Certificados de seguridad para proteger la información que se mueve en tu web

Internet se ha convertido en algo fundamental en nuestra vida. Cada día que pasa, su uso es mayor, y desde la red podemos hacer prácticamente cualquier tipo de acción. En muchos casos, la información que se mueve es de gran importancia, de ahí que sea necesario contar con algún sistema de seguridad que proporcione seguridad extra a toda esa información. Esto lo conseguimos con el uso de los certificados de seguridad, de los que hablaremos a lo largo de este White Paper.

¿Qué es un certificado de seguridad?

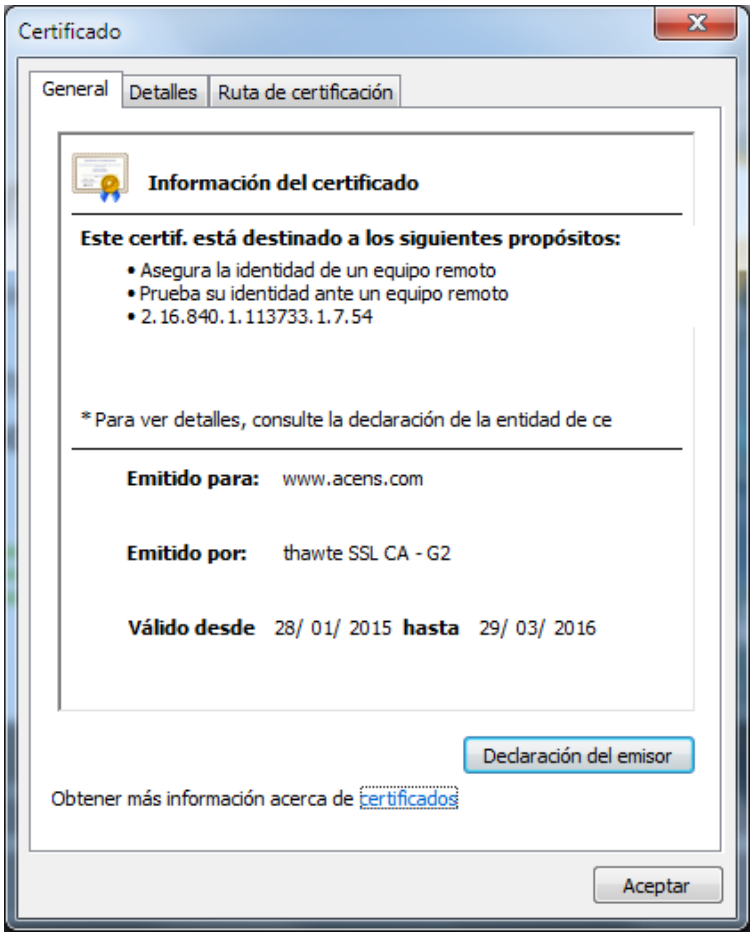
Los certificados de seguridad son un añadido extra a nuestras webs para todas aquellas personas que la visitan y hacen algún tipo de transacción desde ella. Para mejorar esta seguridad, lo que hacen estos certificados es encriptar la información que se mueve desde el portal y así evitar que terceras personas puedan capturarla.

El encargado de ofrecer esta seguridad es el SSL (Secure Socket Layer), que es un protocolo de seguridad desarrollado por la empresa Netscape Communications para lograr la transmisión de datos entre el usuario y el servidor, o viceversa, de forma totalmente segura. Este protocolo de seguridad puede ser utilizado sobre cualquier protocolo de servicios comunes relacionados con Internet como son HTTP, FTP, SMTP... aunque lo más habitual es utilizarlo con el tráfico de la web.

¿Cómo saber si una web hace uso de un certificado de seguridad?

Saber si un sitio hace o no uso de un certificado SSL es fácil, pudiéndose ver a simple vista en los principales navegadores del mercado.

Podemos saber que una página web hace uso de algún certificado de seguridad si al navegar por ella, en la barra de direcciones del navegador aparece reflejado el protocolo "HTTPS", que significa HTTP seguro. Otra opción que nos ofrecen algunos navegadores es la aparición de un icono en forma de candado que nos informa de que hace uso de un certificado. Pulsando sobre ese candado, podemos ver información referente al certificado instalado. Por ejemplo **en Chrome pulsando el candado con botón derecho hacemos clic en 'Conexión -> Datos del certificado'**.



Ventajas en el uso de los certificados de seguridad

El uso de certificados SSL en nuestro portal web ofrece un gran número de ventajas. Veamos a continuación algunas de las más importantes.

- **Mejora la seguridad**. Con su uso, garantizamos que toda la información que se mueva entre el ordenador del usuario y portal vaya encriptada.
- **Aumenta la confianza**. Los usuarios confían más en los portales que utilicen un certificado que en otros que no lo hagan, ya que en caso de robo, saben que su información estará cifrada.
- **Certificas que realmente eres tú**. Con el uso de estos certificados, estamos garantizando a los visitantes que realmente somos quien decimos ser, y de esta forma luchar contra ciertos problemas que hay en la red como es el caso de phishing.
- **Legitimación de la página web**. Conseguimos que una entidad independiente dé el visto bueno a nuestro sitio.
- **Aumento del tráfico de tu web**. Desde hace algún tiempo, los principales buscadores, posicionan mejor a los sitios que hacen uso de estos certificados ya que ofrecen una mayor seguridad que otros sitios que no lo utilizan.
- **Evitamos que los usuarios se vayan del sitio**. Esto ocurre sobre todo con el comercio online, ya que a la hora de introducir los datos de tu tarjeta para realizar la compra, si vemos que no aparece el protocolo "https" por ningún lado, el usuario podría abandonar esa compra a no tener la garantía de que su información vaya encriptada.
- **No da problemas**. El uso de SSL es compatible con el 99% de los navegadores actuales del mercado, por no decir el 100%.

