esto consiste en que una parte genera dos claves: Una privada que se guarda de un modo muy seguro y una pública que se da a todo el mundo. Estas claves están matemáticamente relacionadas, de tal modo que lo que se codifica con una clave, solo se descrypta con la otra.

En el mundo Web, este tercero de confianza se denomina CA (entidad certificadora) la cual, previa presentación de documentación notarial, proporciona un fichero que asegura al cliente Web que el servidor es quien dice ser (ya que no hay presencia física y nunca se puede estar seguro).

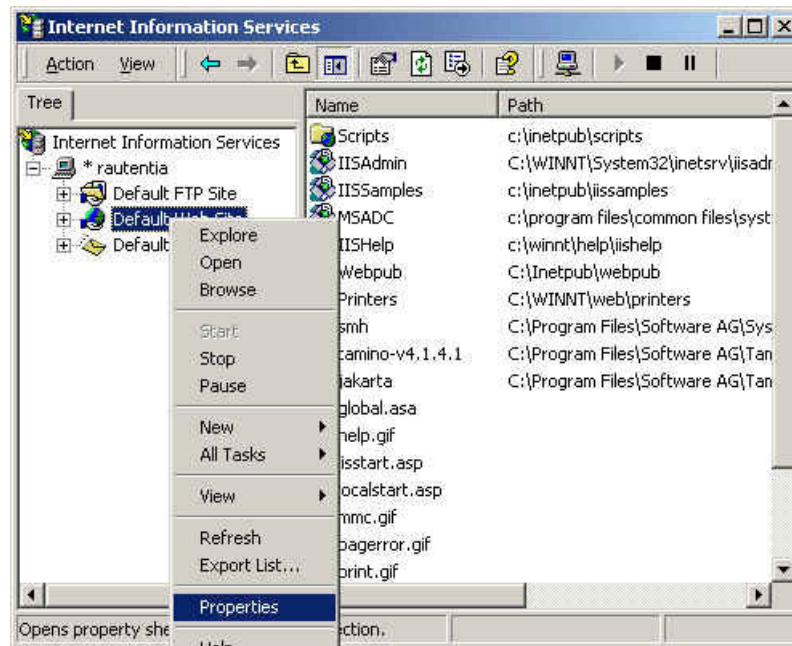
Este fichero es lo que se denomina un certificado digital (La entidad certificadora emite y firma un certificado digital). Este certificado digital, contiene, además de información identificativa del servidor, una clave (la clave pública) del servidor Web. Como hemos dicho, esta clave es muy curiosa ya que si se encripta algo con ella, solo nuestro servidor puede decodificarla

Así que cuando un usuario desde un navegador se conecta a un Web seguro (que tiene activada la seguridad), el servidor le manda el certificado. Como este certificado ha sido emitido por la entidad certificadora, el navegador verifica si es correcto o no.. y si es así utiliza la clave pública de nuestro servidor Web para encriptar mensajes y comunicarse con el servidor. Nadie más que el servidor destino tiene capacidad de descryptar la información

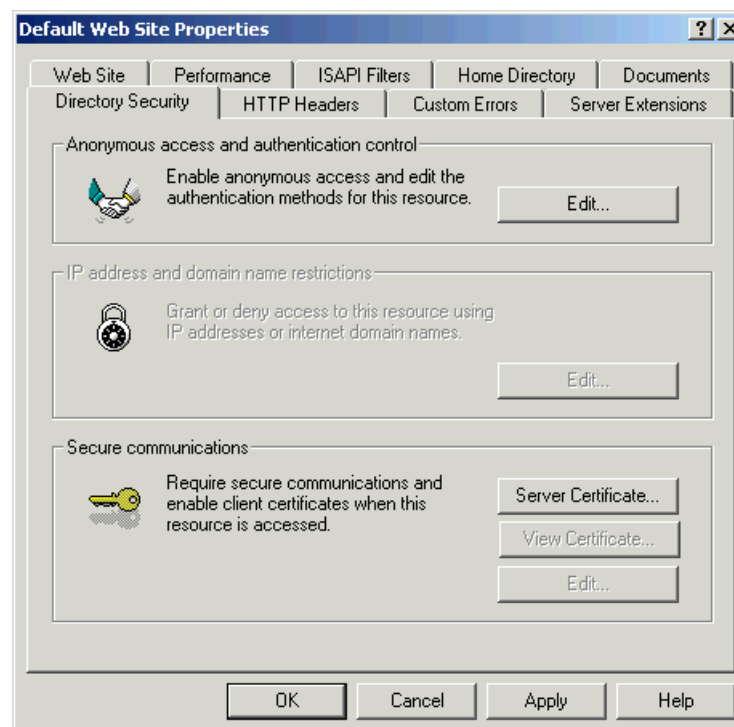
Lo vamos a dejar aquí ... el movimiento se demuestra andando

Solicitar un Certificado Digital con IIS

Para poder instalar la seguridad (soporte https) en IIS, debemos ir a su consola de administración y pinchar en propiedades



En la lengüeta de seguridad, pichamos en **Server Certificate**

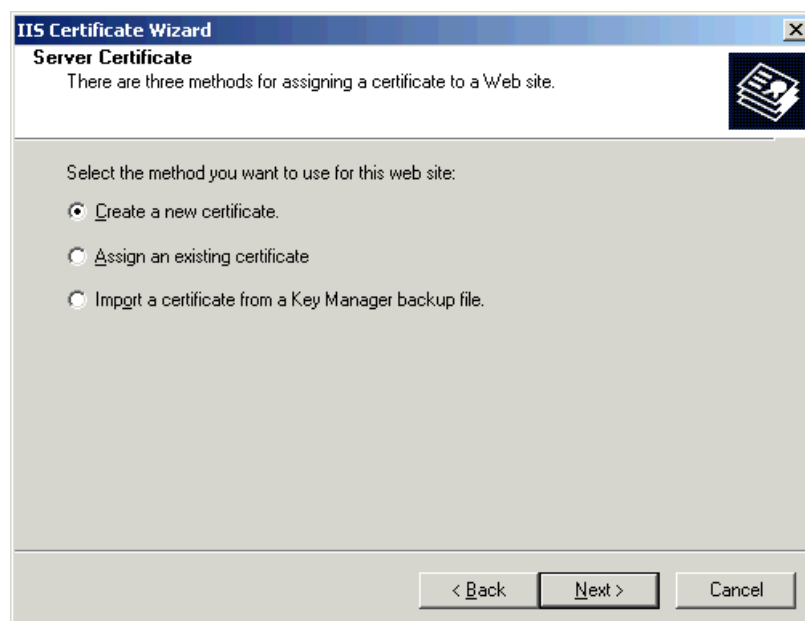


IIS hace casi de modo automático todas las labores necesarias para solicitar e instalar un certificado digital.

