WHITE PAPER:
GUÍA PARA PRINCIPIANTES
SOBRE LOS CERTIFICADOS SSL

White paper

Guía para principiantes sobre los certificados SSL

Cómo tomar la mejor decisión a la hora de considerar sus opciones de seguridad en Internet

Symantec

Norton SECURED powered by Symantec

Guía para principiantes sobre los certificados SSL

Cómo tomar la mejor decisión a la hora de considerar sus opciones de seguridad online

CONTENIDO

Introducción

Independientemente de que se trate de una persona o una empresa, usted se debe encargar de la seguridad online de la misma manera en que se encarga de la seguridad física en su hogar o su empresa. No solo le hará sentir más seguro, sino que además protege a las personas que visitan su hogar, el lugar de trabajo o el sitio web. Es importante comprender los riesgos potenciales y asegurarse de estar totalmente protegido contra ellos. En el vertiginoso mundo de la tecnología, no siempre es sencillo mantenerse al día con los avances más recientes. Por este motivo, es aconsejable asociarse con una empresa de seguridad en Internet de buena reputación.

Esta guía desmitificará la tecnología involucrada y le brindará la información que necesita para tomar la mejor decisión a la hora de considerar sus opciones de seguridad online. Para ver un glosario de términos, consulte “Términos técnicos para inexpertos” al final de este documento.

¿Qué es un certificado SSL?

Un certificado SSL es un archivo informático digital (o un código de tamaño pequeño) que tiene dos funciones específicas:

1. **Autenticación y verificación**: el certificado SSL tiene información acerca de la autenticidad de ciertos datos referentes a la identidad de una persona, empresa o sitio web, la cual se mostrará a los visitantes en su sitio web cuando estos hagan clic en el símbolo del candado del navegador o en la marca de confianza (por ejemplo, el sello Norton™ Secured). Los criterios de aprobación que usan las autoridades de certificación para determinar si un certificado SSL se debe emitir son más estrictos para un certificado SSL Extended Validation (EV), lo cual le convierte en el certificado SSL disponible de mayor confianza.
2. **Cifrado de datos**: el certificado SSL también posibilita el cifrado. Esto significa que absolutamente nadie, excepto el destinatario deseado, puede interceptar y leer la información confidencial que se intercambia por la Web.

De la misma manera que un documento de identidad o un pasaporte solo puede ser emitido por funcionarios gubernamentales de un país, un certificado SSL es más confiable cuando es emitido por una autoridad de certificación (CA) de confianza. La autoridad de certificación debe seguir políticas y reglas muy estrictas acerca de quién puede recibir un certificado SSL y quién no puede hacerlo. Cuando tiene un certificado SSL válido de una autoridad de certificación de confianza, hay un mayor grado de confianza por parte de sus clientes o partners.

¿Cómo funciona el cifrado SSL?

De la misma manera que usted cierra y abre las puertas con una llave, el cifrado usa claves para bloquear y desbloquear su información. A menos que tenga la clave correcta, usted no podrá “abrir” la información.

Cada sesión de SSL consta de dos claves:

- La clave pública se usa para cifrar (codificar) la información.
- La clave privada se usa para descifrar (decodificar) la información y restaurarla a su formato original para que pueda ser leída.

La sigla SSL significa “capa de socket seguro”. Se trata de una tecnología que establece un vínculo de sesión segura entre el navegador web del visitante y su sitio web, de modo que todas las comunicaciones que se transmiten mediante este vínculo se cifran y, por lo tanto, son seguras. La tecnología SSL también se usa para transmitir correos electrónicos, archivos y otro tipo de información de manera segura.

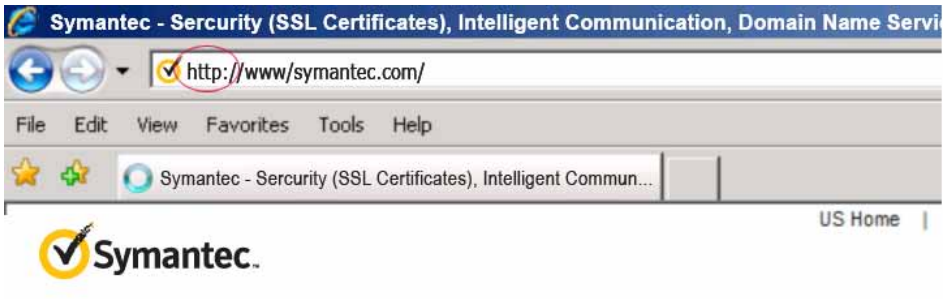
¿Usted le enviaría a alguien su información privada o datos bancarios en el reverso de una postal?

SSL crea un canal privado y seguro para que usted se comunique.

