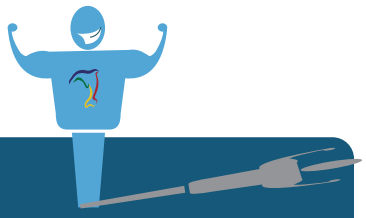
autentia

Avenida de Castilla,1 - Edificio Best Point - Oficina 21B
28830 San Fernando de Henares (Madrid)
tel./fax: +34 91 675 33 06
info@autentia.com - **www.autentia.com**

¿**Qué ofrece** Autentia Real Business Solutions S.L?

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

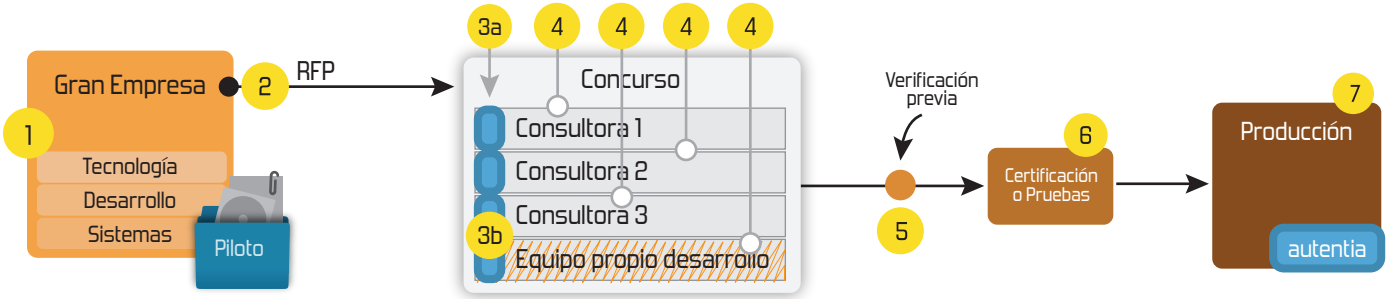
1. Desarrollo de componentes y proyectos a medida



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

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

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

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

Compartimos nuestro conocimiento en:
www.adictosaltrabajo.com

Para más información visítenos en:
www.autentia.com

Tutorial desarrollado por:
Roberto Canales Mora 2003-2005
Creador de AdictosAlTrabajo.com y

Director General de Autentia S.L.

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 policia 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 gerena dos claves: Una privada que se guarda de un modo muy seguro y una pública que se dá a todo el mundo. Estas claves están matemáticamente relacionadas, de tal modo que lo que se codifica con una clave, solo se desencripta con la otra.

En el mundo Web, este tercero de confianza se denomína CA (entidad certificadora) la cual, previa presentación de documentacion 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).

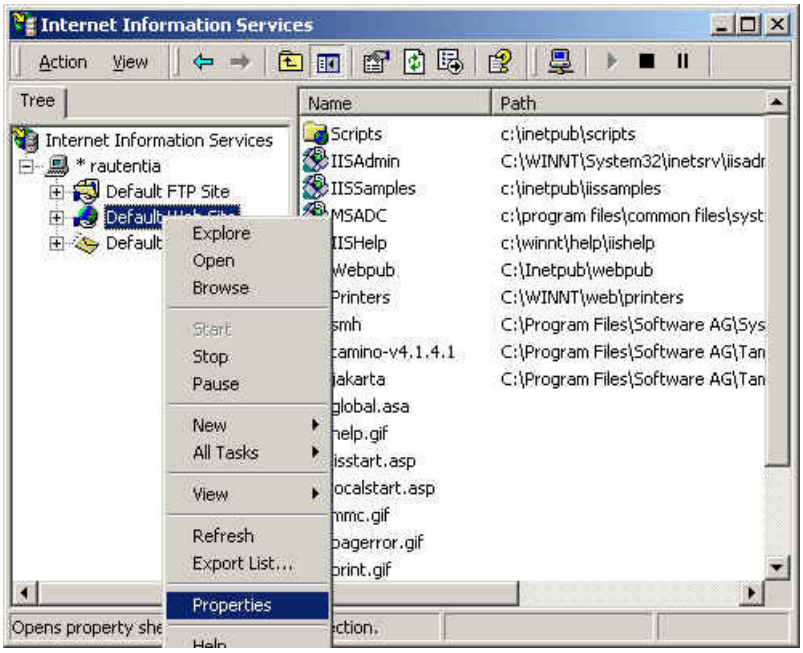
Este fichero es lo que se denomina un certificado digital (La entidad certificadora emite y firma un certificado digital). Este certificado digital, contiene, ademas de información identificativa del servidor, una clave (la clave pública) del servidor Web. Como hemos dicho, esta clave es muy curiosa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

Asi 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 desencriptar la información ....

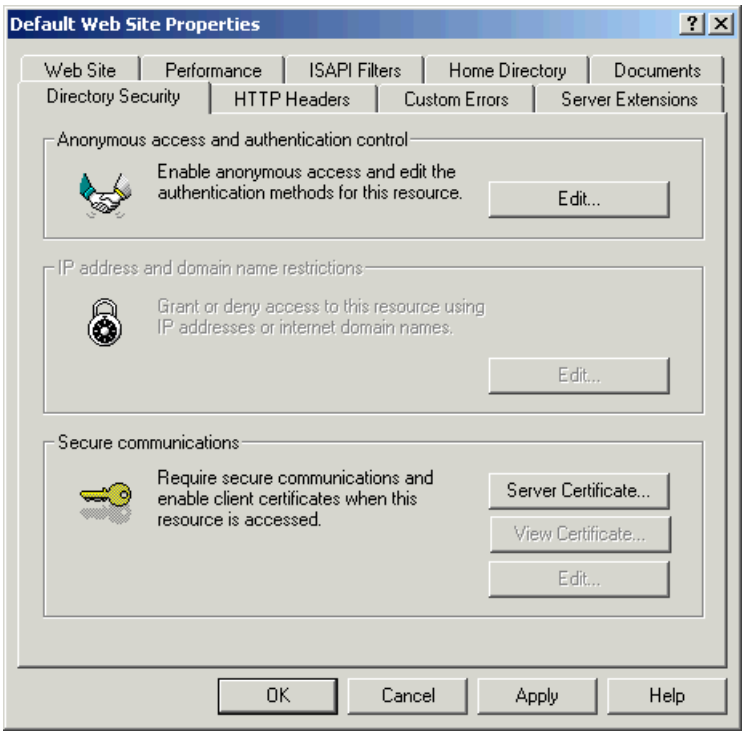
Lo vamos a dejar aqui ... el movimiento se demuestra andando