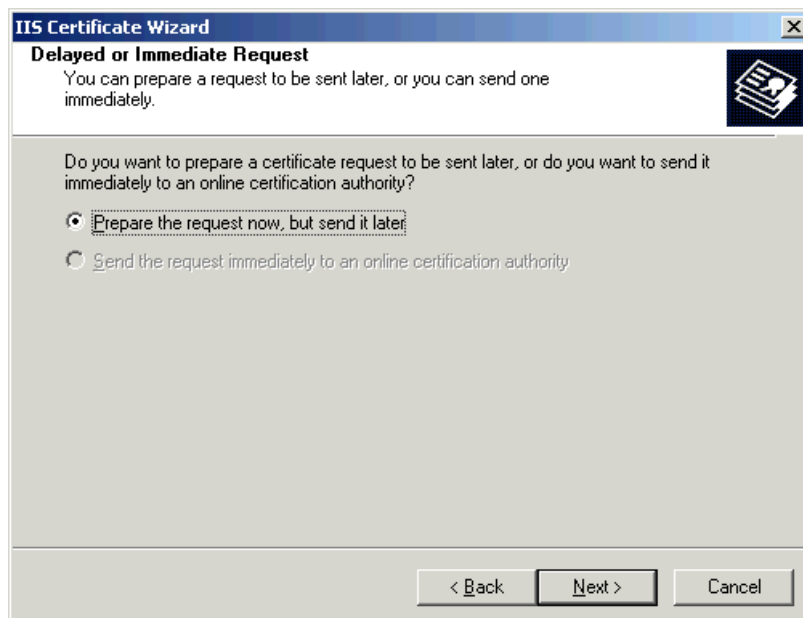
Esto consiste en generar una clave privada, una clave pública y enviar a la entidad certificadora la clave pública para que la valide, firme y genere el certificado.



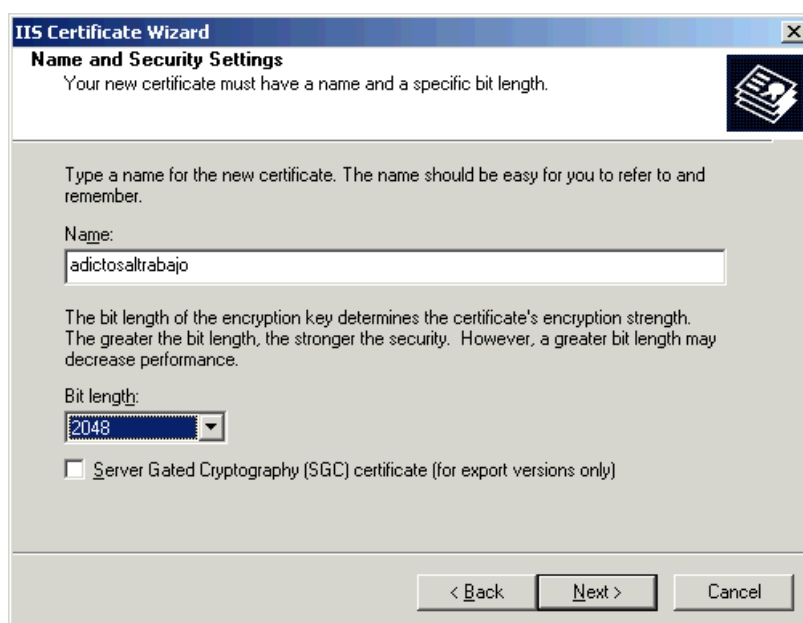
Solicitamos generar un nuevo certificado



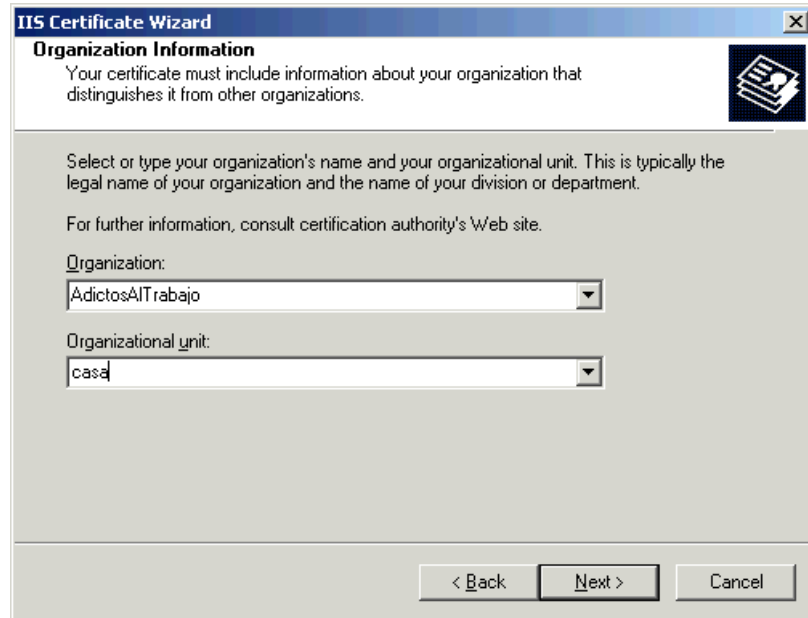
Podemos online solicitar a la CA directamente el certificado pero ... nosotros lo vamos a hacer más manual ...



Ahora, vamos a rellenar los datos necesarios para generar el certificado ... nombre para reconocerlo y longitud de la clave.



Ahora rellenamos datos sobre la organización



IIS Certificate Wizard

Organization Information
Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

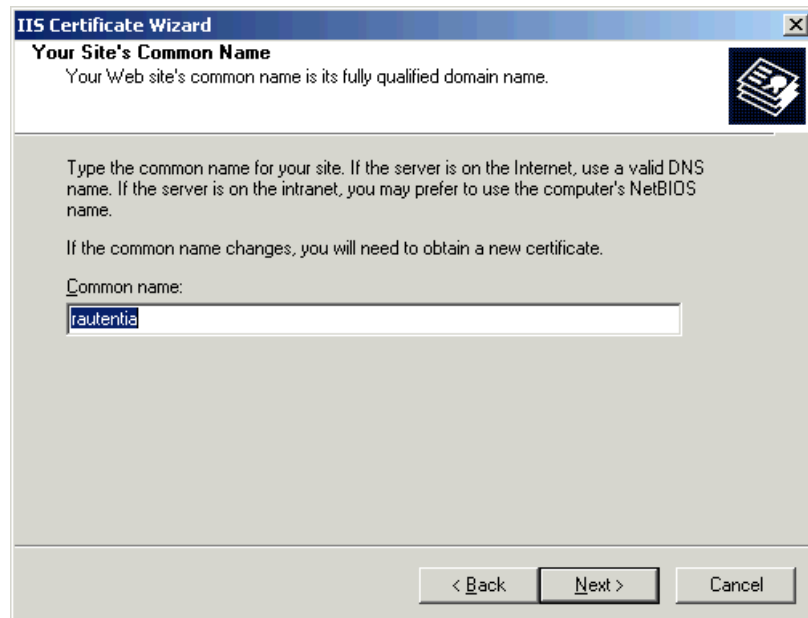
Organization:
AdictosAlTrabajo

Organizational unit:
casa

< Back Next > Cancel

Ahora, rellenamos el nombre de nuestra máquina. Este punto es vital porque un certificado solo vale para un nombre de dominio válido.

Como estoy en un portatil ... pongo el nombre de mi máquina



IIS Certificate Wizard

Your Site's Common Name
Your Web site's common name is its fully qualified domain name.

