Universidad Técnica Federico Santa María

Semiracio de Redes de computadores

ELO-323

"Implementación y análisis del protocolo HTTPS"

Francisco Cid
francisco.cidn@alumnos.usm.cl
Vanessa Pulgar
vanessa.pulgar@alumnos.usm.cl

Profesor: Agustín González

1. Introducción

HTTPS (Hypertext Transfer Protocol Secure), como su nombre lo dice es un protocolo de aplicación en el cual se implementa el protocolo HTTP (Hypertext Transfer Protocol) con seguridad. A nivel mundial esta comenzando una migración desde el protocolo HTTP a HTTPS, esto tiene que ver con la seguridad con la que los usuarios de las distintas páginas web puedan tener confianza en el lugar donde dejan sus datos.

Para el e-commerce por ejemplo el protocolo estudiado tiene muchas ventajas que se traducen en la seguridad con la cual viajan por la red los datos privados.

2. ¿Por qué HTTPS?

Como ya se menciona HTTPS es la forma segura de envío a través del protocolo HTTP mediante la red, usando un puerto distinto a éste, HTTP utiliza el puerto 80 y HTTPS el 443. Se refiere tanto a HTTP sobre SSL como a HTTP sobre TLS, que es una versión actualizada de SSL 3.0, los cuales son protocolos criptográficos que permiten la encriptación de datos.

Ventajas:

- Encripta el flujo de datos desde y hacia la página web, lo que es importante para los datos privados de los usuarios en contra del tipo de ataques man-in-the-middle .
- Garantiza que el dominio está asociado a el lugar donde se necesita navegar.
- Contiene capas de seguridad que permite que los ataques malintencionados tengan mayor dificultad en infectar.

Desventajas:

- Si la página logra ser infectada por algún archivo o software malicioso que desee transmitir datos, estos se transmitirán como seguros.
- La migración de HTTP a HTTPS puede que baje el rendimiento de la página web.

3. Protocolos SSL y TLS

SSL (Secure Socket Layer) es un protocolo criptográfico que proporciona comunicaciones seguras por una red, o en servidores web (en general en Internet) mediante el uso de algoritmos de encriptación y la utilización de certificados encriptados por un tercero de confianza para ambos (Autoridad Certificadora), que lleva los datos del emisor, el nombre de la página web a validar, una clave de encriptación asimétrica y la firma del documento de la Autoridad Certificadora.

Además, este protocolo en vez utiliza para el envio y recibo de datos el puerto 443 mediante un handshaking para negociar la seguridad.

El protocolo TLS (Transport Layer Security) sucede al protocolo SSL mejorando sus vulnerabilidades. Este utiliza una conexión insegura primero para luego habilitar el cifrado mediante comandos especiales.

En general cualquiera de los dos protocolos llega a dar una conexión cifrada y segura.
Los certificados, que se detallan próximamente, también (en su mayoría) se pueden utilizar para los dos protocolos.

4. Certificados y Autoridades Certificadoras

Los certificados son un punto clave en el protocolo SSL y por tanto el TLS y el HTTPS. Estos proveen una seguridad y confianza adicional con el sitio en el que se navega.

Las Autoridades Certificadoras (CA) son entidades de confianza que permiten certificar dominios de paginas web para introducirlo en el protocolo SSL. Los requisitos para ser autoridades certiificadoras dependen del país, por ejemplo una clara guía de instrucciones y requisitos para ser CA en Costa Rica se pueden ver en la página (que irónicamente tiene protocolo http) http://www.firmadigital.go.cr/gestionCA.html del ministerio de ciencia y tecnología. En Chile se preocupa de esto el Ministerio de Economía.

Existen 3 tipos de certificados que pueden entregar las CA:

Validación Extendida (EV): El el más completo, y por tanto el que más se demora, se debe cumplir con los siguientes requisitos para obtener este certificado:

- Verificación de la existencia legal, física y operativa de la entidad
- Verificación de que la identidad de la entidad coincide con los registros oficiales
- Verificación de que la entidad tiene el derecho exclusivo a utilizar el dominio especificado en el certificado SSL con EV
- Verificación de que la entidad ha autorizado adecuadamente la emisión del certificado SSL con EV

Validación de Organización (OV): Para obtener esta certificación se hace una investigación simple de si la organización que pide el certificado es dueña del dominio al cual se le esta solicitando la certificación y que la organización exista.