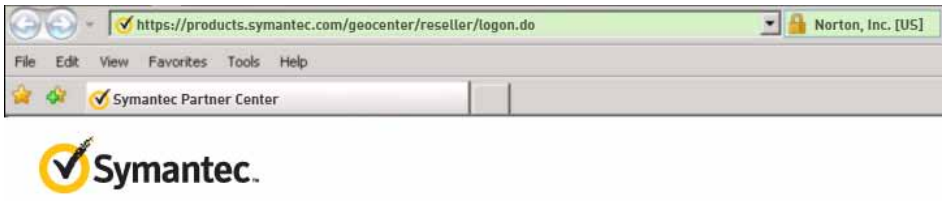
El proceso: cada certificado SSL que se emite para una entidad verificada por una autoridad de certificación se emite para un dominio de sitio web (*dirección de sitio web*) y servidor específicos. Cuando una persona usa el navegador para dirigirse a la dirección de un sitio web con un certificado SSL, se establece un protocolo de enlace de SSL (*reconocimiento*) entre el navegador y el servidor. Se solicita información del servidor, la cual entonces es visible para la persona en su ventana del navegador. Usted notará cambios que indican el inicio de una sesión segura, por ejemplo, aparecerá una marca de confianza. Si hace clic en la marca de confianza, verá información adicional, como el período de validez de un certificado SSL, el dominio asegurado, el tipo de certificado SSL y la autoridad de certificación que emite el certificado. Todo esto significa que se estableció un vínculo seguro para esa sesión con una clave de sesión única y que pueden comenzar las comunicaciones seguras.

¿Cómo sé que un sitio tiene un certificado SSL válido?

1. Un sitio web estándar sin seguridad SSL muestra “http://” antes de la dirección del sitio web en la barra de direcciones del navegador. Este alias significa “protocolo de transferencia de hipertexto” y es la manera convencional para transmitir información por Internet.



En cambio, un sitio web protegido con un certificado SSL mostrará “https://” antes de la dirección. Esto significa “HTTP seguro”.



2. También verá el símbolo de un candado en la parte superior o inferior del navegador de Internet (según del navegador que use).
3. Con frecuencia, además, notará una marca de confianza que se muestra en el sitio web en sí. Los clientes de Symantec™ usan como marca de confianza el sello Norton Secured en sus sitios web. Cuando usted hace clic en el sello Norton Secured o en el símbolo del candado en la página, se mostrarán datos detallados del certificado con toda la información de la empresa, verificada y autenticada por la autoridad de certificación.
4. Al hacer clic en el candado cerrado en la ventana del navegador o en determinadas marcas de confianza SSL, como el sello Norton Secured, el visitante del sitio web ve el nombre de la organización autenticada. En los navegadores de alta seguridad, el nombre de la organización autenticada se

muestra de manera prominente, y la barra de direcciones aparece de color verde cuando se detecta un certificado SSL Extended Validation (EV). Si la información no coincide o el certificado caducó, el navegador muestra un mensaje de error o una advertencia.

¿Dónde usaría yo un certificado SSL?

La repuesta corta a esta pregunta es que usted usaría un certificado SSL siempre que desee transmitir la información de manera segura.

A continuación, se muestran algunos ejemplos:

- Proteger la comunicación entre el sitio web y el navegador de Internet del cliente.
- Proteger las comunicaciones internas en la intranet corporativa.
- Proteger las comunicaciones de correo electrónico entrantes y salientes de la red (*o de una dirección personal de correo electrónico*).
- Proteger la información entre servidores (*tanto internos como externos*).
- Proteger la información que se envía y se recibe mediante dispositivos móviles.

Diferentes tipos de certificados SSL

En la actualidad, existe en el mercado una cantidad de certificados SSL diferentes.

- El primer tipo de certificado SSL es un certificado autofirmado. Como su propio nombre indica se trata de un certificado generado con fines internos y no es emitido por una autoridad de certificación. Dado que el propietario del sitio web genera su propio certificado, este no tiene el mismo peso que un certificado SSL completamente autenticado y verificado, emitido por una autoridad de certificación.
- Un certificado de dominio validado se considera un certificado SSL básico y se puede emitir rápidamente. La única comprobación de verificación que se realiza es para garantizar que el solicitante es dueño del dominio (dirección del sitio web) donde se piensa usar el certificado. No se realizan comprobaciones adicionales para garantizar que el propietario del dominio es una entidad comercial válida.
- Un certificado SSL totalmente autenticado es el primer paso para generar confianza y seguridad online verdaderas. Estos certificados tardan ligeramente más en emitirse y solo se otorgan una vez que la organización aprueba una determinada cantidad de procedimientos de validación y comprobaciones a fin de confirmar la existencia de la empresa, la propiedad del dominio y la autoridad del usuario para solicitar el certificado.