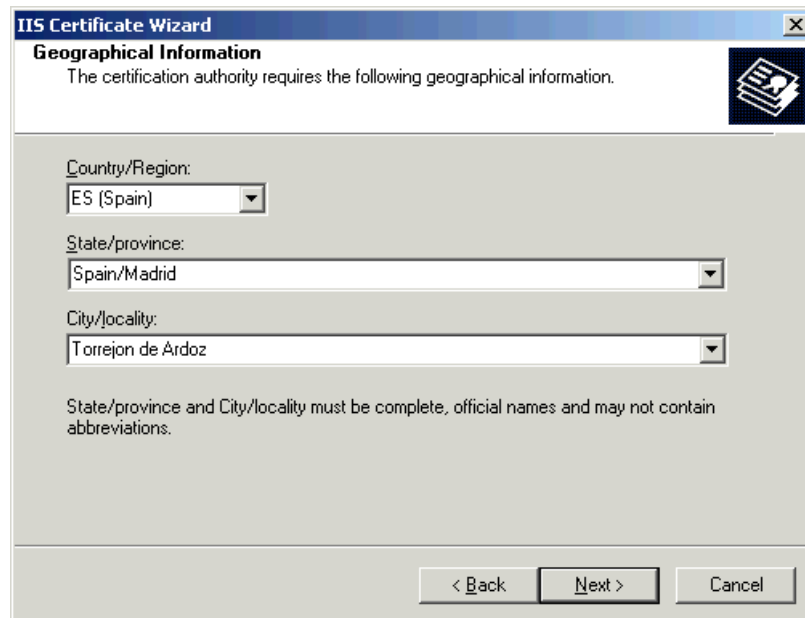
Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:
rautentia

< Back Next > Cancel

Introducimos la información geográfica



IIS Certificate Wizard

Geographical Information

The certification authority requires the following geographical information.

Country/Region:
ES (Spain)

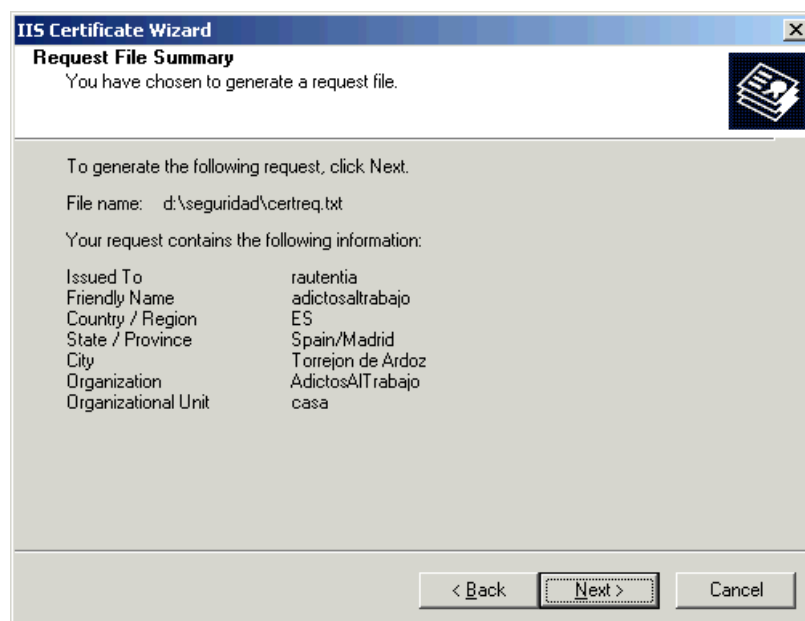
State/province:
Spain/Madrid

City/locality:
Torrejon de Ardoz

State/province and City/locality must be complete, official names and may not contain abbreviations.

< Back Next > Cancel

Comprobamos que los datos son los deseados y seguimos



IIS Certificate Wizard

Request File Summary

You have chosen to generate a request file.

To generate the following request, click Next.

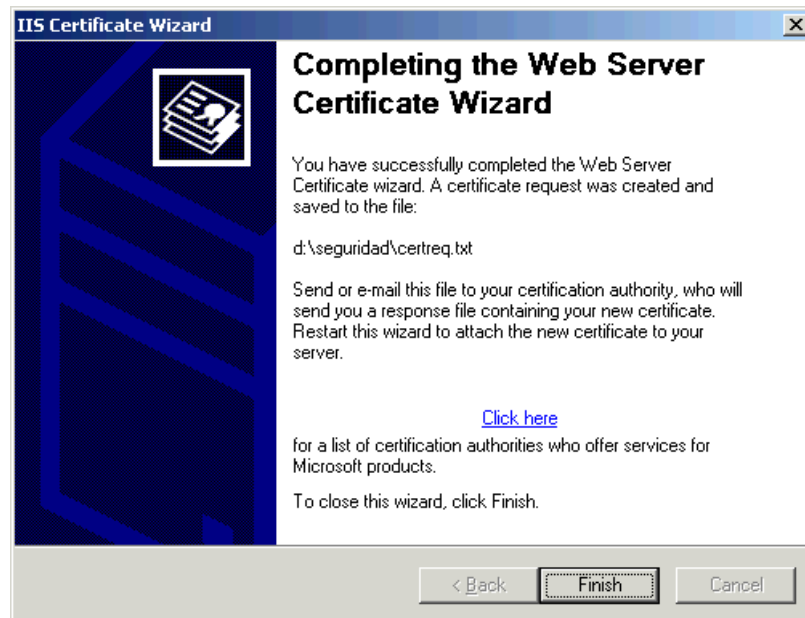
File name: d:\seguridad\certreq.txt

Your request contains the following information:

Issued To	rautentia
Friendly Name	adictosaltrabajo
Country / Region	ES
State / Province	Spain/Madrid
City	Torrejon de Ardoz
Organization	AdictosAlTrabajo
Organizational Unit	casa

< Back Next > Cancel

Comprobamos que se ha generado y el nombre del fichero



Creamos una Entidad Certificadora

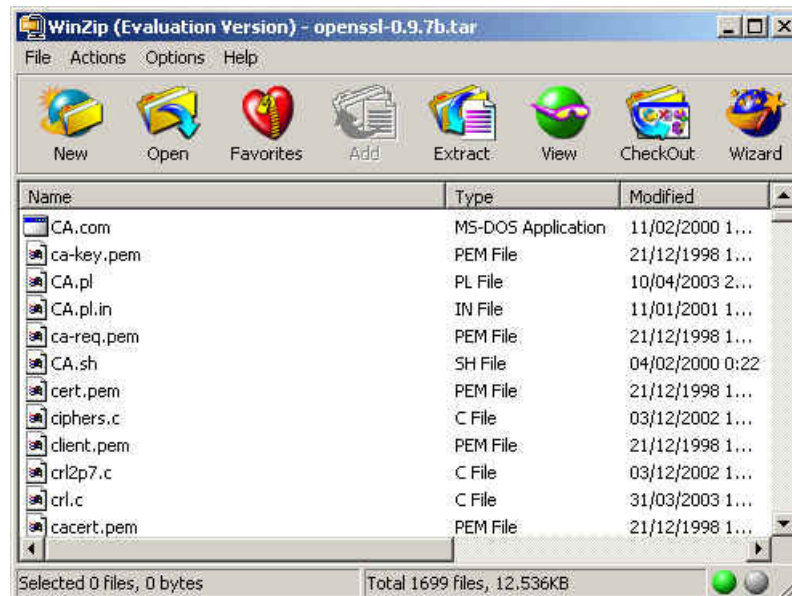
Si queremos obtener un certificado para nuestro servidor ... deberemos contactar con una empresa que los emita ... o bien... si lo queremos solo para probar o para usarlo en la intranet, nosotros podemos crear nuestra propia CA.