Validación de Dominio (DV) Es el más simple, se verifica en la base de datos WHOIS si el dominio está registrado a nombre de quien pidió el certificado. También es la certificación más rápida.

Existen Autoridades Certificadoras gratuitas y de paga. Entre las de paga no existen muchas diferencias entre si, pero las gratuitas se pueden diferenciar en el tiempo de duración del certificado y número de veces que se puede pedir.

Para analizar esto se tomó en cuenta la Autoridad Certificadora Gratuita Let's Encrypt, que tiene las siguientes características:

- Sólo entrega Certificados del tipo Validación de Dominio (DV).
- No todos los navegadores web y móviles los reconocen, sin embargo Google Chrome y Firefox lo recomiendan.
- La duración de los certificados es de 3 meses, luego de los cuales se pueden volver a instalar por 3 meses.
- Sólo se muestra «HTTPS» en la barra del navegador.
- Cada subdominio necesita un certificado adicional y esta CA entrega un máximo de 20 certificados cada 7 días.

Un ejemplo de un certificado de esta Autoridad es el de la Figura 1

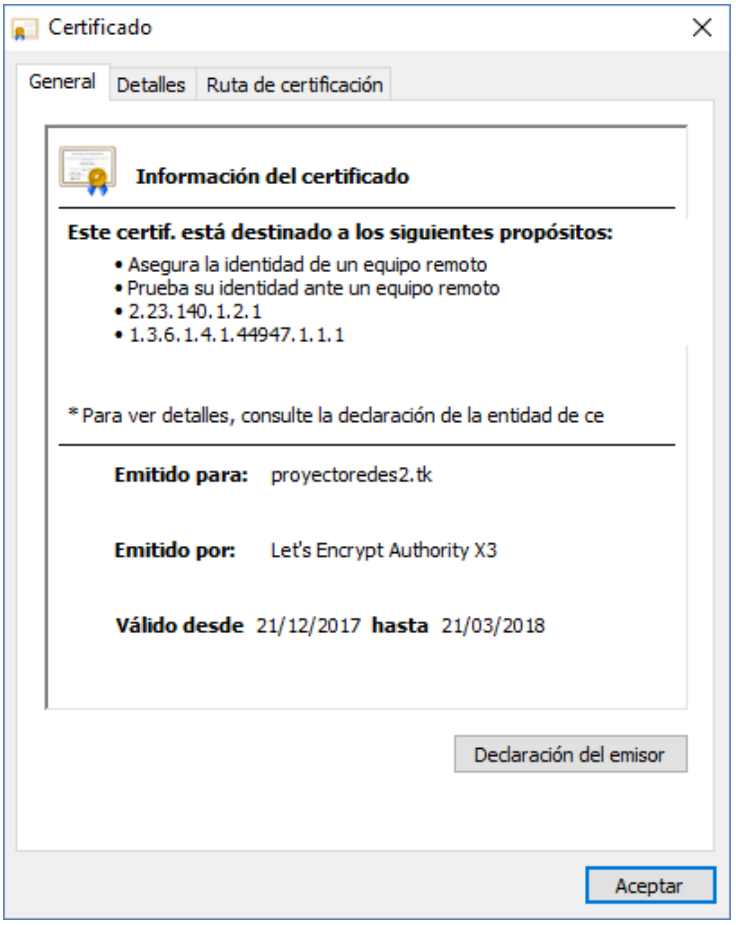

Figura 1: Comprobante de certificado DV de Let's Encrypt en Google Chrome

Para los Certificadores de pago las características son las siguientes:

- Entregan todo tipo de Certificado segúns ea el requerimiento

- Son reconocidos por todos los navegadores
- Tecnología punta de cifrado para encriptar la información del navegador al servidor.
- El Certificado dura 1, 2 o 3 años.
- Muestra HTTPS + barra de dirección en verde + nombre de la empresa en la barra (EV).
- Tiene un sello de confianza
- Garantiza el buen funcionamiento con asistencia técnica

En la Figura **??** se muestra un comprobante de certificado de validación extendida.

