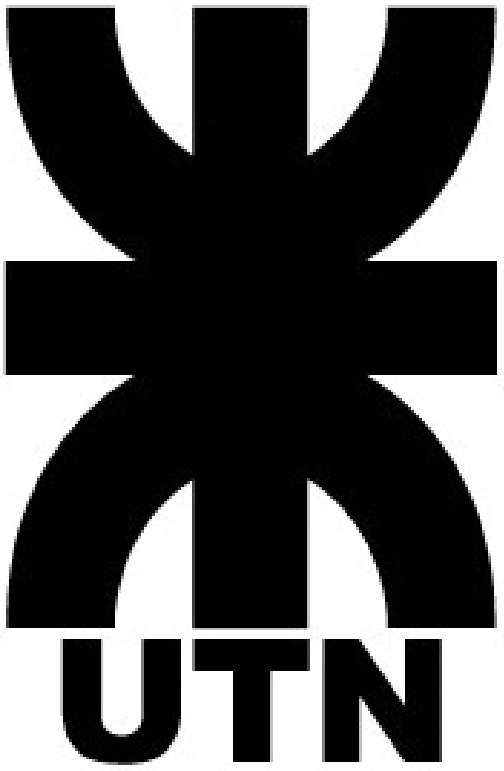
Actividad Semana 3

Certificados SSL

UTN FRC - Integración de Aplicaciones en Entorno Web - 5K4



Cátedra: 5K4
Profesores:

- María Soledad Romero
- Rubén Aníbal Romero

Estudiante:

- 85828 Gutierrez, Santiago

Fecha: 08/09/2024

Índice

Certificado SSL

Un certificado SSL es el recurso que utilizan las empresas y organizaciones en sus sitios web para proteger las transacciones en línea, mantener la privacidad y seguridad de la información del cliente. Es un certificado digital que autentica la identidad de un sitio y habilita la conexión cifrada. La sigla SSL, indica Secure Sockets Layer, un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.

Funcionamiento de los certificados SSL

Mediante un certificado SSL, se asegura que los datos se encuentren encriptados, protegiendo información sensible. Se implementa un protocolo de cifrado asimétrico para establecer la comunicación segura, y luego se utiliza cifrado simétrico mediante la clave de sesión para asegurar la transmisión de datos.

Proceso de implementación

1. **Solicitud de certificado SSL:** Cuando un sitio desea utilizar SSL, debe solicitar un certificado a una Autoridad de Certificación (CA).Esta verifica la identidad del solicitante y emite el certificado SSL si cumple con los requisitos de validación establecidos.
2. **Instalación del certificado:** El certificado emitido se instala en el servidor web del sitio. Contiene una clave pública, la cual es visible para todos los usuarios, y una clave privada, que permanece en el servidor y es secreta.

Establecimiento de conexión segura

1. Un sistema cliente, por ejemplo un navegador como Google Chrome, se conecta a un servidor que tiene un certificado SSL.
2. El navegador envía una solicitud al servidor para que se identifique.
3. El servidor retorna una copia de sus certificado SSL, incluyendo tipo, periodo de validez y detalles organizacionales.
4. El navegador verifica si confía en el certificado y envía una aprobación de vuelta al servidor. Si el certificado no esta instalado, no esta actualizado con protocolos de seguridad adecuados o no está emitido por un CA confiable

para el navegador, el usuario verá un mensaje de advertencia en la barra de direcciones del navegador.

5. El servidor envía de vuelta un acuse de recibo firmado digitalmente para iniciar una sesión cifrada por SSL.
6. Cualquier dato compartido entre el navegador y el servidor ahora está seguro mediante cifrado.

Empresas que proveen certificados SSL

Existen diversas empresas que proporcionan certificados SSL, tanto gratuitos como pagos. Ejemplos de estas son:

- DigiCert
- GlobalSign
- Sectigo
- Comodo SSL
- AlphaSSL
- GoDaddy
- Let’s Encrypt

Entidad autorizante

Las entidades que emiten certificados SSL se denominan **Autoridades de Certificación (CA).** Tienen la responsabilidad de verificar la legitimidad del sitio web que solicita el certificado y emitir el mismo si cumple con los requisitos.

Tipos de certificados SSL

Dependiendo del nivel de validación y la cantidad de dominios que protegen, existen varios tipos de certificados SSL.