Lo vamos a hacer así..... para ello y sin profundizar más, necesitamos el software para emitir y firmar certificados

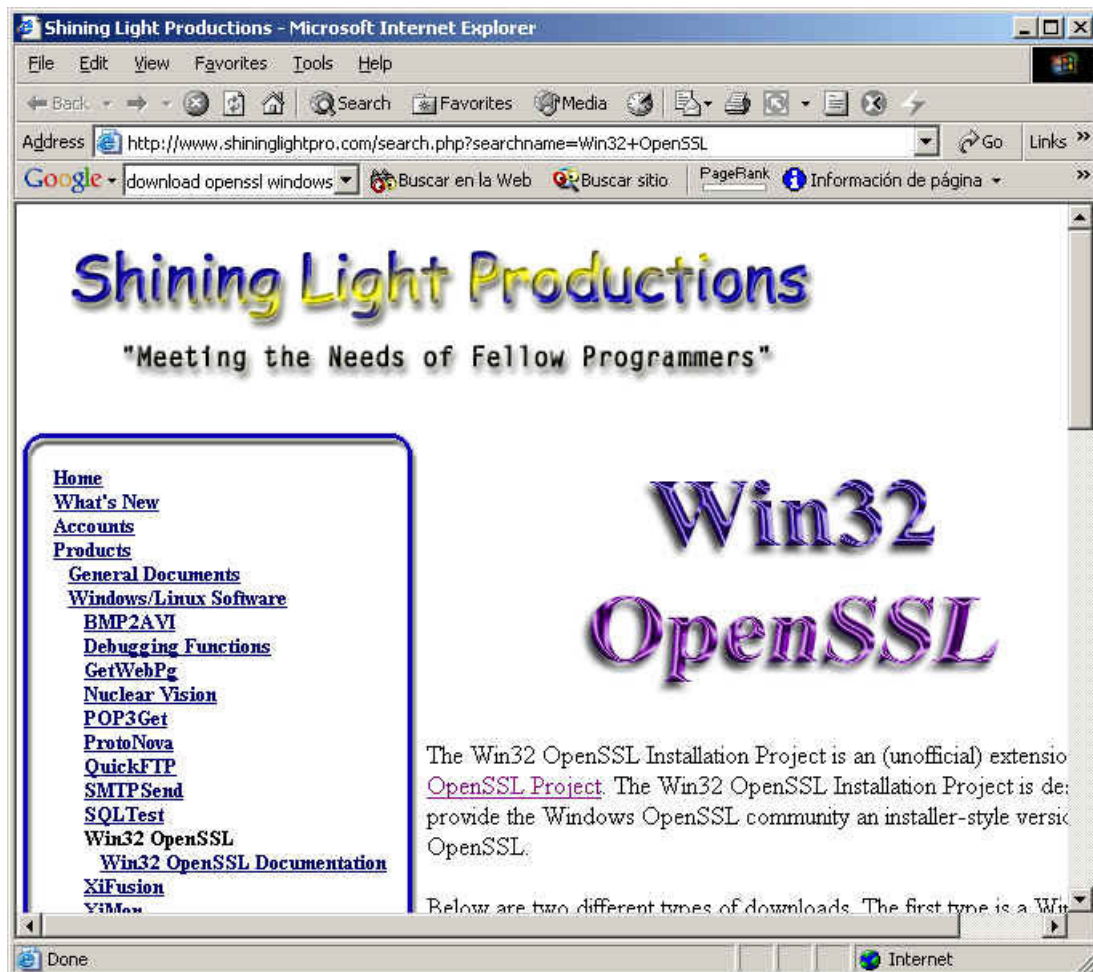
Uno de los programas más distribuidos para esta labor se llama OpenSSL



Como podemos observar, OpenSSL viene en código fuente. No lo vamos a compilar porque ya hay gente que lo hace por nosotros.

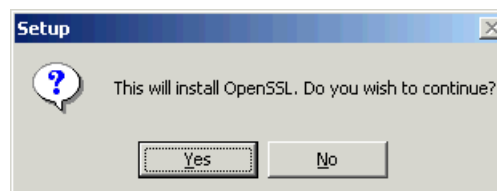


Buscamos una distribución ya compilada

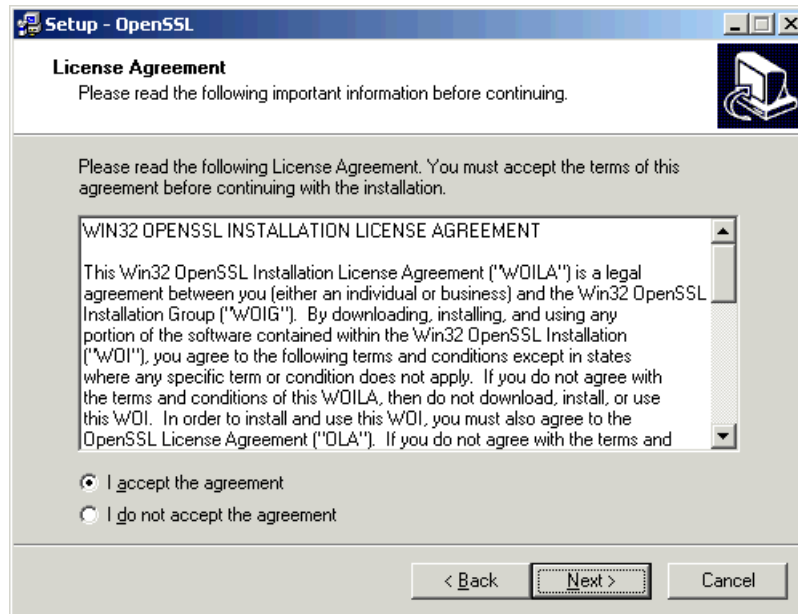


Que suerte tenemos ... así que la instalamos (esto en entornos reales hay que pensárselo mucho.. y verificar que nadie ha modificado los ficheros.... sería lamentable que instalásemos software virulento en nuestro Web seguro

