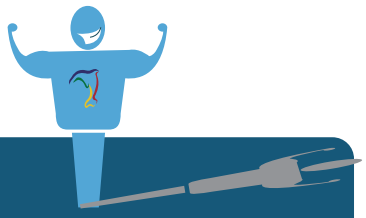
autentia

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...

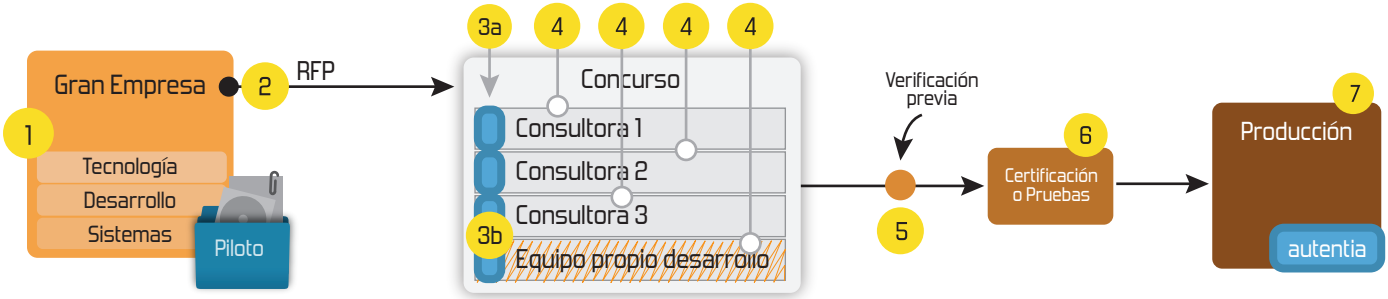
1. Desarrollo de componentes y proyectos a medida



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: Alejandro Perez García 2003-2005, nuestro experto en J2EE, Linux y optimización de aplicaciones empresariales.

Si te gusta lo que ves, **puedes contratarme** para impartir **cursos presenciales** en tu empresa o para ayudarte en proyectos (Madrid).

Contacta: alejandropg@autentia.com.

autentia real business solutions

Manejo de certificados con IIS para la activación de SSL

Creación: 10-08-2005

Índice de contenidos

1. Introducción

La seguridad es un aspecto del desarrollo de aplicaciones que, a menudo, se deja de lado; cuando debería ser todo lo contrario. Si en nuestra aplicación web estamos trabajando con datos sensibles (número de cuentas, informes médicos, datos de nuestros clientes, ...) es fundamental que esta información este protegida para que terceros malintencionados no puedan hacer un mal uso de ella.

Desde Autentia (http://www.autentia.com) os recomendamos que tengáis esto siempre muy presente en vuestros desarrollos. De hecho, la seguridad, debería ser algo ha identificar durante la fase de toma de requisitos. De lo contrario puede que nuestra aplicación no cumpla con las expectativas del cliente, e incluso podría no cumplir la ley.

Si dejamos la seguridad para el final puede ser demasiado tarde. Si no la hemos tenido en cuenta desde el principio puede que el impacto sobre la aplicación sea tan grande, que sea necesario rehacer gran parte del trabajo.

En este tutorial vamos a ver algo sencillito. Veremos como habilitar el SSL (Secure Socket Layer, comunicación segura por https) en un servidor IIS (Internet Information Server de Microsoft).

Con SSL o Secure Socket Layer conseguimos que, una vez esté habilitado, todas las comunicaciones entre el servidor y el cliente estén cifradas, de forma que terceros no puedan entender los datos que viajan del cliente al servidor y viceversa.

