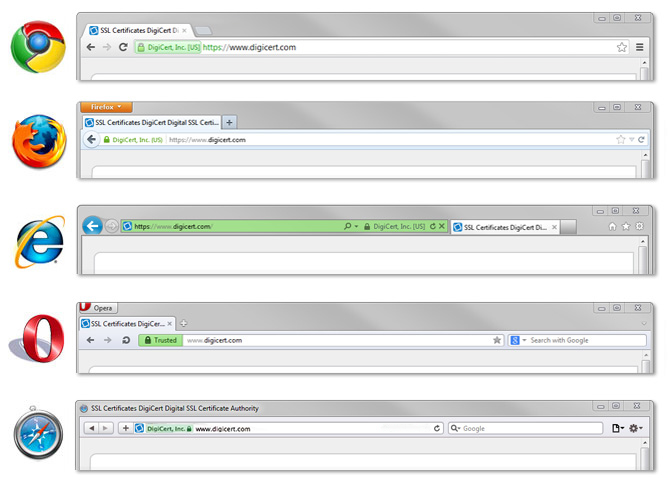
SSL y TLS

SSL (Secure Sockets Layer) és un protocol de seguretat que utilitza certificats digitals per a establir comunicacions segures entre un client i un servidor, normalment entre un servidor web i un navegador o entre un client i un servidor de correu electrònic, és a dir, permet la transmissió segura de dades en línia. Per exemple, quan una web utilitza aquest protocol, en el navegador de l’usuari apareix la direcció d’aquesta manera: https://... i un icona d’un cadenat.



Característiques del protocol SSL

L’objectiu inicial del disseny del protocol SSL va ser protegir les connexions entre clients i servidors web amb el protocol HTTP. No obstant, les funcions de seguretat no es van implementar directament en el protocol d’aplicació HTTP, sinó que van ser introduïdes en un protocol apart. D’aquesta manera podria haver moltes aplicacions que fessin ús d’aquesta funcionalitat.

Els serveis de seguretat que proporcionen els protocols SSL/TLS són:

Confidencialitat: a l’inici de cada sessió, client i servidor es posen d’acord en les claus que utilitzaràn. Sempre s’utilitzen dues claus diferents (asimetrica).

Autenticació d’entitat: mitjançant el certificat digital es pot conèixer la clau pública del servidor i, d’aquesta manera, el client pot confiramar la seva identitat.

Autenticació del missatge: El missatge s’envia xifrat i, a més, pot incorporar un codi MAC per a comprobar que no ha estat modificat posteriorment.

Per finalitzar, cal dir que el protocol SSL serà substituït per TSL, que és una evolució d’aquest. TSL es crea per a afegir millores de seguretat en conseqüència de les falles detectades i millores en els diferents tipus d’atacs.