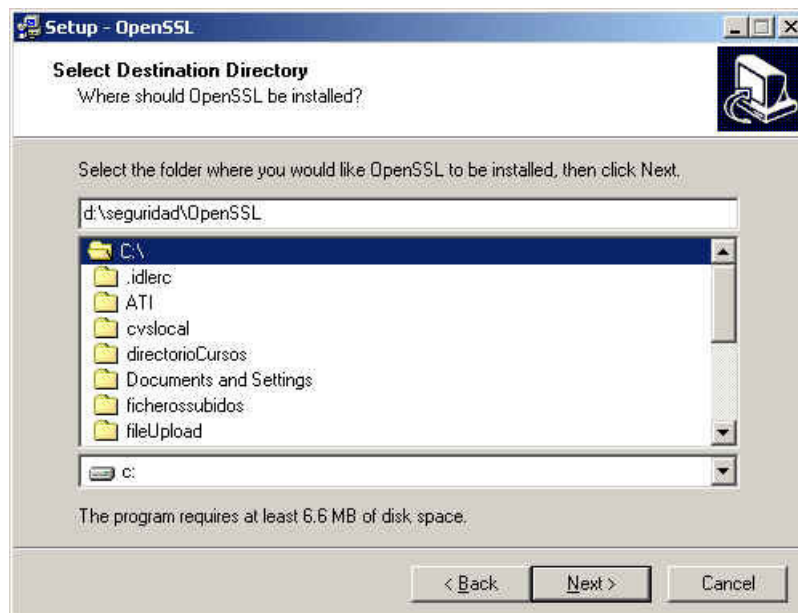
Nos descargamos los ficheros e instalamos.



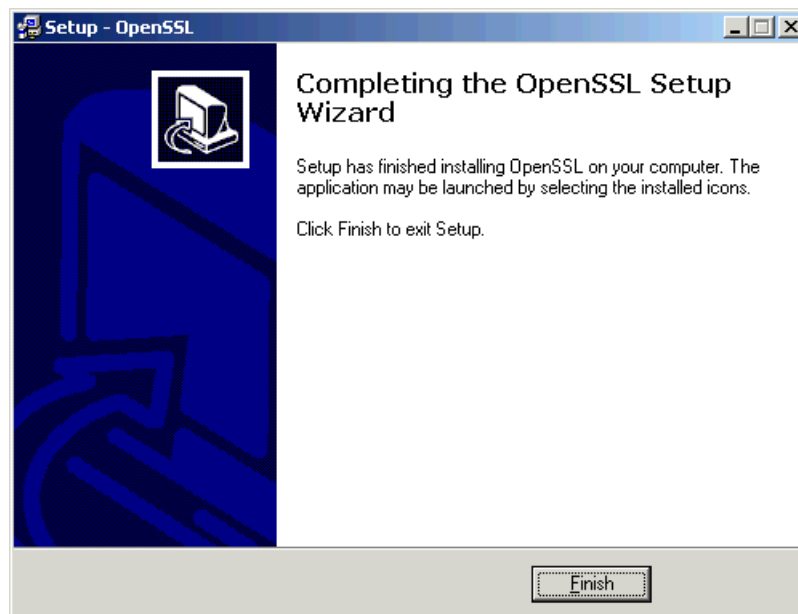
Hay que leerse la licencia



Seleccionamos el directorio destino



Y no nos tenemos que preocupar de mucho más (excepto de incluir el directorio de trabajo en el path)



Generación de claves de la CA

El primer paso que debemos dar es generar una clave privada para la CA. Con la clave privada de la CA... firmaremos la información enviada por el servidor Web (descripción y clave pública del Web). Cuando un cliente reciba la clave pública del Web, puede verificar que es correcto .. gracias a que esta firmado por la CA

Sin enrollarnos más, generamos la clave privada... nos pide una contraseña para protegerla

openssl genrsa -des3 -out cakey.pem 2048

```

C:\WINNT\System32\cmd.exe
D:\seguridad>openssl genrsa -des3 -out cakey.pem 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for cakey.pem:
Verifying - Enter pass phrase for cakey.pem:
D:\seguridad>_

```

La clave privada tiene un aspecto como este no os la muestro entera porque las claves privada son secretas ;)

```

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC,E6C2CECEBE48F032

GDYQKGN8NvxWoU0gR1hfzMSI1HyUdR3st7IbJdEdfohaXIWMJw7ztWI
Tuaxa+9+hs0I+IOncnwqCmY3GIB5TMb8mjdQpGMcb96Nh4A7fHMgXU
6GGbveD+R/ I1Z52oeARZ+DFhwLBPC9yco+yV8sFZ7Ji9E2Yu2QoLN5u
r3TQ8svmLPLauG29m9AL6uHHXyasHMWCWBnEipIUoNjgUHtp6nAebcp
lnt5QwMO84SpcBTv5zjs2SjpsdTzXSYJxvc4g4A4rtwQymxNi7XzGY
ni2J5vQwoJo0Miij5jnon7apIvbc7VarDB/72kbJM6bCGVAn/1COJW
fpMQKDTCogstjsEz7dx1iNIVBKEgzwROCz6I5rovbAspOHa13H8sRW
qfR4qaPrD3gWgyIVEguebVbdat/IQpZtRQIOv66wKwXJFfuFJbKq+VU
UiZSipkoMf4wYVPAuKry7FHxMan/WlwuiCkHs2JuNPEO/OtGGwsNOKw
XoUb915jgOt4PBGistWBpmCJJiOLY6TRL5fKszOO1XA6v58F6Rzs+gp
DCaePbMtNROkLC8icKw/X4ztPHN5NidDbfOj/8rhzEsFFWcBBT/P+Yo
-----END RSA PRIVATE KEY-----

