



Introducción a la tecnología SSL

Es importante que todos los socios que estén interesados en distribuir certificados SSL entiendan a la perfección los principios básicos de la seguridad SSL y los tipos de certificados SSL que GlobalSign oferta (y que, por ende, sus socios pueden distribuir).

A medida que aumenta el volumen de transacciones de comercio electrónico y las organizaciones adoptan más servicios online, la seguridad comienza a jugar un papel cada vez más importante en empresas de todos los tamaños. Es vital que usted, como distribuidor, informe y eduque a sus clientes sobre la importancia de proteger las transacciones online, las transferencias de datos, el tráfico en las redes de trabajo y las comunicaciones digitales. Con ello, no sólo protegerá al usuario final, mejorará la reputación de sus clientes y multiplicará el número de sus transacciones, sino que además maximizará su potencial de generación de ingresos.

Desde la perspectiva de los consumidores, las amenazas de la era digital, como los ataques de phishing o los robos de identidad, siguen en aumento, y los clientes electrónicos demandan hoy mayores niveles de seguridad que en el pasado. Que los certificados SSL son un requisito operativo fundamental para todas las organizaciones con presencia en la Red es, hoy por hoy, un hecho innegable. Informe ahora a sus clientes de la necesidad de contar con un certificado SSL.

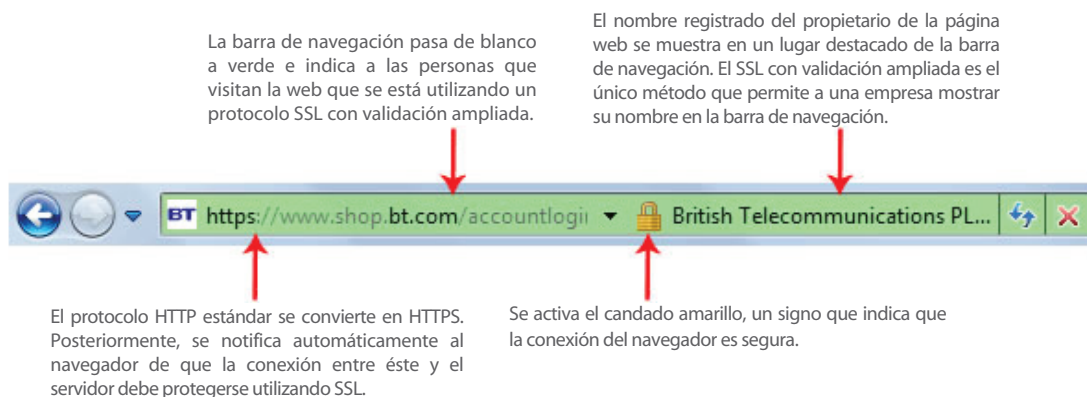
¿Qué es el SSL?

El Nivel de Conectores Seguros (Secure Sockets Layer o SSL) y la Seguridad del Nivel de Transporte (Transport Layer Security o TLS) son los protocolos de seguridad de uso común en la actualidad. Se trata de protocolos que establecen un canal seguro entre dos ordenadores conectados a través de Internet o de una red interna. En nuestra vida cotidiana, en la que Internet juega un papel tan destacado, es habitual comprobar como las conexiones entre navegadores web y servidores web realizadas a través de conexiones de Internet no seguras emplean tecnología SSL. Técnicamente, el protocolo SSL es un método transparente para establecer una sesión segura que requiere una intervención mínima por parte del usuario final. En la práctica, el navegador alerta al usuario de la presencia de un certificado SSL mostrando un icono con forma de un candado o coloreando de verde la barra de navegación. Si se trata de un certificado SSL con validación ampliada, el navegador muestra tanto el candado como la barra de navegación verde. En este hecho reside el éxito del protocolo SSL: es una experiencia sorprendentemente sencilla para los usuarios finales.

Los certificados SSL son un servicio fundamental para todas las páginas web que reciben transacciones de comercio electrónico o recopilan cualquier tipo de información de clientes.

Se espera que antes de 2014 37 millones de personas realicen compras a través de Internet por un valor anual que rondará los 64 millones de euros. En 2008 se detectaron 135.426 ataques de phishing en todo el mundo, de los cuales el 40% se produjeron en el Reino Unido. El número de ataques de phishing en todo el mundo creció en 2008 un 60% con respecto al año anterior, con un pico claro en abril, mes en el que se identificaron más de 15.000 ataques diferentes. www.silicon.com

Certificados SSL con validación ampliada, como ExtendedSSL (EV) de GlobalSign



Certificados SSL estándar, como DomainSSL y OrganizationSSL de GlobalSign



El SSL es una tecnología esencial en la lucha contra los delitos de phishing, los ataques de intrusos (MitM) y el fraude en Internet.

A diferencia de las URL HTTP, que comienzan con el protocolo "http://" y emplean el puerto 80 por defecto, las URL HTTPS comienzan con el protocolo "https://" y emplean el puerto 443 por defecto. El protocolo HTTP es inseguro y susceptible de sufrir ataques de intrusos. Si los datos confidenciales transmitidos (por ejemplo, los datos de una tarjeta de crédito o la información de usuario de una cuenta) cayesen en manos de la persona equivocada, los intrusos podrían acceder a cuentas online y consultar información confidencial. Sin embargo, cuando se emplea un protocolo HTTPS para enviar información a través de un navegador, la información se encripta y se protege.