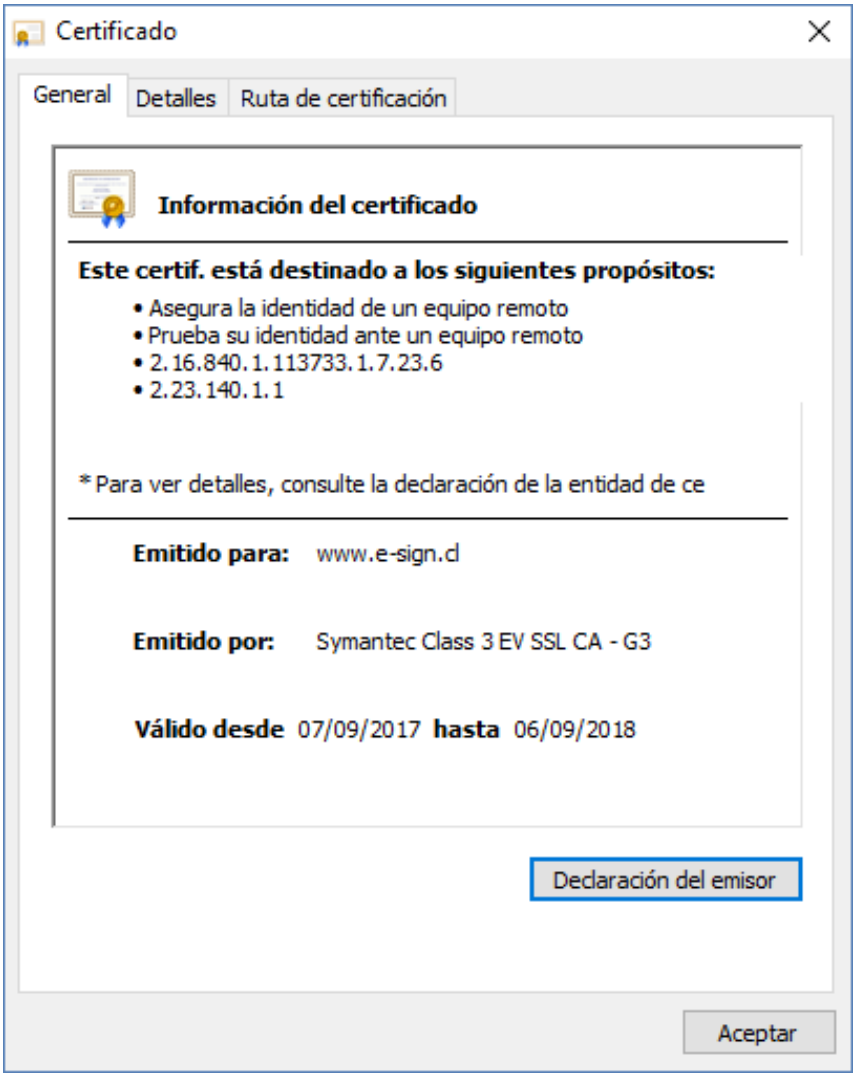

Figura 2: Comprobante de certificado EV de CA Pagada en Google Chrome

5. Cómo crear o migrar una página HTTP a HTTPS

Para que una página sea https es necesario primero tener un certificado de una Autoridad Certificadora. El tipo de certificado (como se menciona anteriormente) depende de la página web que se quiera implementar.

Si se utiliza apache, hay que tener acceso al archivo HTACCESS (hypertext access) que es un archivo de configuración men servidores web basados en Apache que permite a los administradores aplicar distintas políticas de acceso a directorios o archivos para mejorar la seguridad de su página web y evitar acceso a terceros.

Para la **creaciónd e la página web bajo protocolo HTTPS** primero se crea un servidor web de infraestructura LAMP (Linux, Apache, MySQL, PHP) mediante el script provisto en el informe. Luego se vincula la URL www.proyectoredes2.tk a la dirección IP del servidor.

Posterior a esto, se utiliza Certbot para obtener un certificado SSL de Let's Encrypt para la página web (Clave RSA pública de 2048 bits), el cual se renueva automáticamente cada 3 meses. Además, gracias a Certbot, las peticiones HTTP al servidor (y por tanto, al puerto 80), las fuerza a conectarse a través de HTTPS y al puerto 443.

Luego es necesario instalar el certificado y verificar que tenga un buen funcionamiento, como se puede observar en las Figuras 3 y 4.

