Introducción

Al navegar por la Internet, existen ocasiones en cuando es necesario enviar datos de carácter privado o confidencial, los cuales deseamos sean mantenidos en reserva, como por ejemplo información personal o números de tarjetas de crédito y/o cuentas bancarias. Debido a lo delicada que resulta este tipo de información, es deseable que solo sea recibida por el destinatario deseado, de ahí que resulta indispensable identificar y autentificar que el servidor al cual le estamos enviando esta información, para asegurar que primero, es quien dice ser, y segundo la información no será recibida por algún intruso no deseado. Además de esto, también es sumamente necesario que las comunicaciones entre el navegador web del usuario y el servidor web (ya autentificado) viajen protegidas por la red (encriptadas) de modo que resulte imposible entenderlas para algún intruso que pueda hipotéticamente interceptarlas mientras estas viajan por la Internet.

Para poder solucionar esto, actualmente los navegadores web soportan un protocolo conocido como Capa de Socket Seguro (Secure Socket Layer, SSL) el cual ofrece una ayuda para solucionar estas dificultades. El funcionamiento y estas ayudas serán expuestas en las páginas que siguen, luego de lo cual se hablará de OPENSSL, un paquete de código libre disponible en la Internet del protocolo SSL y sus principales características.