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



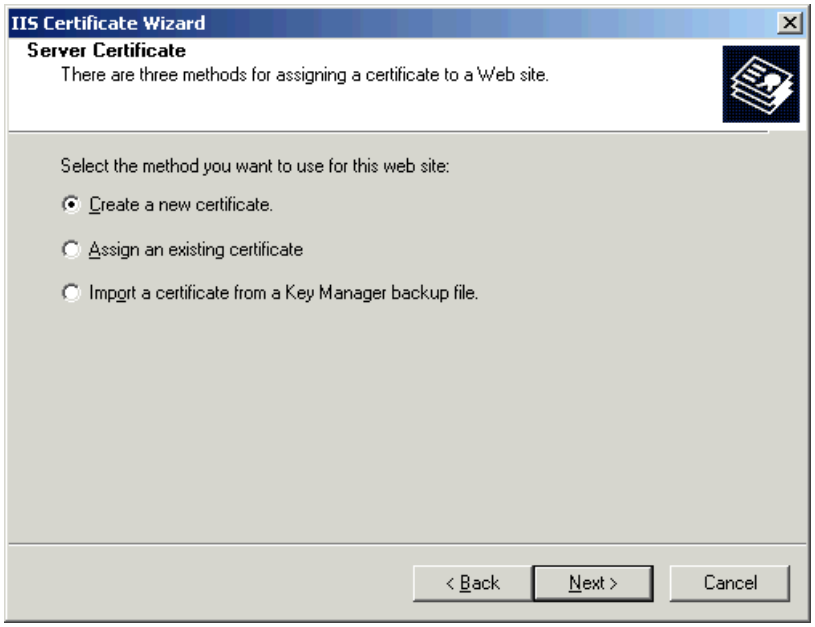
En la lengüeta de seguridad, pichamos en **Server Certificate**



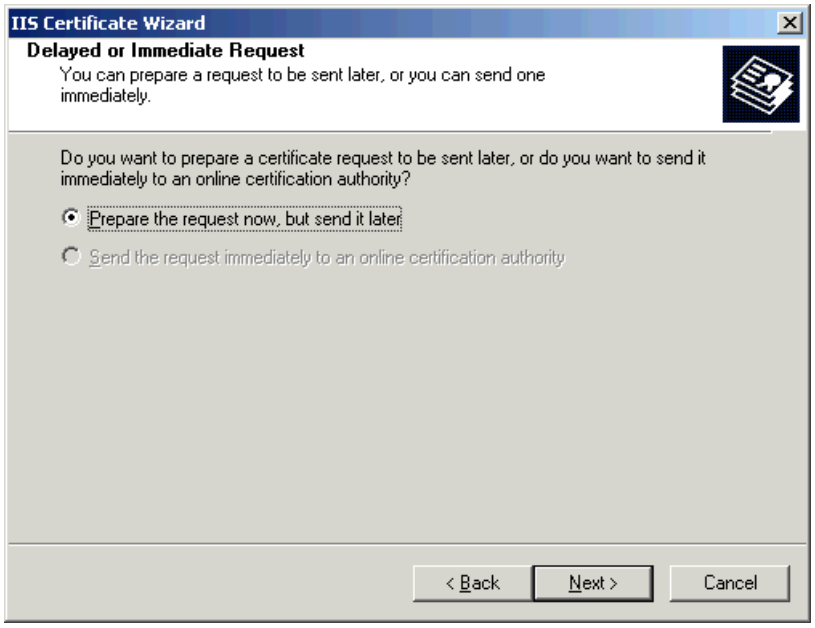
IIS hace casi de modo automático todas las labores necesarias para solicitar e instalar un certificado digital.

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.

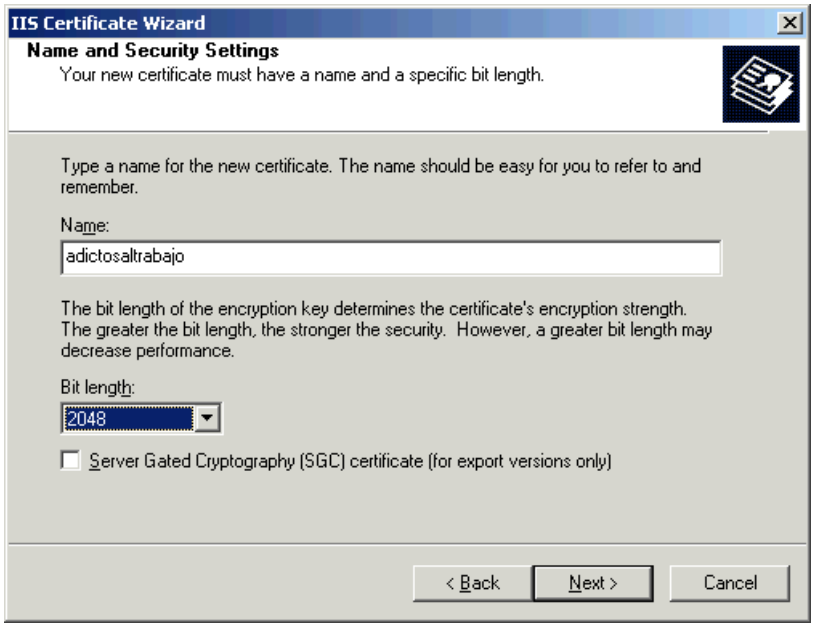
Solicitamos generar un nuevo certificado



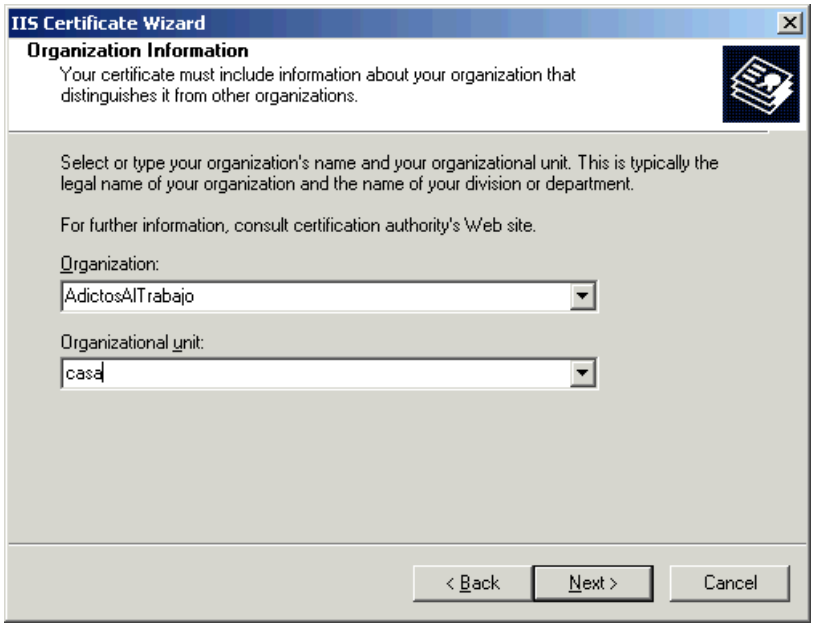
Podemos online solicitar a la CA directamente el certificado pero ... nosotros lo vamos a hacer más manual ...



