Transferencia segura de Datos en Línea con SSL

Guía para comprender los certificados SSL,
cómo funcionan y su aplicación…

thawte
it's a trust thing

1. Aspectos generales

thawte es uno de los principales proveedores de certificados SSL del mundo. Al usar un certificado SSL de *thawte* en el/los servidor(es) web de su empresa, puede reunir información sensible en línea de modo seguro y aumentar su volumen comercial al brindar a sus clientes la fiabilidad de que sus transacciones son seguras.

Esta guía tiene el propósito de ofrecerle una presentación de la seguridad de los certificados SSL cubriendo los puntos básicos de su funcionamiento. También se incluye una descripción de las varias aplicaciones de los certificados SSL y su uso correcto, junto con los detalles de cómo puede probar los certificados SSL en su servidor de la Web.

2. ¿Qué es SSL?

Secure Socket Layer (SSL) es un protocolo desarrollado por Netscape en 1996 que pronto se convirtió en el método elegido para asegurar las transmisiones de datos por Internet. SSL es una parte integral de la mayoría de los exploradores y servidores web y hace uso del sistema de codificación con dos claves: una pública y una privada, desarrollado por RSA.

Para establecer una conexión SSL, el protocolo SSL requiere que el servidor tenga instalado un certificado digital. Un certificado digital es un archivo electrónico que identifica de modo único a individuos y servidores. Los certificados digitales funcionan como una especie de pasaporte o credencial digital que autentica al servidor antes de establecer la sesión SSL. Por lo general, los certificados digitales están firmados por un tercero independiente y fiable para garantizar su validez. El “firmante” de un certificado se denomina autoridad de certificación (CA), como *thawte*.

SSL proporciona comunicaciones seguras mediante la combinación de los siguientes dos elementos:

1] Autenticación –
el certificado digital va unido a un dominio específico y una CA realiza una cantidad de verificaciones para confirmar la identidad de la organización que solicita el certificado antes de emitirlo. De este modo, el certificado sólo puede instalarse en el dominio contra el cual ha sido autenticado, ofreciendo a los usuarios la seguridad que necesitan.

2] Codificación –
la codificación es el proceso de transformar la información para hacerla incomprensible para todos salvo el receptor al que va dirigida. Esto constituye la base de la integridad y privacidad de los datos, necesarias para el comercio electrónico.

Nota

La aplicación más corriente de los certificados SSL es la de asegurar la transferencia de datos entre exploradores y servidores web. Si bien SSL puede usarse para asegurar comunicaciones entre servidores, esta guía ilustrará el funcionamiento de SSL con ejemplos de explorador-servidor.

Para obtener información adicional sobre cómo asegurar comunicaciones entre servidores con SSL, comuníquese con un representante de ventas de *thawte*.

3. Cómo saber si un sitio Web es seguro

La primera clave para establecer si un sitio web está asegurado con un certificado SSL se encuentra en la barra de estado del explorador: busque si tiene un icono con un candado. En los exploradores de Internet, cuando las páginas no están aseguradas, el icono del candado no estará visible. Sin embargo, cuando se establece una sesión SSL, aparecerá el icono del candado. En Netscape, hay iconos con candados “cerrados” y “abiertos”, que indican sitios web seguros e inseguros, respectivamente.

Microsoft IE
Seguro: 
NetScape Navigator
Seguro: 
Inseguro: 

La otra clave que debe buscar está en la barra de dirección. Si se establece una sesión segura entre el explorador y el servidor de la Web, la porción “http:” de la dirección de la Web cambiará a “https”. Por ejemplo: “http://www.thawte.com” se convierte en “https://www.thawte.com”.

También es posible conocer la fortaleza de la codificación de una sesión SSL particular. En Internet Explorer, simplemente desplace el ratón sobre el candado para ver la fortaleza de la codificación.

En Netscape, haga doble clic sobre el candado para ver el certificado. La fortaleza de la codificación se detalla en la primera ficha del certificado.

4. ¿Cómo se ve un certificado SSL?

Para ver el certificado de un sitio web, haga doble clic sobre el icono del candado cerrado que aparece en la barra de estado inferior.