2. Entorno

El tutorial está escrito usando el siguiente entorno:

- Hardware: Portátil Ahtex Signal X-9500M (Centrino 1.6 GHz, 1024 MB RAM, 60 GB HD).
- Sistema Operativo: GNU / Linux, Debian Sid (unstable), Kernel 2.6.11, KDE 3.4
- Máquina Virtual Java: JDK 1.5.0_03 de Sun Microsystems

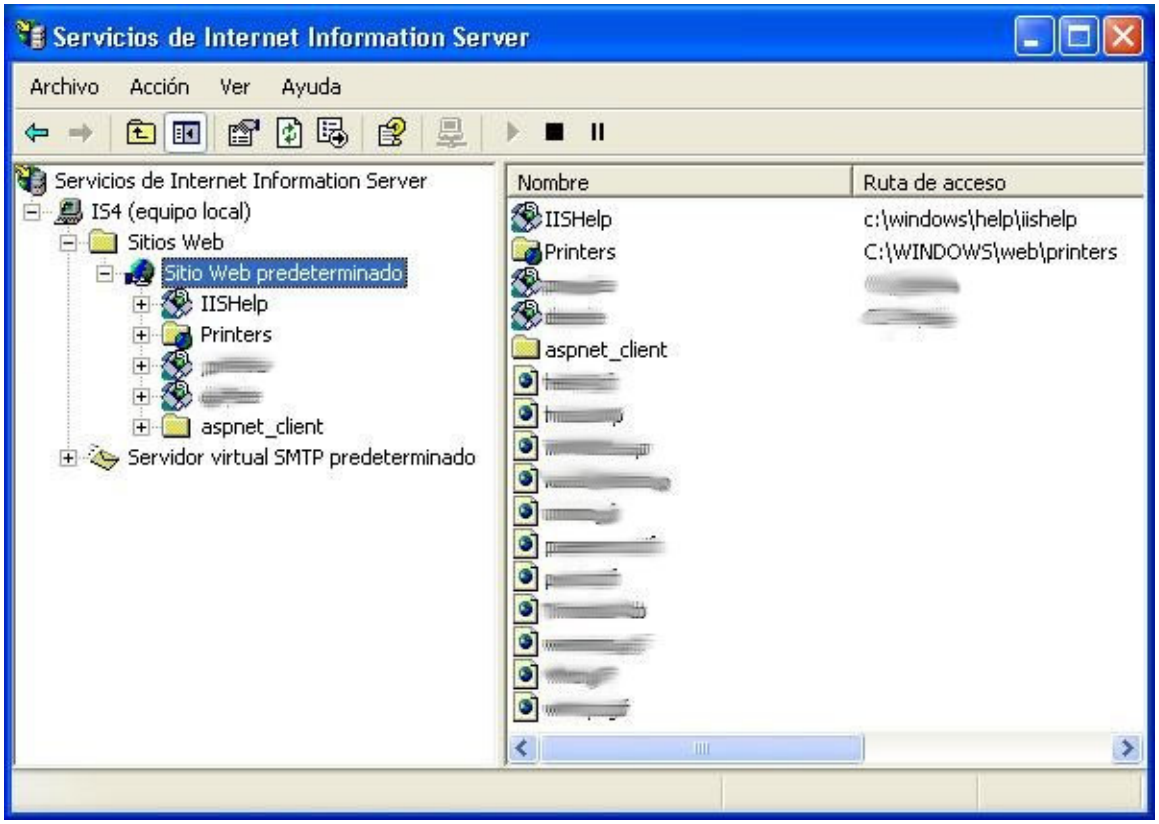
3. Proceso para habilitar SSL en un servidor

Independientemente del servidor en el que queramos activar el SSL (comunicación segura por https), el proceso siempre es similar:

1. Nosotros, como dueños del servidor donde queremos activar el SSL, tendremos que generar una petición de certificado.
2. Esta petición se la mandaremos a una entidad certificadora (CA). Estas entidades están reconocidas a nivel mundial, y su papel es como el de un notario. Es decir, la labor de estas entidades será echar una firmita sobre nuestra petición, asegurando ante cualquiera de nuestros clientes que nosotros somos realmente quienes decimos ser (no suplantación). Ejemplos de estas CAs son VeriSign o VISA, aunque hay muchas más (las podéis encontrar en la configuración de vuestro navegador).
3. Una vez tengamos la respuesta de la CA, la pondremos en el lugar correspondiente en nuestro servidor. Con esto estamos capacitando al servidor para establecer comunicaciones usando SSL.
4. Por último sólo nos queda configurar nuestra aplicación Web para que la comunicación con ella sea obligatoriamente usando SSL.