```

Ahora, hay que crear un certificado digital de la CA que contendrá información sobre la misma.. rellenamos toda la información que nos pide. Por línea de comando decimos que es válido por un año

```
openssl req -new -x509 -key cakey.pem -out cacert.pem -days 365
```

```

C:\WINNT\System32\cmd.exe

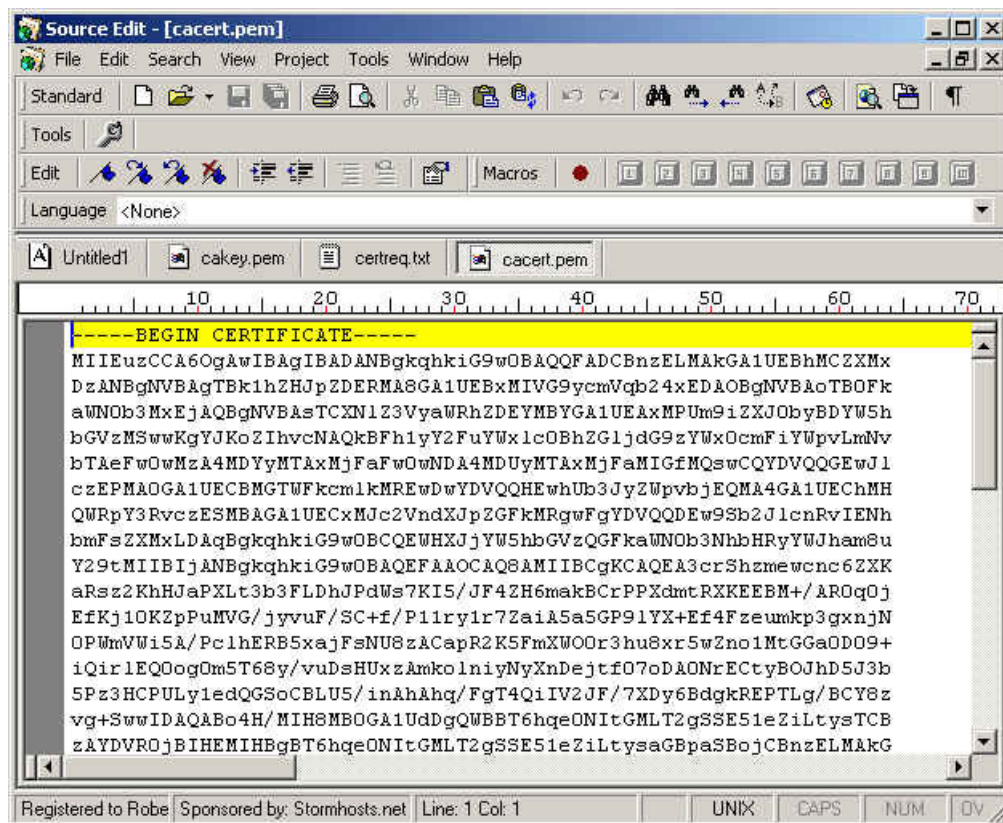
D:\seguridad>openssl genrsa -des3 -out cakey.pem 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for cakey.pem:
Verifying - Enter pass phrase for cakey.pem:

D:\seguridad>openssl req -new -x509 -key cakey.pem -out cacert.pem -days 365
Enter pass phrase for cakey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:es
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Torrejon
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Adictos
Organizational Unit Name (eg, section) []:seguridad
Common Name (eg, YOUR name) []:Roberto Canales
Email Address []:rcanales@adictosaltrabajo.com

D:\seguridad>

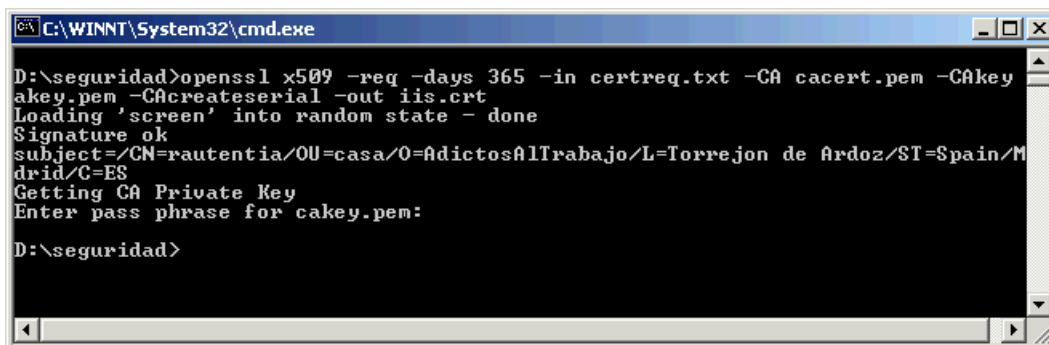
```

Vemos como queda el certificado

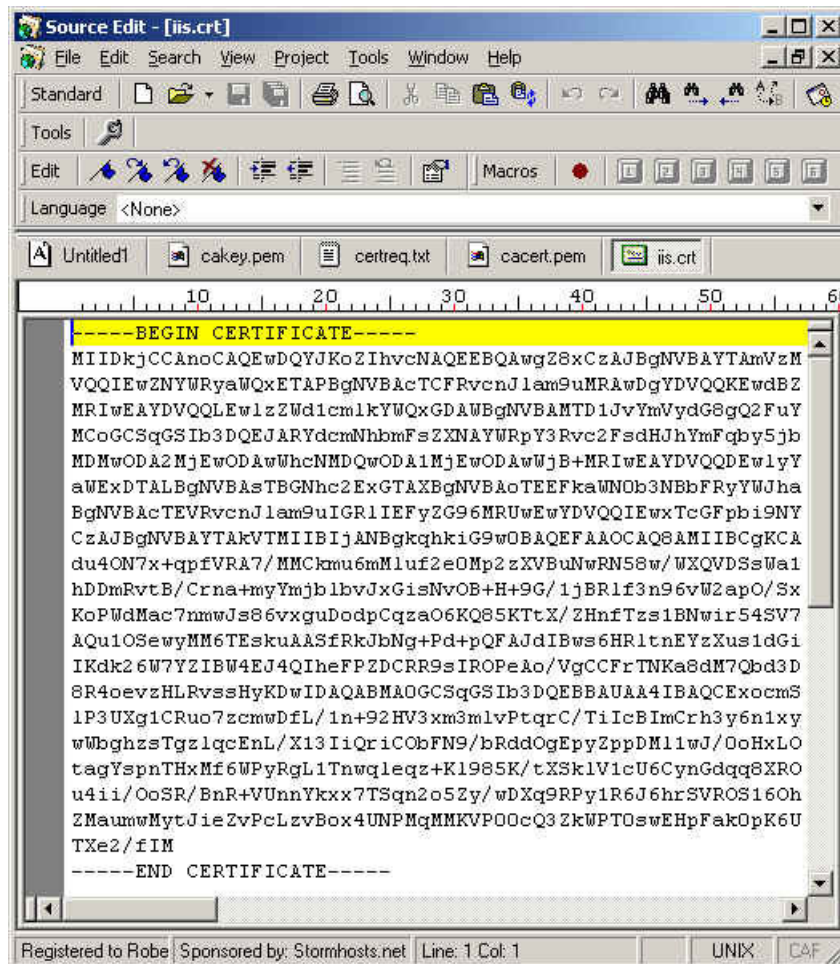


Ahora, creamos el certificado digital de nuestro Web

```
openssl x509 -req -days 365 -in certreq.txt -CA cacert.pem -CAkey cakey.pem -CAcreateserial -out iis.crt
```