Certificado digital visto con un explorador Netscape 7.0:

Certificado digital usado con un explorador IE 6.0:

Un certificado de servidor web SSL o un SuperCert SGC de *thawte* permite que sus clientes vean la siguiente información:

- El dominio para el cual se emitió el certificado. Esto les permite verificar que el certificado de servidor web SSL fue emitido para su host y dominio exacto (www.midominio.com).
- El propietario del certificado. Esto funciona como garantía adicional, ya que los clientes pueden ver con quién están haciendo negocio.
- La ubicación física del propietario. Una vez más, esto garantiza a los clientes que están tratando con una entidad de existencia real.
- Las fechas de validez del certificado. Esto es de suma importancia, ya que muestra a los usuarios que su certificado digital está vigente

5. Alertas de seguridad del explorador

Su explorador cuenta con una función de seguridad incorporada que muestra un mensaje de advertencia cuando usted intenta enviar un mensaje a un sitio Web que tiene algún problema con el certificado.
El siguiente es un ejemplo de mensaje de advertencia que se muestra en Microsoft Internet Explorer:

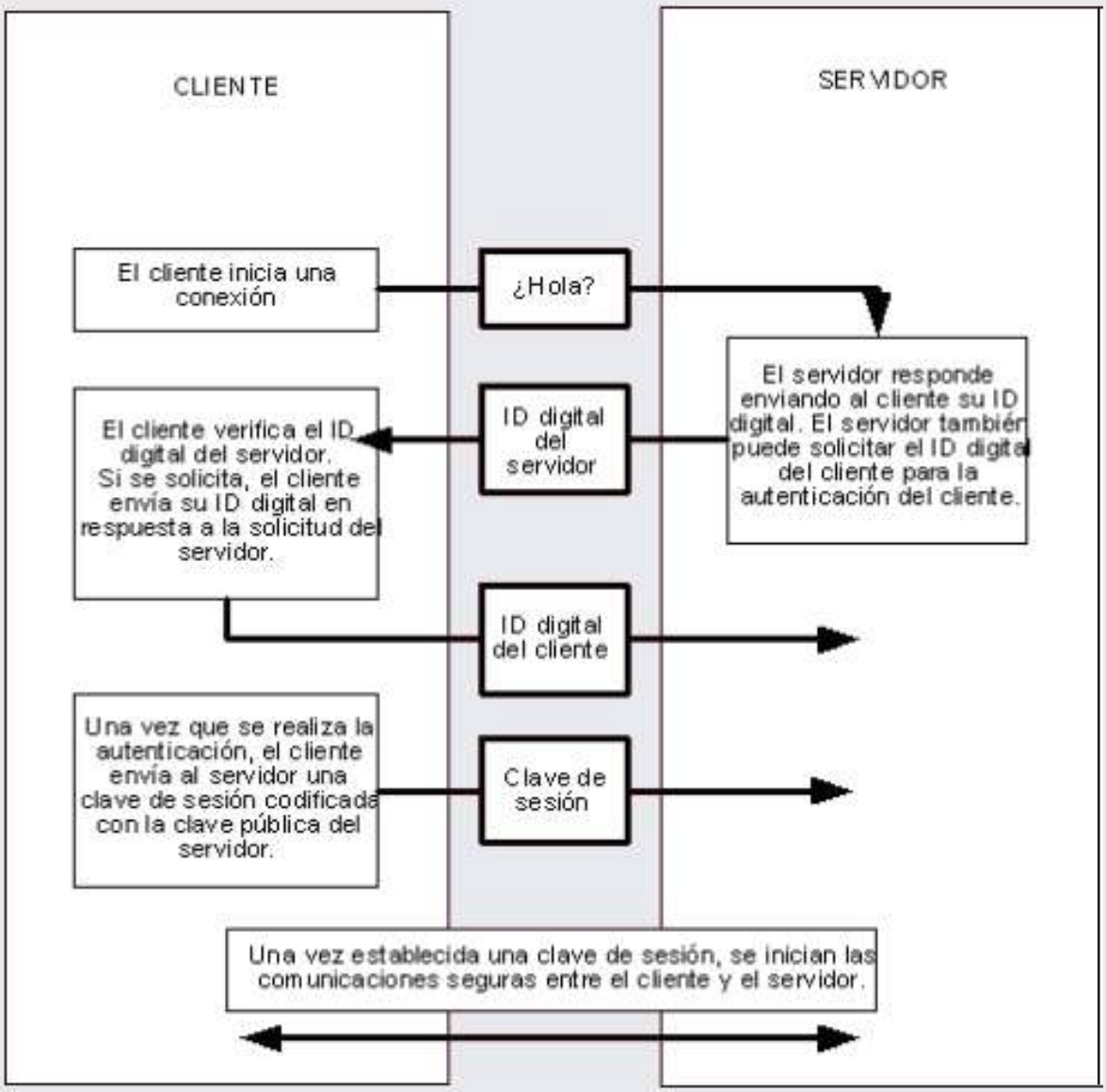
En el ejemplo anterior, se activa la alerta de seguridad porque el nombre del dominio no coincide con el del sitio web al que desea acceder, lo que indica que el sitio en el cual está instalado el certificado no tiene derecho a usar dicho certificado. Otras alertas de seguridad se activan si ha vencido el período de validez de un certificado. De igual modo, la advertencia se mostrará si el certificado está firmado con una raíz no reconocida (una raíz que no está instalada de modo predeterminado en el explorador).