Clasificación según la cantidad de dominios

- Certificados SSL de dominio único: Certificado aplicable a un único dominio. No es posible utilizarlo para autenticar ningún otro dominio, ni subdominios.

- Certificados SSL comodín: Certifican un solo dominio y sus subdominios
- Certificados SSL multidominio (MDC): Certifica varios dominios distintos en un único certificado.

Clasificación según el nivel de validación

- Certificados SSL de validación de dominio: Es el nivel menos estricto y el más barato. Solo se debe demostrar el control sobre el dominio que se quiere certificar.
- Certificados SSL de validación de la organización: Implican el contacto entre la CA y la organización solicitante, existiendo la posibilidad de investigación adicional. Estos certificados incluyen nombre y dirección de la organización, otorgando mayor fiabilidad para los usuarios.
- Certificados SSL con validación extendida: Es el mayor nivel de validación, y consiste en una comprobación completa de los antecedentes de la organización. La validación es extensa y la más costosa, pero en consecuencia son los más fiables.

Certificados gratuitos versus certificados pagos

Aspecto	SSL Gratuito	SSL de Pago
Cifrado	Ambos utilizan protocolos criptográficos modernos como SHA-256 y TLS 1.2, 1.3. Los certificados gratuitos como los de Let's Encrypt, Amazon, y Cloudflare usan claves RSA de 2048 bits, actualizables a 4096 bits.	Además de lo ofrecido por el SSL Gratuito, estan disponibles en varias configuraciones según el proveedor.
Validación	Solo Validación de Dominio (DV), confirma control del dominio, pero no la identidad legal del solicitante.	Ofrecen Validación de Dominio (DV), Validación de Organización (OV), y Validación Extendida (EV). Las validaciones OV y EV proporcionan mayor garantía de legitimidad empresarial.

Tamaño del Sitio Web	Adecuado para sitios web personales, blogs y portafolios sin procesamiento de pagos en línea.	Preferido para plataformas de comercio electrónico, ONGs, grandes empresas, startups fintech, e instituciones financieras.
Soporte al Cliente	Menos probable recibir soporte rápido; puede haber retrasos significativos.	Soporte dedicado 24/7 proporcionado por el CA o proveedores como SSL Dragon.
Restricciones Geográficas	Los certificados gratuitos de Amazon pueden no estar disponibles en todas las regiones y solo se instalan en servidores de Amazon.	Los certificados de pago se pueden instalar en casi cualquier lugar del mundo.
Propiedad	No siempre se puede transferir a otros servidores o proveedores de alojamiento.	Total propiedad y control; se puede instalar en cualquier servidor o proveedor de alojamiento.
Compatibilidad con Navegadores	Buen soporte para navegadores modernos, pero menos confiable en versiones antiguas y dispositivos móviles.	Compatible con el 99.9% de los navegadores, sistemas operativos y dispositivos móviles, incluidos los antiguos.
Características de Seguridad	Sin características adicionales de seguridad como evaluaciones de vulnerabilidad y escaneo de malware.	Incluye características adicionales de seguridad, evaluaciones de vulnerabilidad, y escaneo diario de malware.
Periodo de Validez	Válido por 90 días; renovación manual o automática según el servidor.	Válido por hasta 1 año; se pueden adquirir suscripciones de varios años con descuentos.
Garantía	No incluye garantía contra filtraciones de datos o emisión fraudulenta de certificados.	Incluye una garantía que cubre pérdidas financieras en caso de brechas de seguridad, que puede superar un millón de dólares.

Bibliografía

Kaspersky. (s.f.). *Qué es un certificado SSL: definición y explicación*. https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

Sectigo. (s.f.). What is an SSL certificate? https://www.sectigo.com/resource-library/what-is-an-ssl-certificate#:~:text=SSL%20works%20by%20making%20the,a%20secure%201%3A1%20communication.

Cloudflare. (s.f.). *Tipos de certificados SSL: tipos de certificados SSL explicados*. Cloudflare. https://www.cloudflare.com/es-es/learning/ssl/types-of-ssl-certificates/

SSL Dragon. (s.f.). *Free SSL vs. Paid SSL: What is the difference?* SSL Dragon. https://www.ssldragon.com/blog/free-ssl-vs-paid-ssl/