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

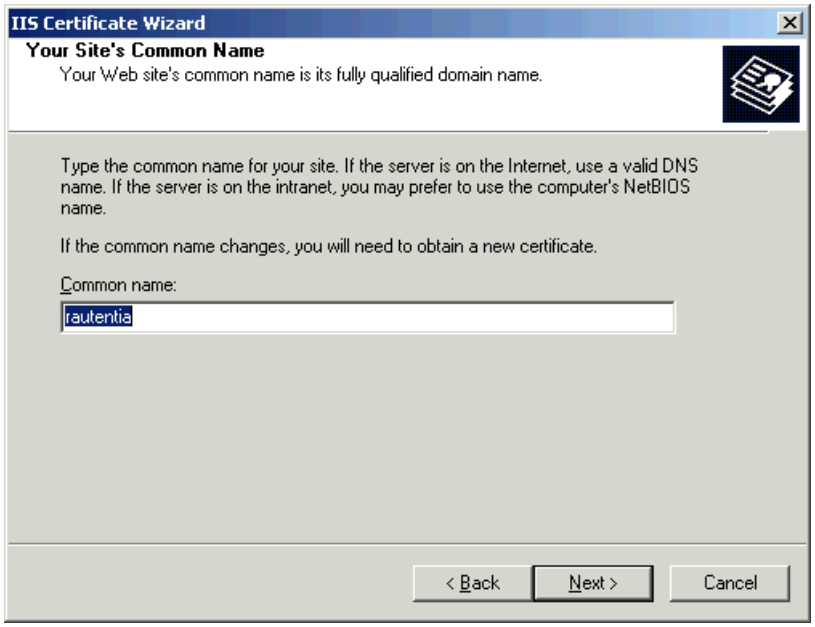


Ahora rellenamos datos sobre la organización

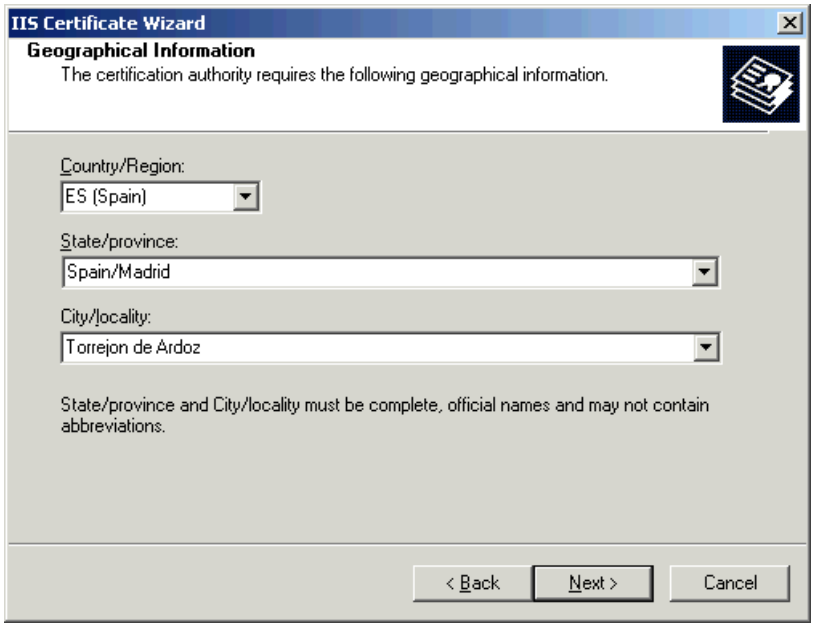


Ahora, rellenamos el nombre de nuestra máquina. Este punto es vital porque un certificado solo vale para un nombre de dominio válido.

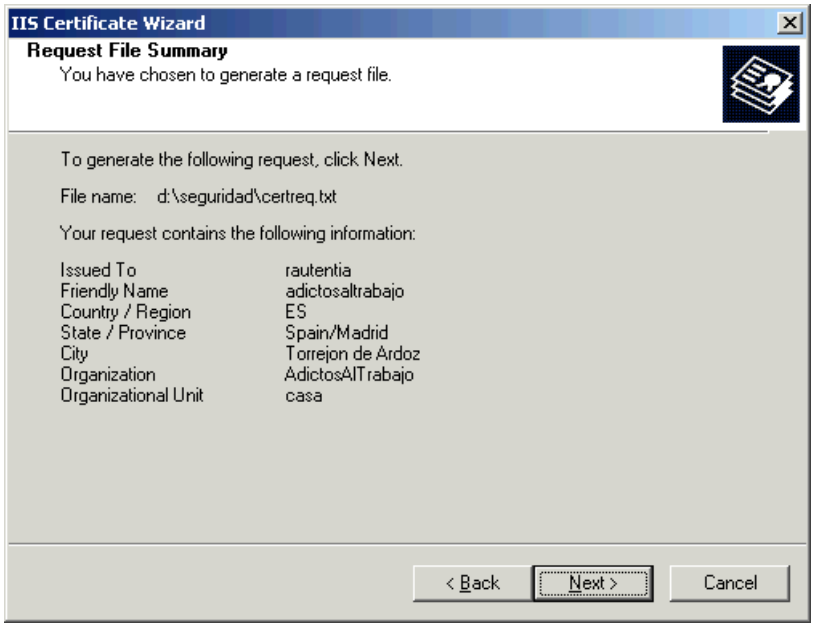
Como estoy en un portatil ... pogo el nombre de mi máquina



Introducimos la información geográfica



Comprobamos que los datos son los deseados y seguimos



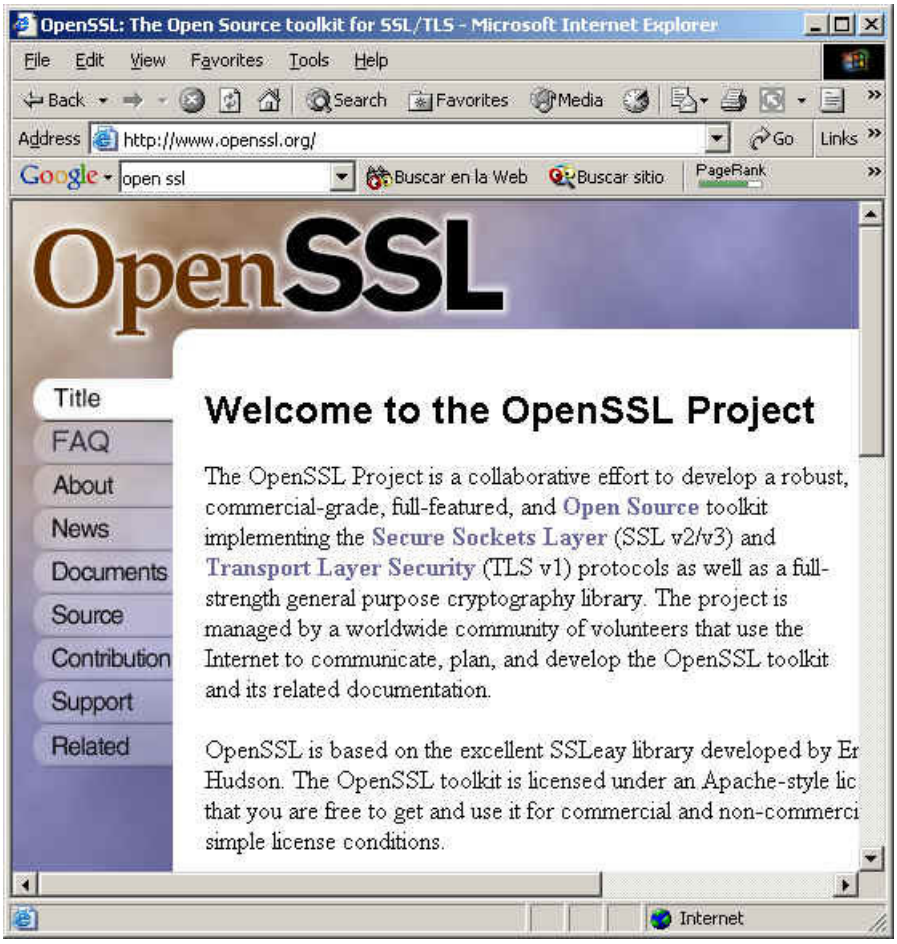
Comprobamos que se ha generado y el nombre del fichero