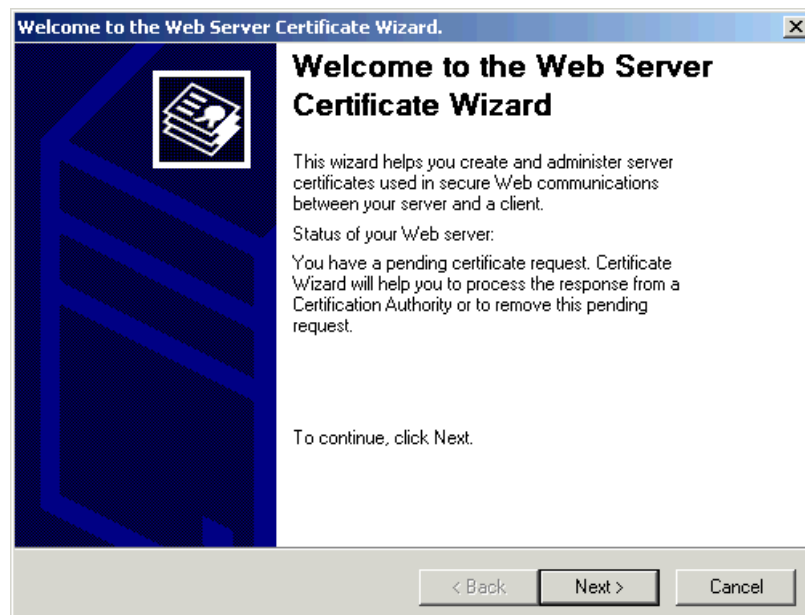


Y vemos el certificado generado

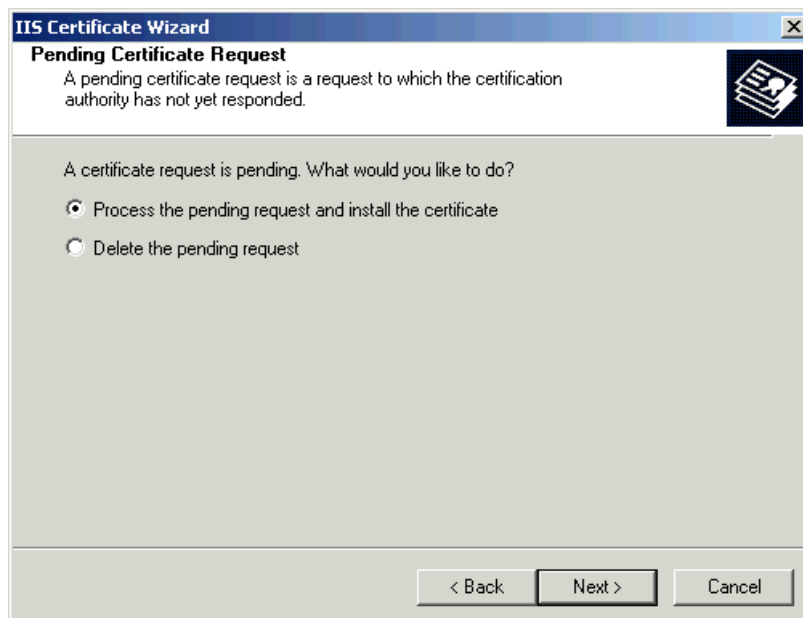


Importar el certificado en IIS

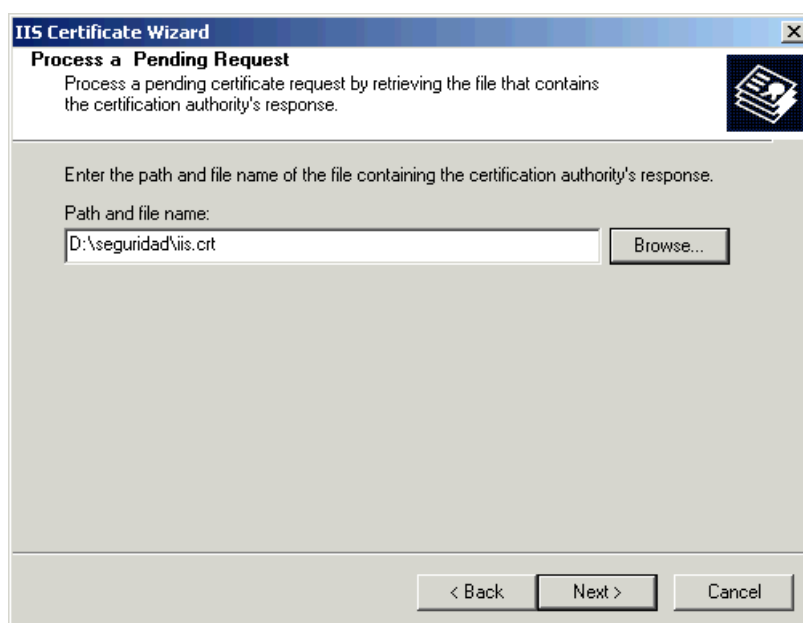
Ahora, volvemos a abrir la ventana de certificados de IIS...



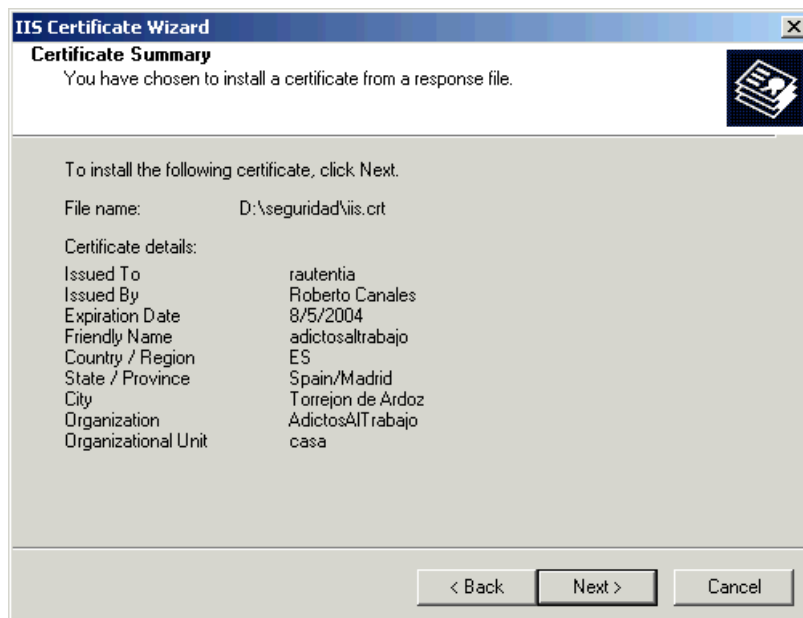
Y esta vez seleccionamos ... procesar una petición pendiente



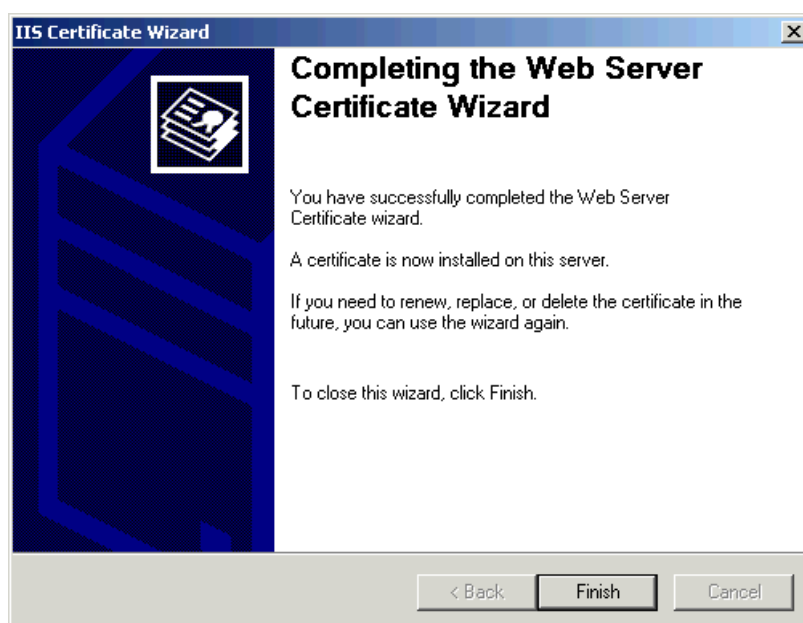
Indicamos el trayectos del certificado que hemos generado