Conceptos de interés que intervienen en el uso de los SSL

A la hora de trabajar con certificados de seguridad, es bueno tener presente algunos conceptos que nos pueden aparecer. Expliquemos a continuación algunos de los más importantes.

a) Cifrado
El cifrado es un concepto que hemos comentado a lo largo de este libro blanco y que consiste en transformar la información de tal manera que no pueda ser entendible por cualquier usuario que la recoja. Esta transformación se lleva a cabo partiendo del uso de un elemento denominado llave. Sólo aquellos que tengan esta llave podrán conocer la información.

b) Llave pública
Se trata de una clave que está asociada a una persona o entidad y que es utilizada para cifrar la información mediante el uso de distintos algoritmos de cifrado.

c) Llave privada
Al igual que en el caso anterior, esta también está asociada a una persona o entidad, y es la que se utiliza para realizar el descifrado de la información. Sólo el conocedor de esta clave tendrá acceso a la información original.

d) Firma digital
Es algo similar a nuestra firma. Es algo que nos identifica y que nos diferente del resto de personas. Esta firma digital se elabora partiendo de la llave privada, por lo que es única y no hay dos iguales.

e) Autoridad certificadora
Una autoridad certificadora es una entidad que se encarga de garantizar que el poseedor de un certificado es quien dice ser.

f) Certificado digital SSL
Se trata de un documento que contiene información sobre el usuario o compañía que lo ha dado de alta. En ella nos podemos encontrar información como nombre, email, organización a la que pertenece o su clave pública.

Funcionamiento de los certificados de seguridad

Pasemos a explicar cómo funciona la comunicación segura entre un usuario y una página web. Lo primero que debemos hacer es escribir en la barra de direcciones de nuestro navegador la URL utilizando el protocolo HTTPS, por ejemplo, https://www.acens.com. En esta petición, el navegador envía un mensaje al sitio de destino indicando que quiere establecer conexión segura, a la vez que le envía información sobre la versión del protocolo SSL que soporta y otros parámetros de interés para llevar a cabo la conexión.

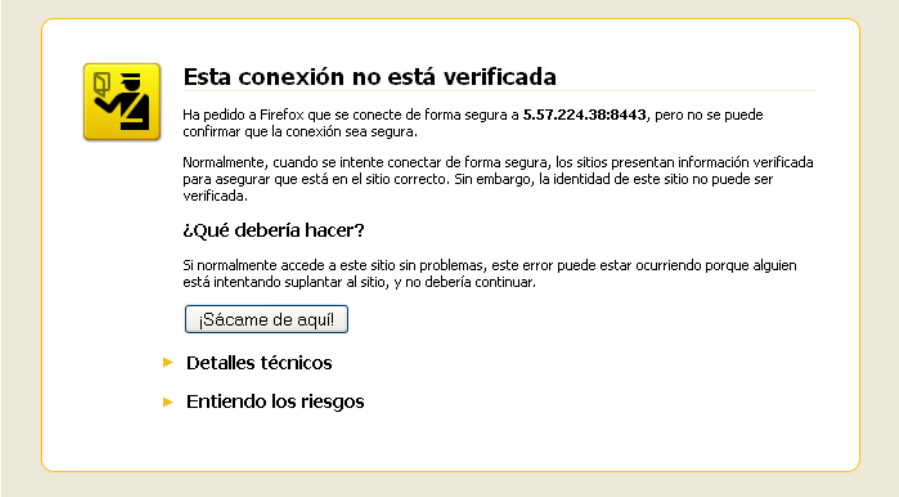
En base a la información enviada por el navegador, el servidor web de la página de destino responde con un mensaje informando que está de acuerdo con establecer una conexión segura con los datos suministrados.

Una vez que ambos conocen los parámetros de conexión, el sitio de destino presenta su certificado de seguridad para presentarse como un sitio confiable.

Cuando el navegador tiene en su poder el certificado que le ha enviado el sitio que queremos visitar, hace una serie de comprobaciones previas antes de confiar plenamente en el sitio. Estas comprobaciones que lleva a cabo son:

- **Integridad de certificado**. El navegador verifica si el certificado se encuentra íntegro y para comprobarlo, lo que hace es descifrar la firma digital incluida en él mediante la llave pública y comparándola con una generada en ese momento. Si ambas son iguales, el certificado es válido.
- **Vigencia del certificado**. También revisa si el certificado no está expirado.
- **Verifica emisor del certificado**. Para llevar a cabo esta comprobación, hace uso de la lista de certificados raíz almacenada en nuestro equipo y que contienen las llaves públicas de las

autoridades certificadoras conocidas. En base a esa lista, el navegador revisa que esté en ella, de no estarlo, mostrará un mensaje indicando que el certificado es emitido por un certificado en la que no confía.



Esto no significa que el certificado no sea válido, sólo que el navegador no lo reconoce, pero aún así, la información se enviaría codificada.

Cómo obtener un certificado SSL

Tras todo lo visto a lo largo de este White Paper, sólo cabe decir que si quieres mejorar la seguridad de los datos que se mueve desde tu web, la mejor opción es dar de alta un SSL a través de un proveedor especializado. Por ejemplo puedes **contratar un certificado de seguridad con acens**, con diferentes precios según el tipo de certificación.