Creamos una Entidad Certificadora

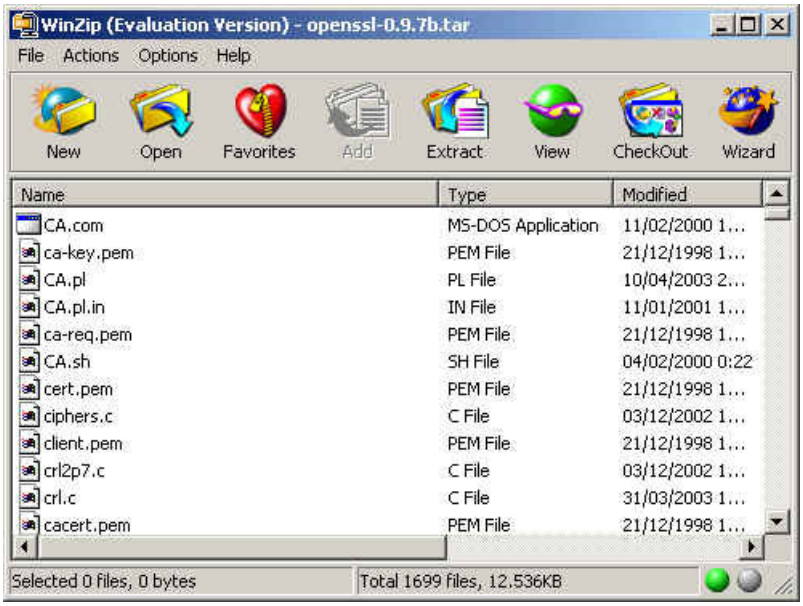
Si queremos obtener un certificado para nuestro servidor ... deberemos contactar con una empresa que los emita ... o bien... si lo queremos solo para probar o para usarlo en la intranet, nosotros podemos crear nuestra propia CA.

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

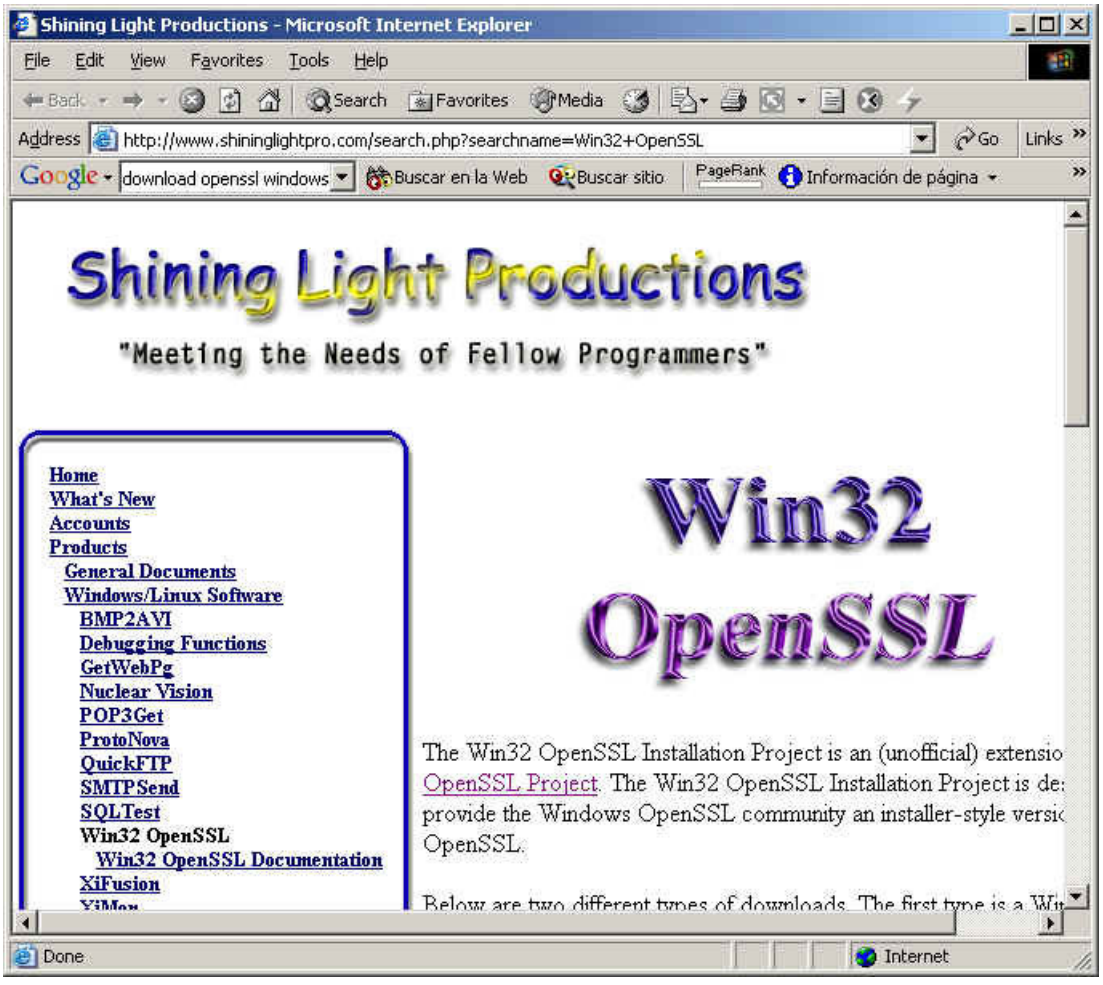
Uno de los programas más distribuidos para esta labor se llama OpenSSL



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

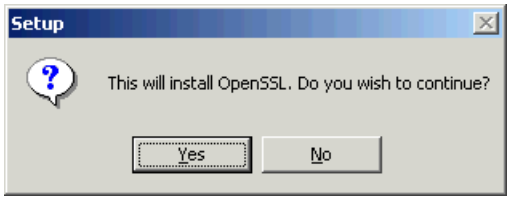


Buscamos una distribución ya compilada .....