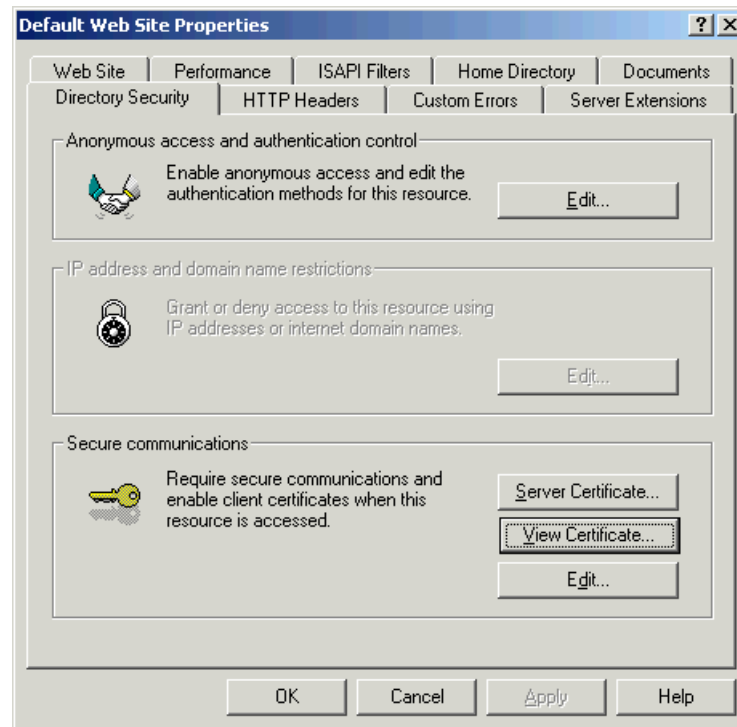
Vemos que los datos son correctos



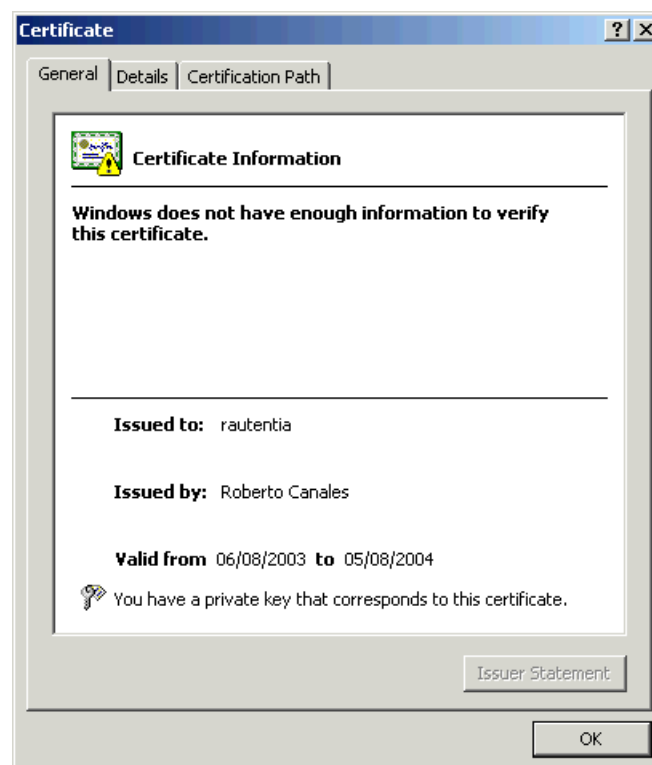
Y comprobamos que todo fue bien



Podemos ver ahora el certificado instalado

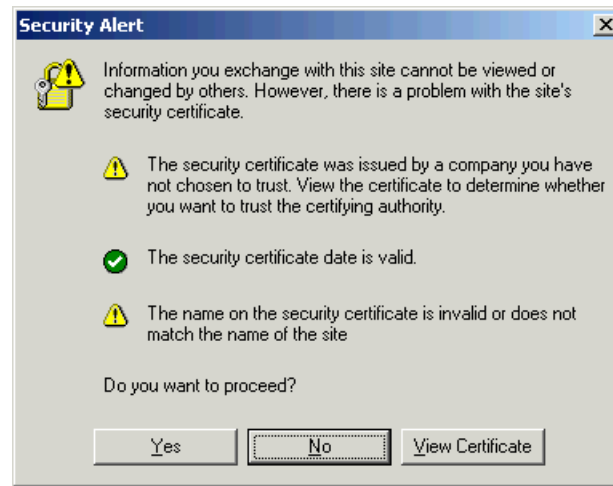


Y comprobamos el resultado. Podemos ver que nos advierte que no tiene información necesaria para verificar el certificado eso es porque no reconoce la CA (no esta dentro su lista de confianza.. aunque podriamos añadirla, añadiendo su certificado)



Probar el servidor via HTTPS

Ahora accedemos al navegador.. **https://localhost** podemos ver que que nos dice que hay algunos problemas fundamentalmente porque no reconoce la CA ...



Aceptamos y ... **ya está** nuestro servidor a través de SSL



En otros tutoriales.. veremos otras técnicas ... como la tunelización genérica de protocolos y tuneles ssh, Estas técnicas nos permitirán aumentar la seguridad de los sistemas ya construidos, aunque no tengan soporte directo de seguridad.



[Sobre el Autor ..](#)

Si desea contratar formación, consultoría o desarrollo de piezas a medida puede contactar con

Gestión de contenidos

[Autentia S.L.](#) Somos expertos en:
J2EE, C++, OOP, UML, Vignette, Creatividad ..
 y muchas otras cosas

Nuevo servicio de notificaciones

Si deseas que te enviemos un correo electrónico cuando introduzcamos nuevos tutoriales, inserta tu dirección de correo en el siguiente formulario.

Subscribirse a Novedades	
e-mail	
	<input type="button" value="Enviar"/>

Otros Tutoriales Recomendados ([También ver todos](#))

Nombre Corto

[Activación de la seguridad en Apache](#)

[Activar soporte SSL en Tomcat](#)

Descripción

Alejandro Pérez nos enseña como securizar Apache a través de autenticación básica y certificados de seguridad SSL.

Os mostramos como activar el acceso SSL en Tomcat, utilizando certificados generados por Keygen (java)

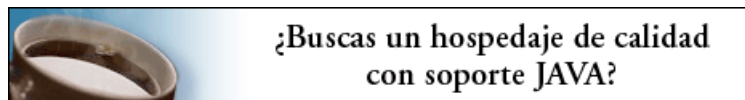
Nota: Los tutoriales mostrados en este Web tienen como objetivo la difusión del conocimiento.

Los contenidos y comentarios de los tutoriales son responsabilidad de sus respectivos autores.

En algún caso se puede hacer referencia a marcas o nombres cuya propiedad y derechos es de sus respectivos dueños. Si algún afectado desea que incorporemos alguna reseña específica, no tiene más que solicitarlo.

Si alguien encuentra algún problema con la información publicada en este Web, rogamos que informe al administrador rcanales@adictosaltrabajo.com para su resolución.

[Patrocinados por enredados.com Hosting en Castellano con soporte Java/J2EE](#)



www.AdictosAlTrabajo.com Optimizado 800X600