Por otra parte, se informará al usuario que accede a un sitio web con certificado válido que el sitio Web que está visitando cuenta con certificado digital emitido por una autoridad de certificación (CA) reconocida, como *thawte*, y que todos los datos que envíe serán codificados. Al controlar el certificado, el cliente puede verificar que el sitio web es propiedad de una empresa real, dueña del nombre del dominio al que está accediendo.

6. ¿Cómo se establece una sesión SSL?

Al conectarse a un servidor web seguro, como https://www.thawte.com, ese servidor debe autenticarse a sí mismo ante el explorador web mediante un certificado digital antes de establecer una conexión segura.

El siguiente diagrama ilustra los pasos que tienen lugar cuando se establece una sesión SSL:



Durante este proceso, el explorador web verifica que:

- el nombre del dominio del certificado coincida con el dominio desde el que se lo envió
- el certificado no esté vencido
- el explorador de la Web considera que la CA que firmó el certificado es fiable

El proceso es perfecto, de modo que el usuario no ve cuando estos pasos tienen lugar. El certificado prueba que un tercero independiente y fiable, como *thawte*, ha verificado que el dominio pertenece a una empresa real y, por lo tanto, es fiable. Un certificado válido brinda a los clientes la confianza de que están enviando información personal de modo seguro a una empresa autenticada

7. Clave pública y privada

Al solicitar un certificado, usted genera un par de claves en su servidor: una pública y una privada. Cuando se genera un par de claves para su negocio, su clave privada se instala en su servidor y es de crucial importancia que nadie más tenga acceso a la misma.

Su clave privada crea firmas digitales que, de hecho, funcionan como el sello de su empresa en línea. Es esencial mantener esta clave lo más segura posible. Si usted pierde su clave privada, ya no podrá seguir usando su certificado. Por esta razón, es esencial que guarde una copia de seguridad de toda la clave privada como una buena práctica de la gestión continuada de las claves.

La clave pública concordante se instala en el servidor de la Web como parte del certificado digital. Ambas claves, pública y privada, se relacionan matemáticamente, pero no son idénticas. Los clientes que deseen comunicarse con usted en privado (mediante SSL) usan la clave pública de su certificado para codificar la información antes de enviársela. Este proceso es instantáneo y perfecto para el usuario. Sólo la clave privada del servidor web puede decodificar esta información. Los clientes sentirán la seguridad de que nada de lo que envíen podrá ser visto por un tercero.

8. Aplicaciones de SSL

Existen dos áreas amplias de aplicación para los certificados SSL:

1] Asegurar la comunicación entre el explorador y el servidor web -
Asegurar la comunicación entre el explorador y el servidor web es actualmente la principal aplicación y se aplica con mayor frecuencia a los sitios web de comercio electrónico para garantizar la transferencia de información sobre pagos. El tipo de datos considerados sensibles se está ampliando actualmente desde los datos financieros para incluir toda la información personal identificable, incluidos los números de identidad y seguridad social, y, cada vez más, las direcciones de correo electrónico.

2] Asegurar la comunicación entre servidores -
Cada vez recurren más empresas a certificados SSL para asegurar las comunicaciones entre servidores. Esta es un área de aplicación que ofrece a las empresas varias opciones para mejorar la seguridad de los datos y la privacidad de la red. Actualmente, asegurar la comunicación entre servidores de correo electrónico es la aplicación más usual, si bien también es posible asegurar sitios ftp, bases de datos y servidores de aplicaciones, entre otros.

9. ¿Cuándo es apropiada la utilización de certificados SSL?