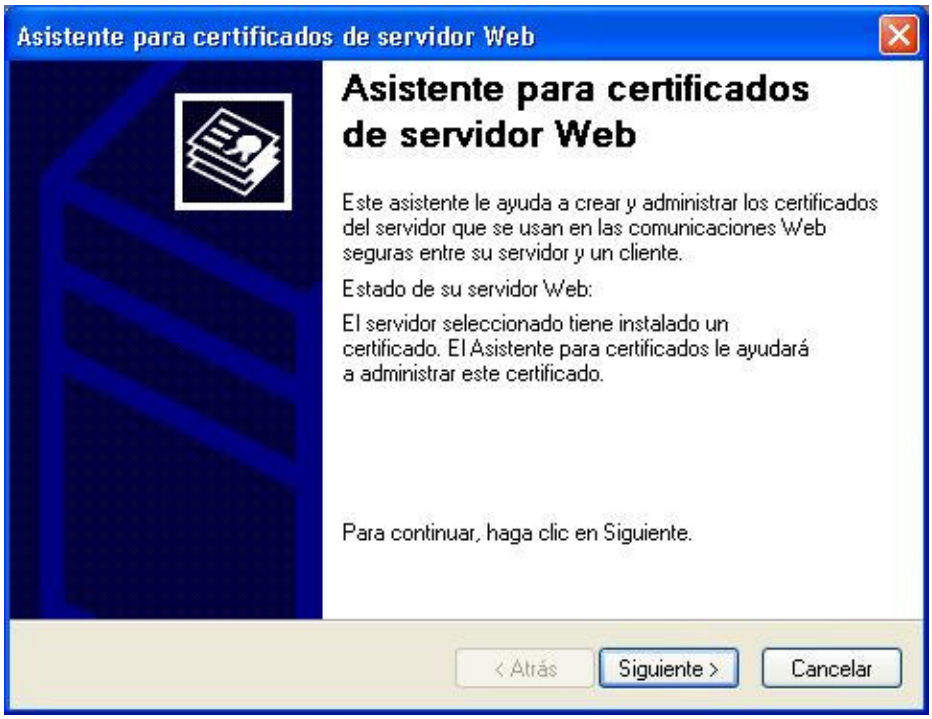
4. Generar la petición de certificado

En primer lugar abrimos la consola de administración de IIS, y con el botón derecho sacamos las propiedades del sitio web que nos interesa (en el ejemplo "Sitio Web predeterminado").



Una vez tenemos las ventana de propiedades, pinchamos sobre la pestaña de "Seguridad de directorios". Y dentro de esa pestaña pulsamos el botón "Certificado de servidor..."