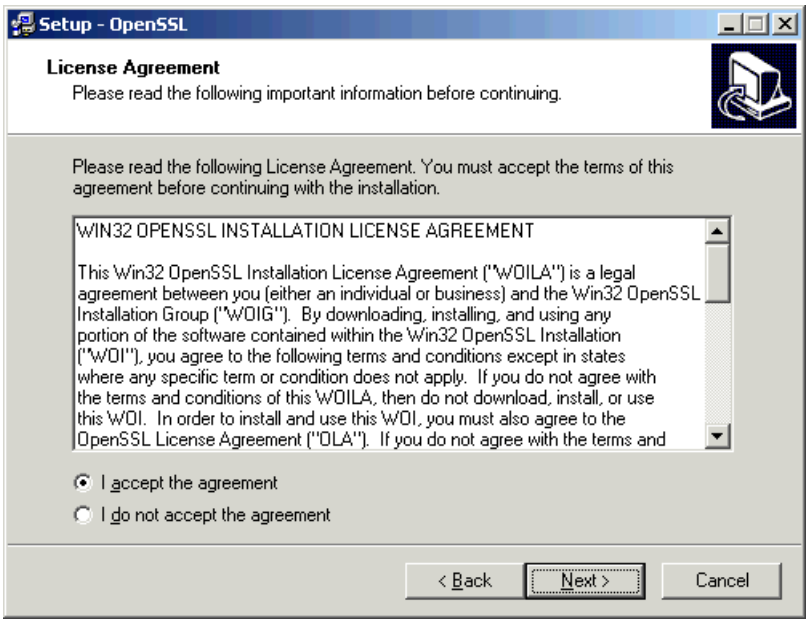


Que suerte tenemos ... asi que la instalamos (esto en entonos reales hay que pensarselo mucho.. y verificar que nadie ha modificado los ficheros.... sería lamentable que instalasemos software virulento en nuestro Web seguro ....).

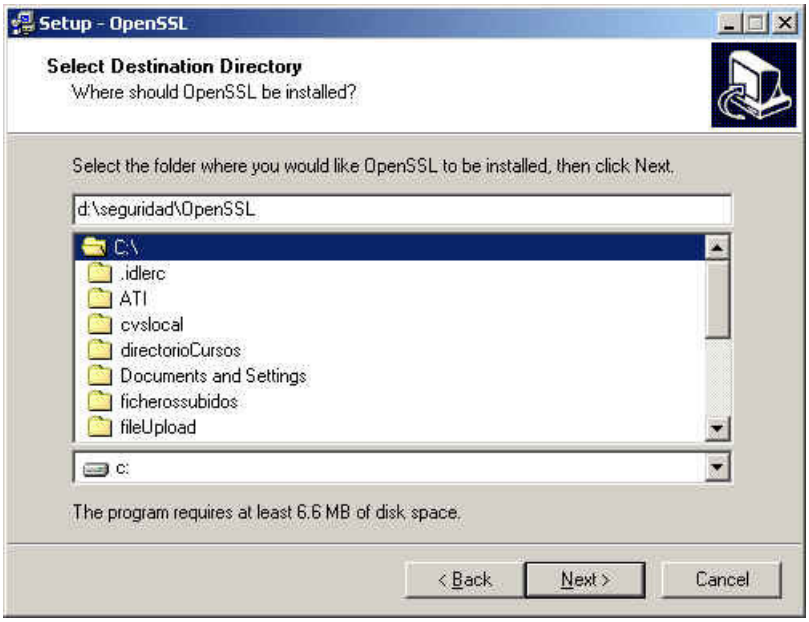
Nos descargamos los ficheros e instalamos.