La decisión de utilizar certificados SSL gira en torno a la importancia asociada con la seguridad de la transferencia de datos en línea. Por ejemplo, si está gestionando transacciones financieras en su sitio web, no hay duda de que necesita certificados SSL. Si está gestionando datos sensibles de los clientes, como números de seguridad social o números de identidad, merece la pena considerar seriamente la utilización de certificados SSL, en especial si la seguridad de sus clientes/miembros ocupa un lugar destacado en su lista de prioridades.

Desde el punto de vista comercial, la utilización de certificados SSL provee a los clientes/usuarios la garantía de que no quedarán expuestos a ningún riesgo asociado con la transmisión de datos por una red abierta. Esto en sí mismo presenta muchos beneficios para su negocio, la mayoría de los cuales fluyen a partir de una mayor fiabilidad al tratar con su organización en línea. Por tanto, si su negocio se basa en el establecimiento de relaciones comerciales fiables con sus clientes para facilitar

10. Soluciones de certificados SSL de *thawte*

Certificados SSL123

SSL123 es un certificado seguro validado a un dominio capaz de encripcion de 128-bit depende del nivel del cifrado apoyado por el explorador del cliente. Este producto se puede emitir dentro de unos minutos y es ideal para un negocio que desea instalar seguridad básica entre su sitio Web y sus usuarios en línea así como usos generales tales como asegurar intranets. Lea más...

Certificados de servidor web SSL

El certificado SSL Web Server Certificate de *thawte* es capaz del encripcion de 128-bit dependiendo del nivel del cifrado apoyado por el explorador del cliente. Estos certificados son un producto ideal para las organizaciones que son serias sobre hacer negocio en línea y reconocen el valor y las ventajas de tener sus detalles de la organización verificada y incluida en el certificado. Para obtener más información. Lea más…

SuperCerts SGC

Un SGC SuperCert de *thawte* permitirá que usted amplíe la encripcion de 128-bit a sus clientes, incluso si utilizan uno de los siguientes más viejos exploradores: IE 5.01 y Netscape 4.7x o versiones posteriores, que están limitados a capacidades de codificación de 40 ó 56 bits. Estos son los certificados de elección si usted está asegurando información altamente sensible y prefiere la codificación de 128 bits. Para obtener más información, lea más...

Programa Starter PKI (SPKI)

El programa SPKI de *thawte* es ideal para cualquier empresa u organización que requiera tres o más certificados digitales por año para su propio uso y de modo continuo. Nuestro programa SPKI le permite controlar completamente sus necesidades de certificados, cosechando al mismo tiempo los beneficios de un ahorro significativo. Para mayor información, lea más.....

11. Prueba de los certificados SSL en su servidor de la Web

Para brindarle una comprensión práctica de los certificados SSL, quizás desee descargar un certificado SSL de prueba a fin de evaluarlo. Estos certificados son válidos durante 21 días y le permitirán familiarizarse con el proceso de instalación además de asegurarse de la compatibilidad con la configuración de su servidor web. Puede descargar el certificado de prueba gratuito desde: http://www.thawte.com/gothawte/cgi/a=w46840165367049000

También puede que desee descargar una de las guías especiales paso a paso de thawte, donde encontrará información sobre la solicitud, configuración e instalación de certificados SSL para las dos plataformas de servidores web más populares:

- Guía de Apache [vínculo]
- Guía de Microsoft IIS [vínculo]

Las pautas de instalación para otras plataformas de servidores web están disponibles en nuestro sitio de asistencia técnica. Haga clic aquí...

12. El sello de sitio de *thawte*

Todos los clientes de certificados de servidor de la Web SSL o SuperCert SGC pueden mostrar el sello de sitio de *thawte* en sus sitios web. El sello de sitio es una imagen de seguridad que ofrece una prueba visible de su fiabilidad, de que usted está completamente autenticado y de que los usuarios pueden realizar transacciones seguras con usted.