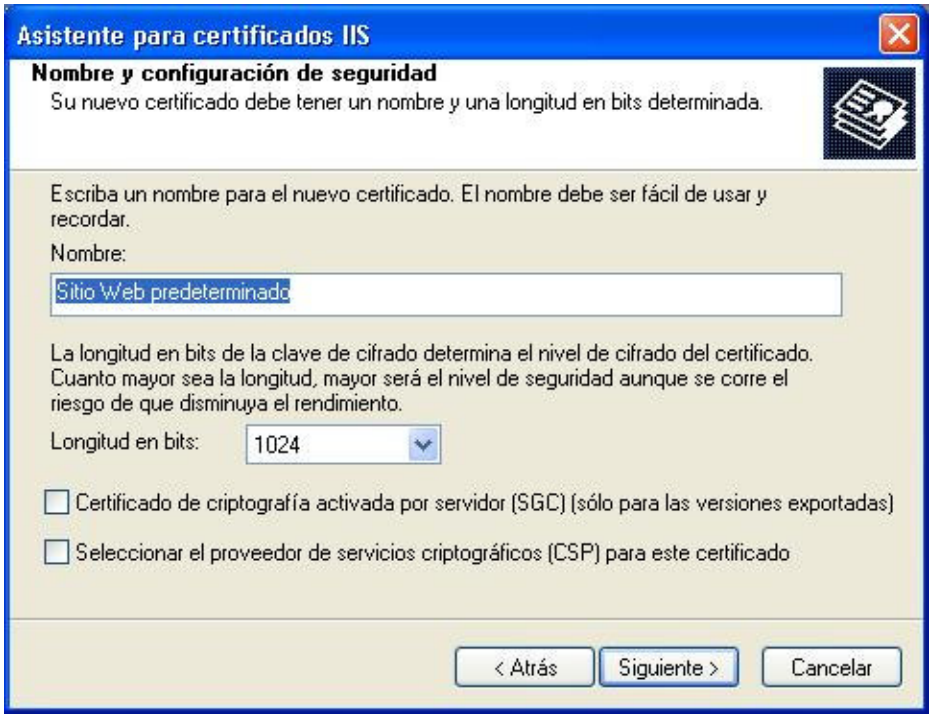
Se abre el asistente para certificados. Pulsamos sobre "0 >"



Elegimos la opción "Crear un certificado nuevo.", y pulsamos sobre el botón "Siguiente >".

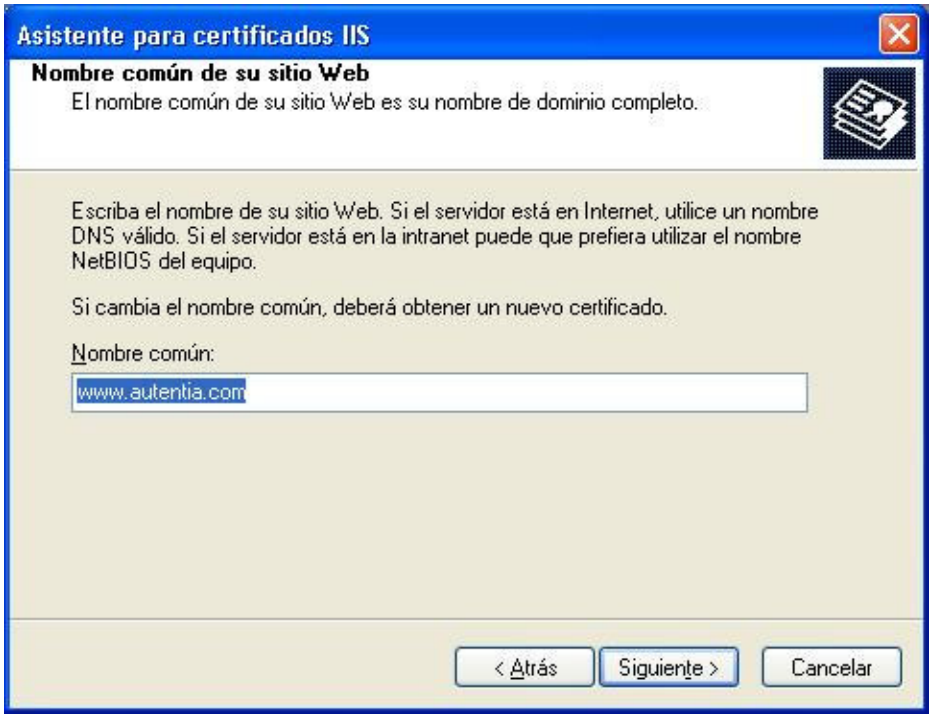
Seleccionamos la opción "Preparar la petición ahora pero enviarla más tarde", y pulsamos sobre el botón "Siguiente >".

En las siguientes pantallas el asistente nos pide cierta información (la misma que el tutorial de keytool al crear el certificado). En primer lugar el nombre del certificado. Este nombre será como haremos referencia al certificado (si veis el tutorial sobre keytool es el equivalente del alias).