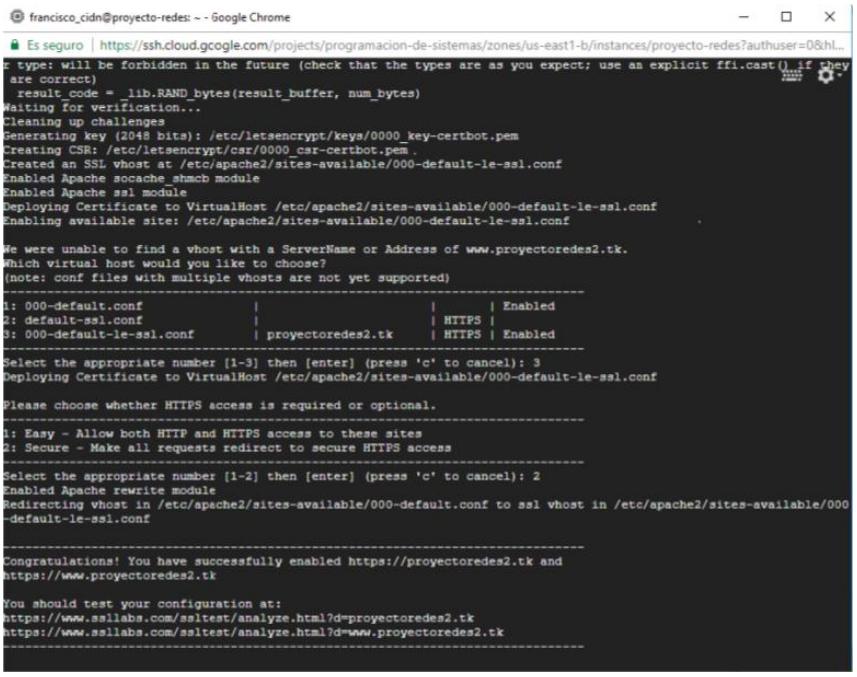

Figura 3: Instalación del certificado

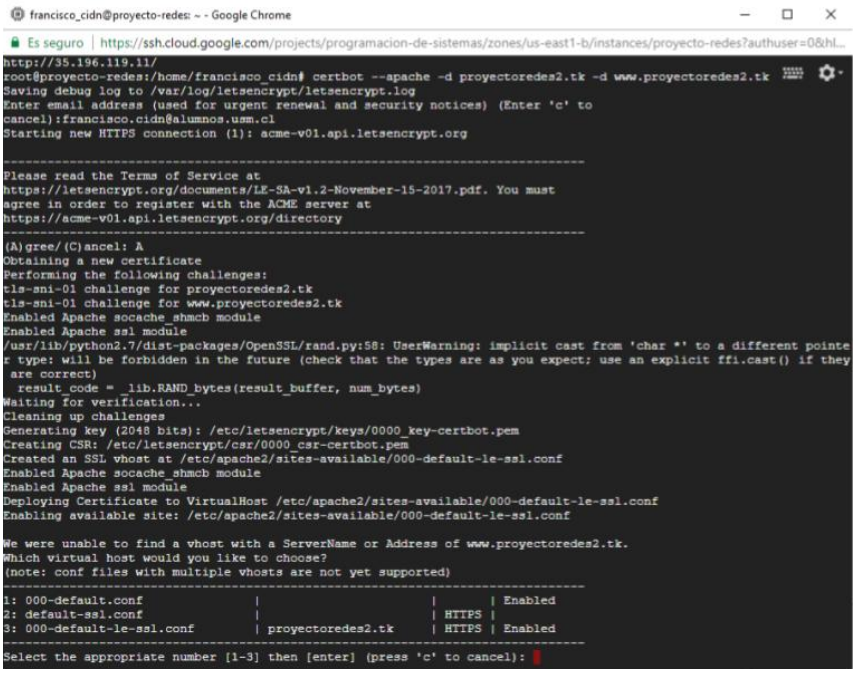

Figura 4: Resultado de la instalación.

Para **migrar una página con protocolo HTTP a HTTPS** se necesita obtener el certificado de la CA y luego instalarlo, actualizar todos los enlaces de redirección para no tener errores 404 dentro de la página. En si mientras más grande sea la página web más difícil es la migración.