Certificados SGC SuperCerts

El SGC SuperCert es el certificado ***Thawte*** con mayor capacidad de codificación. Incrementa de forma automática la protección hasta una codificación mínima de 128 bits, incluso para usuarios que utilicen navegadores antiguos (IE 4.X o Netscape 4.06 y posteriores) con capacidad de codificación limitada a 40 o 56 bits. Es posible conseguir una codificación de 256 bits si tanto la capacidad del navegador de su cliente como el sistema de codificación instalado en su servidor son compatibles con el mismo.

El certificado SGC SuperCert de ***Thawte*** proporciona la mayor seguridad tanto para la entidad como para el usuario.

Características y ventajas del certificado:

Codificación:	256 bits, con un nivel mínimo de protección de 128 para el 99.9% de los usuarios de navegadores antiguos.
Compatibilidad con navegadores:	La más alta de la industria.
Detalles del certificado:	Autenticación y verificación de dominio e identidad.
Sello del Sitio Web de confianza ***Thawte***:	Sí
Re-emisiones gratuitas:	Sí - ilimitadas durante el periodo de validez del certificado
Soporte técnico:	Si
Protección de nombres de dominio internacionalizados:	Sí - ***Thawte*** es la primera Autoridad de Certificación en lograr que todos sus certificados SSL sean compatibles con caracteres de nombres de dominio internacionalizados.
Tecnología SGC:	Sí
Protocolo de estado de certificado virtual:	Sí
Lista de revocación de certificados (CRL):	Sí - Completamente compatible con la Lista de revocación de certificados

ACTIVE WEB

¿Cuál es la función del certificado?

Los certificados SGC SuperCert de ***Thawte*** permiten a un mayor número de usuarios de Windows 2000 (sin instalar el Service Pack 4 o el Paquete de codificación de alto nivel) y a otros conectarse con una codificación de 128 bits. La diferencia supone que decenas de millones de usuarios más en todo el mundo podrían acceder a la codificación de 128 bits o superior si las entidades utilizasen SGC.

Esto fue rotundamente confirmado por un estudio independiente realizado por el **Yankee Group** en septiembre de 2005. Durante el estudio, los consultores de seguridad examinaron 23 combinaciones de configuraciones de clientes y cuatro servidores Web habituales, realizando no menos de 368 pruebas y documentando los resultados en vídeo.

En los años 1990, el gobierno de los Estados Unidos impuso restricciones a la exportación de codificación potentes a otros países. Esta restricción hizo que el software que implementase SSL, tal como navegadores, sistemas operativos y servidores, tuviese que limitar la codificación a algoritmos débiles e inferiores longitudes de claves si se comercializaba para su uso fuera de los Estados Unidos. Los legisladores incluyeron una excepción para las transacciones financieras, para asegurar que los usuarios de todo el mundo pudiesen efectuarlas sin riesgo utilizando codificaciones potentes.

SGC se creó como una extensión de SSL para que los usuarios con navegadores antiguos pudiesen acceder a una codificación superior en sus transacciones. Las leyes de los Estados Unidos se respetaron mediante la restricción de la emisión de certificados SGC a instituciones financieras que reuniesen los requisitos necesarios, creando un punto de refuerzo en el servidor sin ninguna repercusión en el cliente. Las restricciones sobre codificaciones potentes se han levantado desde entonces, y los certificados SGC pueden emitirse para cualquier institución.

Las antiguas restricciones resultan evidentes en anteriores versiones de Windows 2000 con Internet Explorer que continúan en uso. Los consumidores y los vendedores de comercio electrónico, en especial fuera de los Estados Unidos, siguen utilizando codificaciones débiles, a pesar de existir alternativas más potentes y seguras.

Pese a que las nuevas versiones de Windows proporcionan estas características, millones de personas siguen utilizando las anteriores. Los usuarios que continúan utilizando navegadores antiguos que sólo ofrecen una débil codificación de 40 o 56 bits pueden lograr la codificación de 128 bits completa al realizar transacciones con páginas que dispongan de la tecnología SGC.

Con SGC, se permite a los navegadores y sistemas operativos, que de otra forma se conectarían con una codificación débil, alcanzar una seguridad mucho mayor. Hasta que las versiones antiguas de los navegadores y sistemas operativos desaparezcan por completo, los certificados SGC permiten proteger a este sector de los usuarios.

El SGC SuperCert en acción

El certificado SGC SuperCert permite sesiones SSL de 128 bits en navegadores antiguos que normalmente estarían limitados a una codificación de 40 o 56 bits. La diferencia entre los SGC SuperCerts y los Certificados SSL de servidor Web comunes es que siempre que uno de estos navegadores antiguos se conecte a una página con un SGC SuperCert instalado, la sesión de SSL se incrementará automáticamente a 128 bits, en lugar de utilizar el nivel de codificación limitado por defecto para el navegador (40/56 bits). (IE 4.X o Netscape 4.06 y posteriores)

Archivo de Solicitud de Firma de Certificado (CSR, por sus siglas en inglés)

El proceso de solicitud de un SGC SuperCert comienza con la generación y envío de un archivo de Solicitud de Firma de Certificado (CSR). A partir de ahí ***Thawte*** verifica su identidad y, una vez satisfechos los requisitos, firma el archivo solicitado, utilizando su clave raíz de Autoridad de Certificación de confianza ***Thawte***, y se lo envía como su certificado.

Formatos válidos de solicitud de certificado

Cuando emitamos su certificado contendrá dos piezas fundamentales de información. La primera será el "Nombre distintivo", un conjunto de valores que describan su país, provincia, ciudad, organización, departamento y el nombre de dominio de su servidor Web. La segunda será su clave pública.

Claves

Las claves de sesión se componen de una clave pública (emitida junto con su SGC SuperCert) y claves privadas seleccionadas al azar, creadas por cada navegador cuando se conecta a su servidor. Las claves de sesión se utilizan para encriptar y desencriptar datos (transmitidos desde y hacia el servidor) tras el "saludo" inicial entre el navegador y el servidor. (Una clave de sesión no es su clave del Certificado del servidor, que tiene 1024 o bien 512 bits).

Servidores compatibles

Todos los servidores deberían funcionar con el SGC SuperCert. Tenga en cuenta que el SGC SuperCert es encadenado, por lo que deberá comprobar que su servidor es compatible con el encadenamiento de certificados. Los Servidores compatibles son adjuntados en un nuevo documento llamado “compatible_webservers.pdf”.

Renovación de la versión de los navegadores

Los usuarios de navegadores de generación 3.x pueden elevar su seguridad al mismo nivel que la de los de generación 4.0. El proceso lleva unos dos minutos y garantiza que su navegador funcione con las decenas de miles de servidores seguros con certificación ***Thawte*** que existen. Sólo necesitará hacer esto una vez y su navegador quedará permanentemente renovado.