A continuación nos pide el nombre de la organización y el nombre de la unidad organizativa.

Luego nos solicita el "nombre común". En caso de que el servidor esté en Internet, este nombre debe coincidir con el nombre DNS. Si el servidor está en intranet basta con el nombre de la máquina. Este apartado es importante, ya que si cambiamos el nombre del DNS habrá que pedir un nuevo certificado.

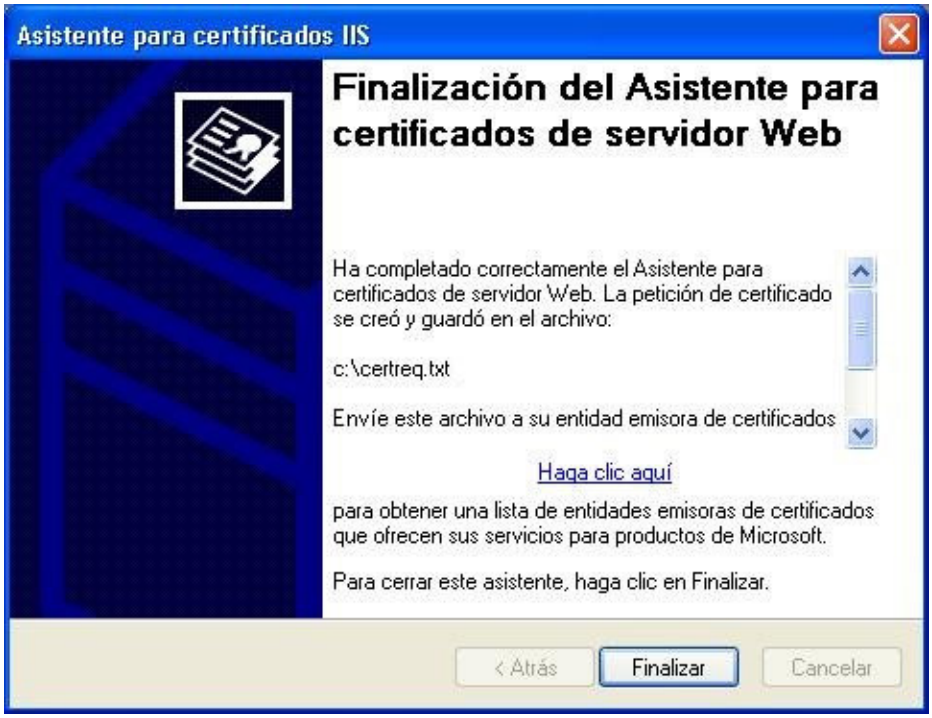


Por último nos pregunta el país, la provincia y la ciudad

Ya queda poco. Ahora tenemos que indicar el fichero donde se guardará la petición de firmado de certificado (CSR).

Antes de terminar se nos muestra el detalle de la petición.

Ya hemos llegado a la última pantalla del asistente. Sólo nos queda pulsar el botón "Finalizar" y obtendremos nuestra petición de firma de certificado (CSR).