Los certificados SSL se utilizan para autenticar servidores, encriptar datos y comprobar la integridad de los mensajes. Además, permiten encriptar las comunicaciones a través de Internet, protegiendo su contenido frente a lectores no autorizados.

Ejemplos prácticos de seguridad SSL

¿Cuál es el uso práctico de la tecnología SSL en una sociedad moderna en la que abundan las transacciones de comercio electrónico?

- **En el tráfico web, como las transacciones con tarjetas de crédito**
- **En otros tipos de tráfico web, como en las páginas de acceso, los formularios web, el correo web, los paneles de control o sencillamente en la protección de páginas web**
- **En la transferencia de archivos sobre https y servicios de FTP, como las actualizaciones de nuevas páginas por parte de un propietario de una página web**
- **En conexiones entre clientes de correo electrónico y servidores de correo electrónico como En el tráfico de intranets, como en el caso de las redes internas, las extranets o las conexiones a bases de datos**
- **En el tráfico de intranets, como en el caso de las redes internas, las extranets o las conexiones a bases de datos**

Todas estas aplicaciones tienen puntos en común:

- **Es necesario proteger la confidencialidad de los datos transmitidos a través de Internet o de cualquier otra red, ya que nadie desea que la información de su tarjeta de crédito quede expuesta en la Red**
- **Es necesario garantizar la integridad de estos datos para evitar que, una vez se han enviado los datos de la tarjeta de crédito y se ha confirmado el importe, un hacker que haya podido interceptar la información pueda modificar la cantidad cobrada o desviar los fondos**
- **Su empresa debe garantizar a sus clientes o a los usuarios de su extranet la autenticidad de su identidad y eliminar cualquier sombra de duda sobre la posibilidad de que un tercero esté suplantándola**
- **Su organización debe cumplir las normativas regionales, nacionales e internacionales en materia de privacidad, seguridad e integridad de los datos**

¿Qué es un certificado SSL?

El SSL es un protocolo para cuyo uso es necesario contar con un certificado SSL. Un certificado SSL es un pequeño archivo de datos que vincula digitalmente una clave de encriptación con los datos de su empresa. Generalmente estos datos son:

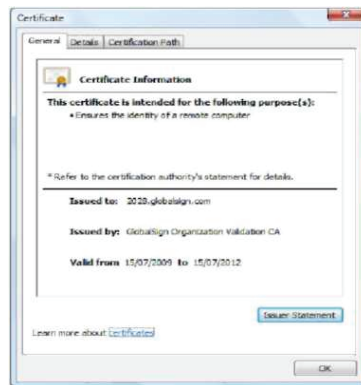
- **Su nombre de dominio o de servidor**
- **El nombre y la ubicación de su empresa**
- **En determinados casos, la información de contacto**

El Nivel de Conectores Seguros (SSL) es un protocolo de encriptación que protege las transacciones y la integridad de los datos en las comunicaciones a través de redes, como por ejemplo Internet.

Para poder iniciar sesiones SSL con navegadores, las organizaciones deben solicitar e instalar el certificado SSL en sus servidores web. Dependiendo del certificado SSL solicitado, la organización deberá superar determinados niveles de inspección. Tras la instalación, al intentar acceder a la página web <https://www.domain...>, el certificado solicitará al servidor que establezca una conexión segura con el navegador, la cual en lo sucesivo protegerá todo el tráfico entre el servidor web y el navegador.

Los certificados SSL deben haber sido emitidos a partir del certificado raíz de una Autoridad de Certificación reconocida. El certificado raíz debe estar presente en el ordenador del usuario final para que el certificado SSL indique que la conexión es fiable. En caso contrario, el navegador mostrará al usuario final un mensaje de error alertando de una conexión no fiable. En el caso de las transacciones de comercio electrónico, estos mensajes de error generan dudas inmediatas acerca de la página web. Por ello, las páginas web que emplean certificados SSL no fiables corren el riesgo de perder la confianza depositada en ellas y dejar de recibir pedidos de la mayoría de sus clientes.

Las empresas como GlobalSign son Autoridades de Certificación reconocidas. Este reconocimiento se debe a que los proveedores de navegadores y sistemas operativos como Microsoft, Mozilla, Opera, BlackBerry, Java, etc. confían en la legitimidad de la Autoridad de Certificación GlobalSign y en su capacidad para emitir certificados SSL de confianza. Cuantas más aplicaciones, dispositivos y navegadores dispongan de la raíz de la Autoridad de Certificación registrada e integrada, mayor es el grado de "reconocimiento" y seguridad que los certificados SSL pueden ofrecer.



Los certificados SSL se utilizan para autenticar servidores, encriptar datos y comprobar la integridad de los mensajes. Además, permiten encriptar las comunicaciones a través de Internet, protegiendo su contenido frente a lectores no autorizados.

Para consultar más artículos informativos sobre la seguridad SSL, visite GlobalSign.com/ssl-information-center