Todos los certificados SSL de Symantec son completamente autenticados.

- Si bien un certificado SSL puede admitir cifrado de 128 bits o 256 bits, ciertos navegadores y sistemas operativos anteriores todavía no se pueden conectar en este nivel de seguridad. Los certificados SSL con una tecnología denominada “criptografía canalizada en el servidor” (SGC) posibilitan el cifrado de 128 bits o 256 bits a más del 99,9% de visitantes de sitios web. Sin un certificado SGC en el servidor web, los navegadores y los sistemas operativos que no admitan el sólido cifrado de 128 bits solamente recibirán cifrado de 40 bits o de 56 bits. Los usuarios con ciertos navegadores y sistemas operativos anteriores se

actualizarán temporalmente a un cifrado SSL de 128 bits si visitan un sitio web con un certificado SSL habilitado para SGC. Para obtener más información acerca de la tecnología SGC, visite el sitio: www.symantec.es/ssl-certificates.

- Con frecuencia, se usa un nombre de dominio con una cantidad de sufijos de host diferentes. Por esta razón, puede emplear un certificado comodín que le permita proporcionar seguridad SSL completa a cualquier host de su dominio, por ejemplo, host.su_dominio.com (donde "host" varía, pero el nombre de dominio se mantiene igual).
- Similar al certificado comodín, pero un poco más versátil, el certificado SSL de SAN (nombre alternativo de sujeto) permite que se agregue más de un dominio a un solo certificado SSL.
- Los certificados de firma de código están especialmente diseñados para garantizar que el software descargado no fue manipulado mientras se transmitía. Hay muchos cibercriminales que manipulan el software disponible en Internet. Pueden adjuntar un virus u otro software malicioso a un paquete inocuo mientras este se descarga. Estos certificados aseguran que esto no suceda.
- Con frecuencia, los certificados SSL Extended Validation (EV) ofrecen el estándar de autenticación más alto del sector y proporcionan el mejor nivel de confianza disponible para el cliente. Cuando los consumidores visitan un sitio web protegido con un certificado SSL EV, la barra de direcciones aparece de color verde (en los navegadores de alta seguridad) y se muestra un campo especial con el nombre del propietario legítimo del sitio web junto con el nombre del proveedor de seguridad que emitió el certificado SSL EV. En la barra de direcciones, también se muestra el nombre del titular del certificado y de la autoridad de certificación que lo emite. Esta prueba visual de certeza ha ayudado a incrementar la confianza del consumidor en el comercio electrónico.

Términos técnicos para inexpertos

Cifrado: la información se "codifica" para que no la use nadie que no sea el destinatario deseado.

Descifrado: se trata de la "decodificación" de la información y de su conversión al formato original.

Clave: una fórmula matemática o algoritmo que se usa para cifrar o descifrar la información. De la misma manera que una cerradura con varias combinaciones diferentes es más difícil de abrir, cuanto mayor es la longitud de la clave de cifrado (medida en números de bits), más sólido es el cifrado.

Navegador: un programa de software que se usa para acceder a Internet. Algunos ejemplos: Microsoft Internet Explorer (IE), Mozilla Firefox, Apple Safari, RockMelt y Google Chrome.

Conclusión

La confianza marca la diferencia de manera rotunda en el mundo de los negocios online. Las inversiones en tecnología para proteger a los clientes y ganar su confianza es un factor crítico de éxito para cualquier empresa que hace negocios online o que aloja un sitio web de comercio electrónico. La implementación efectiva de certificados SSL y la correcta colocación y uso de marcas de confianza son herramientas probadas en la generación de la confianza del cliente.

Para obtener más información, visítenos en www.symantec.es/ssl-certificates.

Más información

Visite nuestro sitio web

www.symantec.es/ssl-certificates

Para obtener más información acerca de los certificados SSL de Symantec, llame a nuestro número gratuito 900 93 1298, o escribanos a: talk2us-es@symantec.com

Para hablar con un especialista en productos

Para comunicarse con un especialista de productos llame al 900 93 1298

Acerca de Symantec

Symantec es un líder mundial en soluciones de seguridad, almacenamiento y gestión de sistemas, que ayudan a consumidores y organizaciones a proteger y gestionar su información. Nuestros servicios y software protegen contra más riesgos, en más puntos y de forma más completa y eficaz, ofreciendo tranquilidad sin importar el lugar donde se utilice o almacene la información.

Symantec Spain S.L.
Parque Empresarial La Finca – Somosaguas,
Paseo del Club Deportivo, Edificio 13, oficina D1, 28223, Pozuelo de Alarcón,
Madrid, España