El sello de sitio está disponible en varios idiomas y tamaños, lo que permite una fácil integración con el diseño de su sitio Web. Encontrará más información en:
http://www.thawte.com/siteseal/index.html

13. Direcciones URL útiles

Para obtener información más detallada sobre los certificados de servidor de la Web SSL de *thawte*, visite:

http://www.thawte.com/ssl/index.html

Los problemas más comunes que se presentan con los certificados de servidor de la Web SSL se explican en la base de conocimiento de thawte:

http://search.thawte.com

También puede encontrar información útil en nuestra sección de preguntas frecuentes:

http://www.thawte.com/support/ssl/index.html

Adquiera los certificados de servidor web SSL:

http://www.thawte.com/buy

14. ¿Qué papel juega *thawte*?

thawte Technologies es una autoridad de certificación (CA) que emite certificados de servidores Web SSL y SuperCerts de 128 bits a organizaciones e individuos en todo el mundo. *thawte* verifica que la organización que solicita el certificado es una organización registrada y que la persona de la organización que solicitó el certificado está autorizada para hacerlo.

thawte también controla que la organización en cuestión sea propietaria del dominio relevante. Los certificados digitales de thawte interoperan perfectamente con la versión más reciente de software de Microsoft y Netscape, para que esté tranquilo de que la adquisición de un Certificado de servidor Web de*thawte* hará que sus clientes confíen en la integridad del sistema: se sentirán seguros de efectuar transacciones en línea.

.

15. El valor de la autenticación

La información es un valor clave para su negocio. Para asegurar la integridad y la seguridad de la información, es importante identificar con quién está tratando y si los datos que recibe son fiables. La autenticación puede contribuir al desarrollo de confianza entre las partes involucradas en todos los tipos de transacciones tras abordar sólo un conjunto de medidas de seguridad que incluye:

Simulación de falsificación de datos: El bajo costo del diseño de sitios Web y la facilidad con la que se pueden copiar páginas existentes facilita en su conjunto la creación ilegítima de sitios Web que aparecen como si hubieran sido publicados por organizaciones establecidas. De hecho, timadores profesionales han obtenido ilegalmente números de tarjetas de crédito mediante la configuración de tiendas de comercio electrónico con aspecto profesional y camufladas en negocios legítimos.

Acción no autorizada: Una persona de la competencia o un cliente descontento puede alterar el sitio Web de modo que no funcione bien o que rechace a clientes potenciales.

Revelación no autorizada: Cuando se transmite información de una transacción "abiertamente", los hackers pueden interceptar las transmisiones para obtener información sensible de sus clientes.

Alteración de los datos: El contenido de una transacción se puede interceptar y alterar durante su trayectoria, bien de forma malintencionada o bien de forma accidental. Los nombres del usuario, los números de la tarjeta de crédito y las cantidades en divisas enviadas “abiertamente” son todas vulnerables de alteración.

16. Cómo ponerse en contacto con *thawte*

Si tiene alguna pregunta sobre el contenido de esta guía o sobre los productos y servicios de thawte, póngase en contacto con un asesor de ventas:

Correo electrónico: sales@thawte.com
Teléfono: +27 21 937 8902
Fax: +27 21 937 8967

17. Glosario

Criptografía asimétrica
Método criptográfico en el que se utiliza un par combinado de clave pública y privada para la encriptación y el descifrado de mensajes. Para enviar un mensaje encriptado, un usuario codifica un mensaje con la clave pública del receptor. Al recibirlo, se descifra con la clave privada del receptor. La utilización de diferentes claves para las funciones de codificación y descifrado se conoce como la función de trampilla unidireccional, es decir, la clave pública se utiliza para codificar un mensaje pero no se puede utilizar para descifrarlo. Sin saber la clave privada, es prácticamente imposible invertir esta función gracias a las potentes funciones de codificación modernas.

Autoridad de certificación
Una autoridad de certificación (CA) es una organización (como *thawte*) que emite y gestiona credenciales de seguridad y claves públicas para la encriptación de mensajes.

Solicitud de firma de certificado (CSR)
La CSR es una clave pública que usted genera en su servidor y que valida la información específica del ordenador relativa a su servidor de la Web y organización al solicitar un certificado de *thawte*.

Clave privada
Una clave privada es un código numérico utilizado para descifrar mensajes codificados con una única clave pública correspondiente. La integridad de la codificación depende de que la clave privada sea mantenida en secreto.

Clave pública
Una clave pública es un código numérico que habilita la codificación de mensajes enviados al propietario de la única clave privada correspondiente. La clave pública puede circular libremente sin comprometer la codificación mientras aumenta la eficacia y la conveniencia de habilitar la comunicación codificadan.

Criptografía simétrica
Método criptográfico en el que se utiliza la misma clave para encriptación y descifrado. Este enfoque se ve afectado por el riesgo de seguridad involucrado en la distribución segura de la clave dado que se debe comunicar tanto al receptor como al emisor sin ser revelada a terceros.