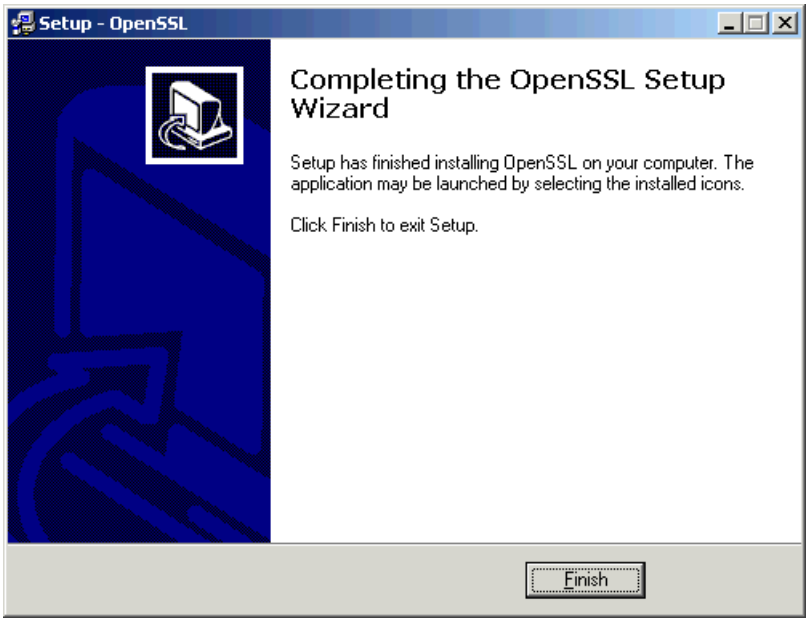
Hay que leerse la licencia



Seleccionamos el directorio destino



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

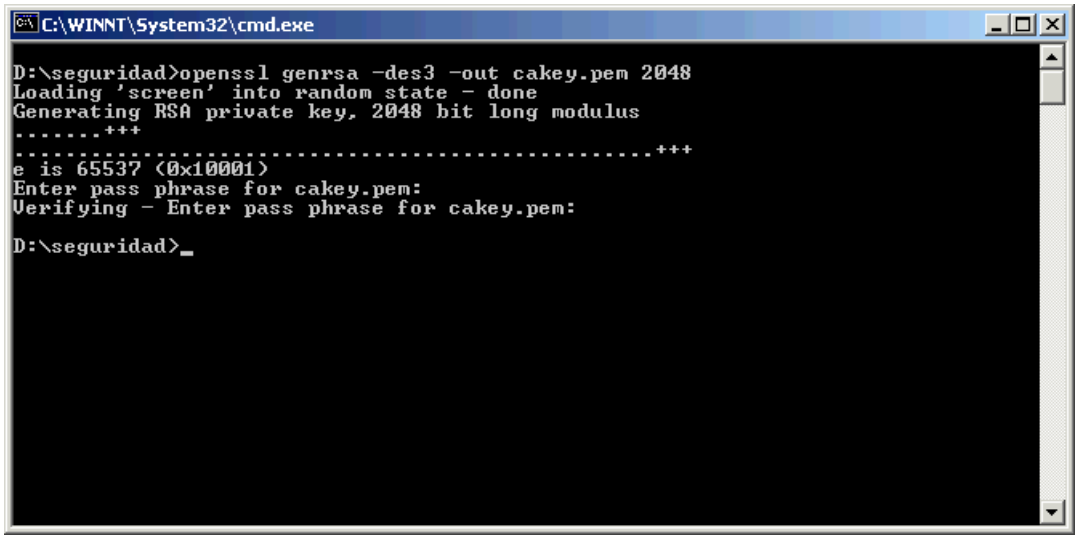


Generación de claves de la CA

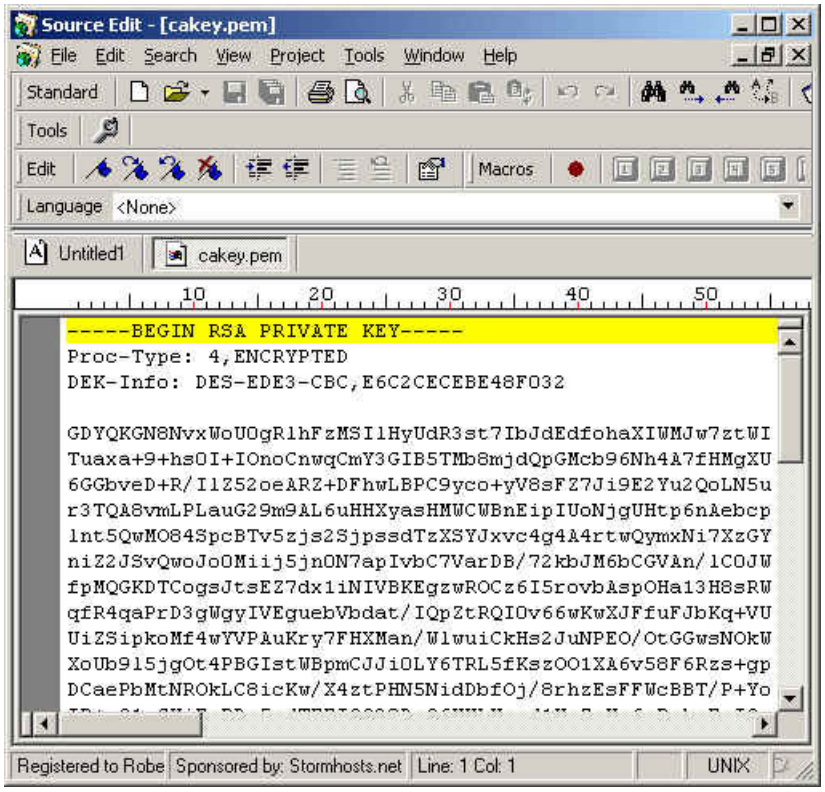
El primer paso que debemos dar es generar una clave privada para la CA. Con la clave privada de la CA... firmaremos la información enviada por el servidor Web (descripción y clave pública del Web). Cuando un cliente reciba la clave pública del Web, puede verificar que es correcto .. gracias a que esta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

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

openssl genrsa -des3 -out cakey.pem 2048

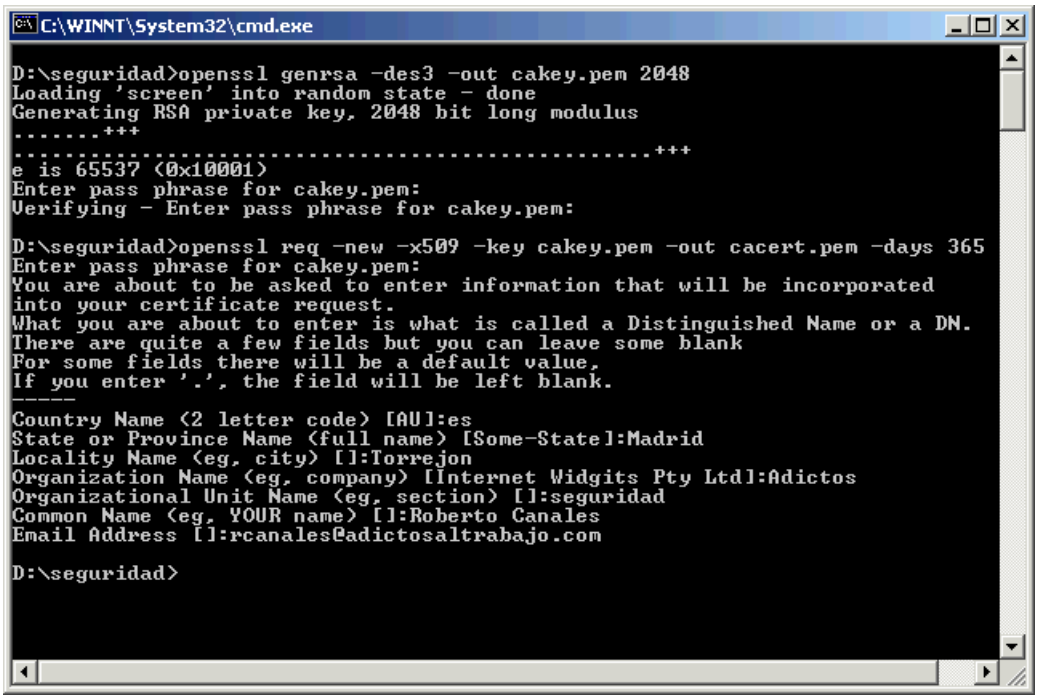


La clave privada tiene un aspecto como este ..... no os la muestro entera porque las claves privada .... son secretas ;)

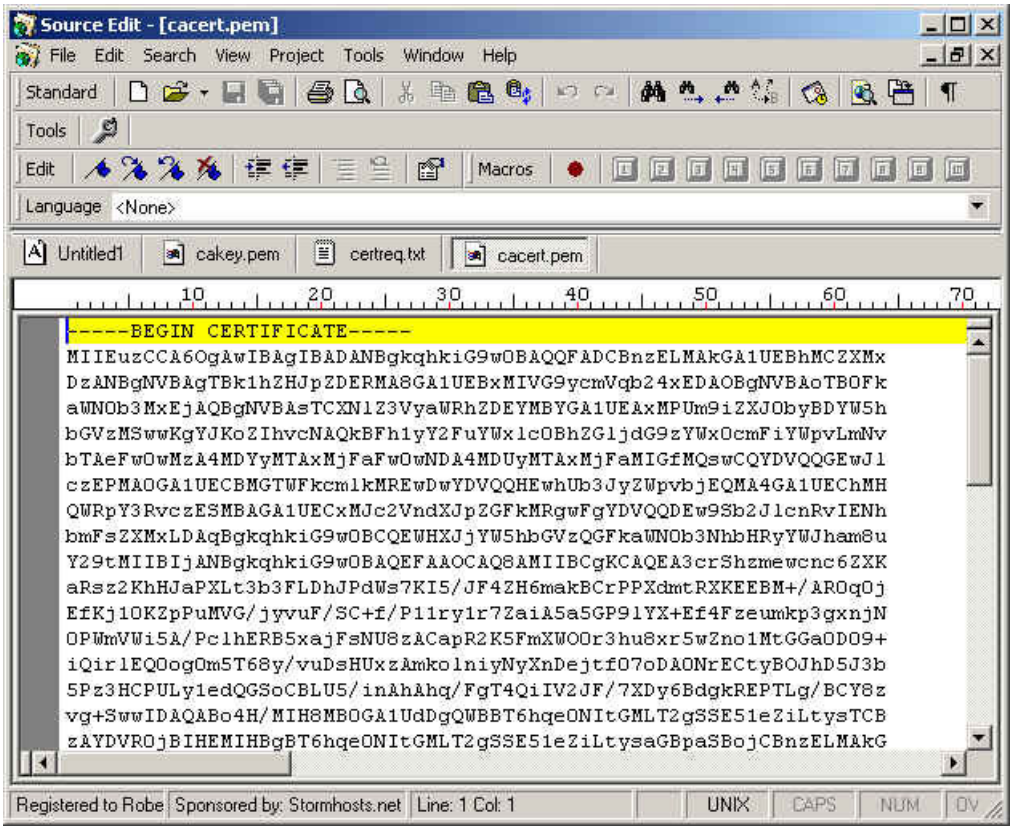


Ahora, hay que crear un certificado digital de la CA que contendrá información sobre la misma.. rellenamos toda la información que nos pide. Por linea de comando decimos que es válido por un año