5. Mandar la petición a la CA

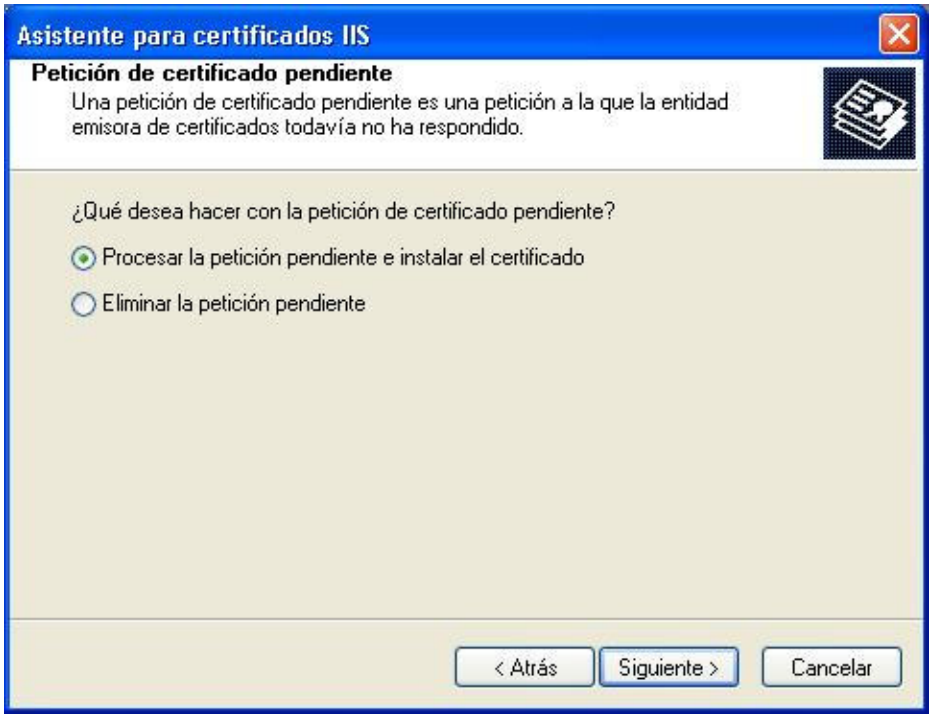
El fichero que hemos obtenido después de realizar los pasos descritos en el punto anterior se lo mandaríamos a una CA (Entidad Certificadora).

En el tutorial de keytool podemos ver como nos cremos nuestra propia CA (Entidad Certificadora), y nos firmamos la petición a nosotros mismos. Esto puede ser muy conveniente para intranets, donde tenemos cierto control sobre los clientes que accederán al servidor.

La CA nos devolverá nuestro certificado firmado por ellos.

6. Instalar la respuesta de la CA

Una vez tengamos la respuesta de la CA, nos volvemos a meter en el consola de administración del IIS. Volvemos a sacar las propiedades del sitio web, volvemos a situarnos sobre la pestaña de "Seguridad de directorios" y pulsamos el botón de "Certificado de servidor..." (pasamos por las tres primeras pantallas del punto anterior). Esta vez nos aparece una pantalla donde seleccionaremos "Procesar la petición pendiente e instalar el certificado", y pincharemos sobre el botón "Siguiente >".



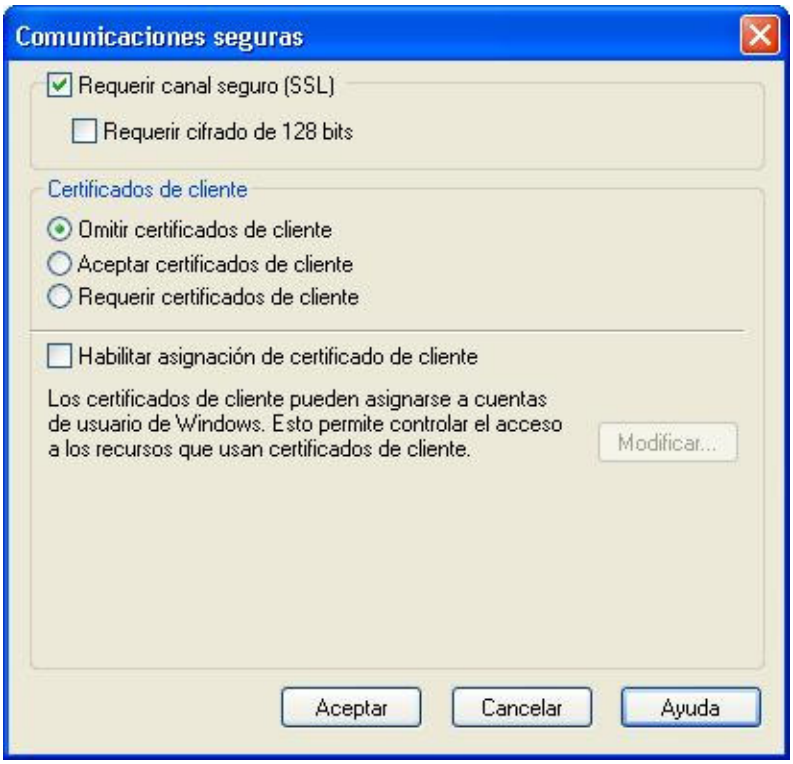
Seleccionamos el fichero que nos ha devuelto la CA.