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

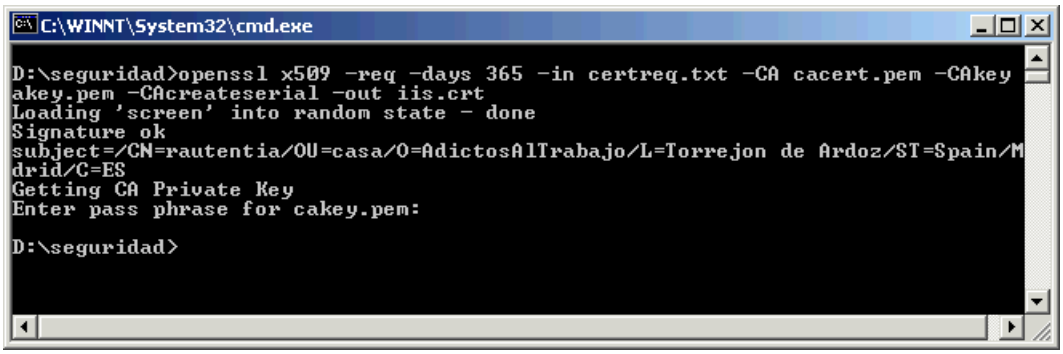


Vemos como queda el certificado

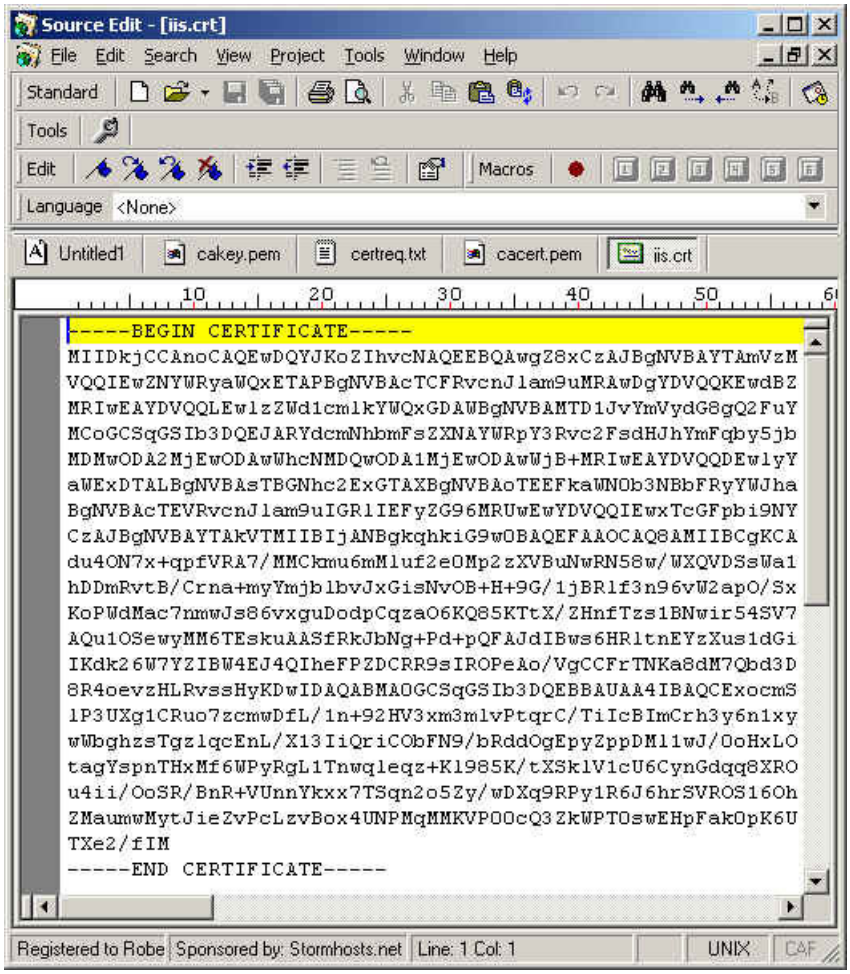


Ahora, creamos el certificado digital de nuestro Web .....

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



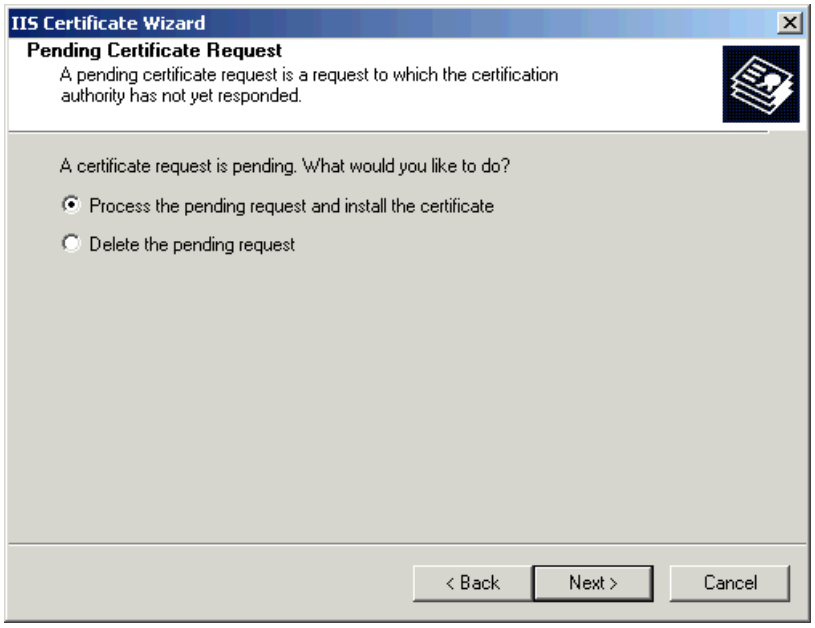
Y vemos el certificado generado



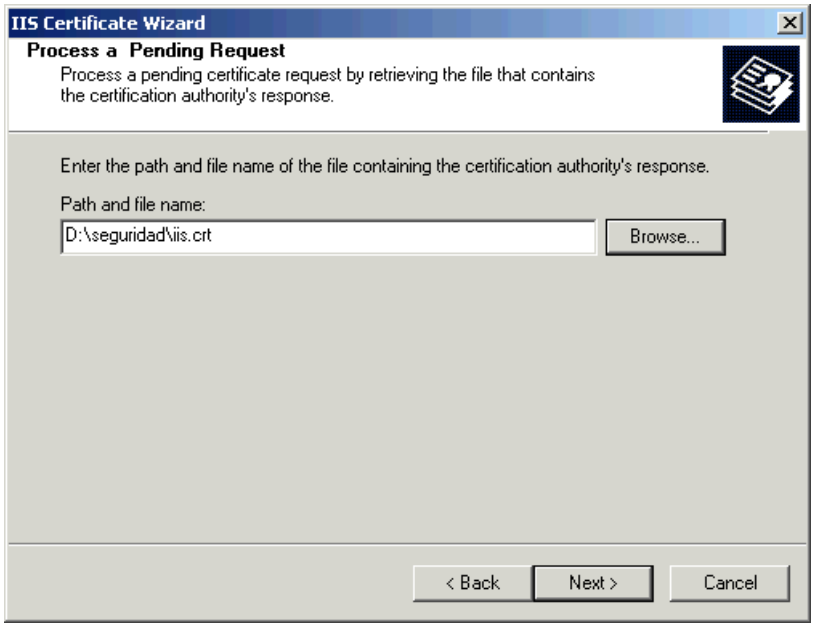
Importar el certificado en IIS

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

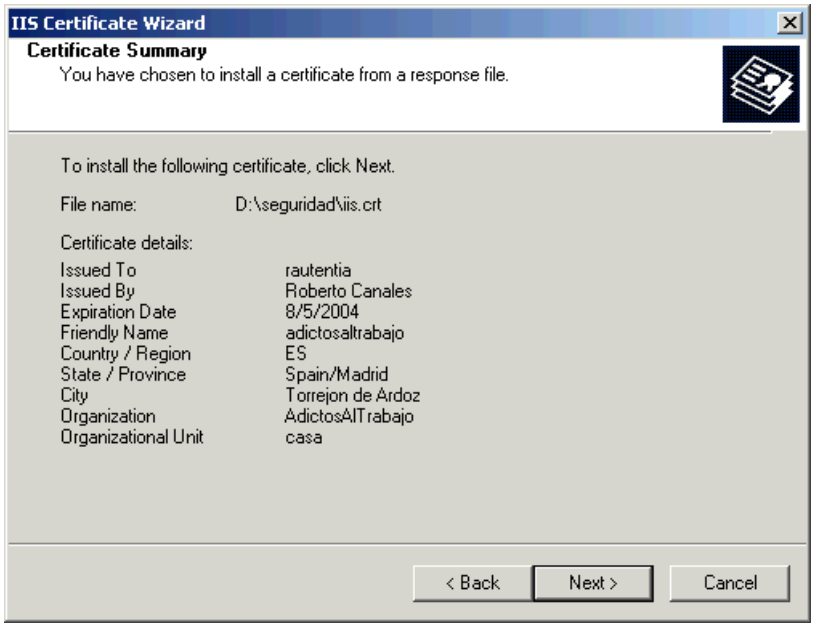
Y esta vez seleccionamos ... procesar una petición pendiente



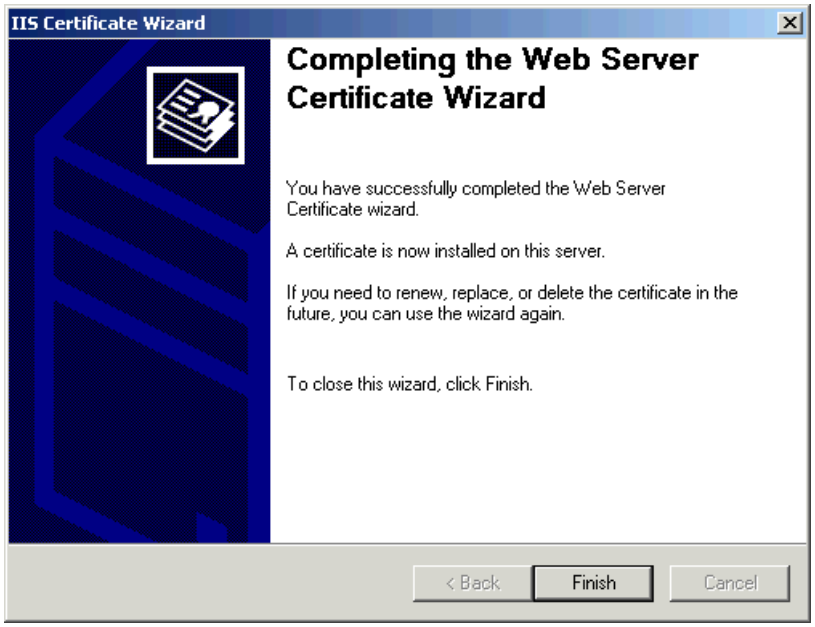
Indicamos el trayectos del certificado que hemos generado



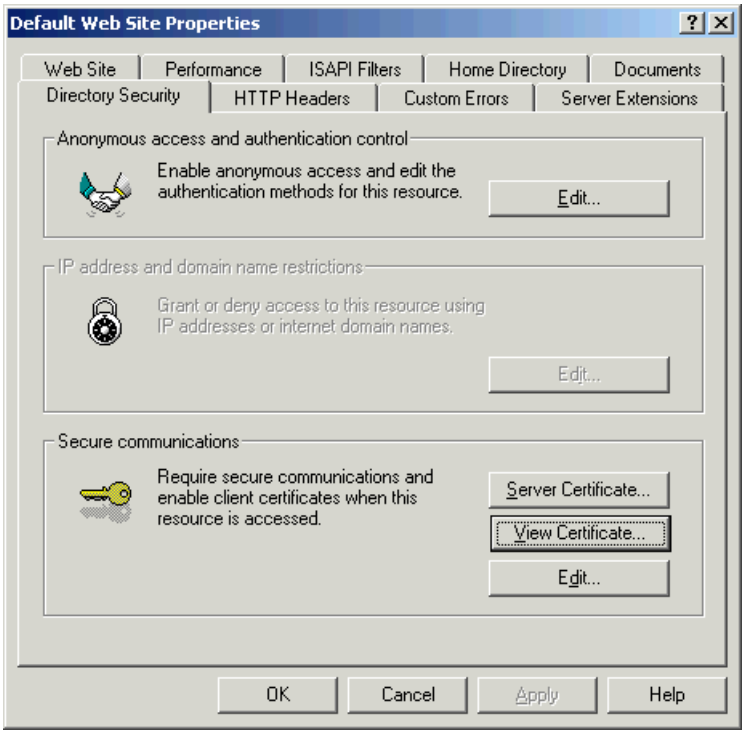
Vemos que los datos son correctos



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 ..

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	
	Enviar

Otros Tutoriales Recomendados (También ver todos)

Nombre Corto	Descripción
Activación de la seguridad en Apache	Alejandro Pérez nos enseña como securizar Apache a través de autentificación básica y certificados de seguridad SSL.
Activar soporte SSL en Tomcat	Os mostramos como activar el acceso SSL en Tomcat, utilizando certificados generados por Keygen (java)