Nos aparece el detalle del certificado que vamos a instalar.

7. Activar SSL en algún módulo web

Dentro de nuestro sitio web (en el ejemplo "Sitio Web predeterminado") seleccionamos algunos de los módulos (en nuestro ejemplo seleccionamos el módulo "deyde") y pulsando botón derecho sobre él, sacamos sus propiedades. En la ventana de propiedades pinchamos sobre la pestaña de "Seguridad de directorios", y en esta pestaña pulsamos sobre el botón "Modificar..." de la sección "Comunicaciones seguras".

Nos aparece una pantalla en la que si seleccionamos "Requerir canal seguro (SSL)" estaremos forzando a que todos los accesos a nuestro módulo web sean a 11 de https. Con esto conseguimos que toda la comunicación entre el cliente y el servidor sea obligatoriamente por SSL, y por lo tanto segura desde el punto de vista que la información va cifrada, por lo que un tercero no podrá entender la conversación entre el cliente y el servidor. También conseguimos evitar la suplantación, es decir, todo cliente que se conecte contra nuestro servidor tendrá la seguridad que somos nosotros, y no un tercero haciéndose pasar por nosotros.



8. Conclusiones

En este tutorial simplemente hemos visto como conseguir que la comunicación entre el cliente y un servidor IIS sea segura. Otro tema sería el método de autenticación de los clientes, o las políticas de acceso de los clientes (una vez se han autenticado, determinar a que partes de la aplicación pueden acceder).

9. Sobre el autor

Alejandro Pérez García, Ingeniero en Informática (especialidad de Ingeniería del Software)

Dir. Implantación y Rendimiento

Formador en tecnologías J2EE, ADOO, UML

mailto:alejandropg@autentia.com

Autentia Real Business Solutions S.L.

http://www.autentia.com

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
Gestión de errores con IIS	Ismael caballero nos enseña como evitar que aparezan pantallas genericas de error cuando trabajamos con IIS
Uso de Tiles en Struts	Os mostramos como utilizar el sistema de plantillas proporcionado por Struts (tiles)
Aplicación básica con RMI	Gracias a este tutorial, podreis aprender paso a paso como crear una aplicación cliente-servidor con RMI
Endogamia y estrategia tecnológica	Este es otro atípico tutorial donde, a través de un cuento, os invitamos a realizar una reflexión sobre las decisiones estratégicas que muchas veces criticamos.
Generación automática de código JDBC	En este tutorial os enseñamos como, sin conocimiento de JDBC, crear vuestro programas en Java, gracias a JDBCTest.
Activar SSL en IIS	Os mostramos comos activar el soporte de https en IIS, creando vuestros propios certificados autofirmados, usando OpenSSL
Planificación de proyectos XP	En este tutorial veremos Xplanner, una herramienta de planificación y seguimiento de proyectos especialmente indicada para la metodología XP (eXtreme Programming).
Cliente y Servidor DCOM con MS Visual C++	Os mostramos como construir un servidor y cliente de Automatización OLE con las facilidades que proporciona el entorno de desarrollo Microsoft Visual C++
Plantear una aplicación Web y Struts	Os mostramos un posible modo de plantear una aplicación Web (análisis) y darla forma. El FrameWork utilizado es struts y tratamos de identificar qué depende de este FrameWork y qué no.
Aplicaciones con el framework de Microsft .NET	Ejemplo de desarrollo de una aplicación con el framework de Microsft .NET (creación de un servicio deEncuestas Web)