TLS

Transport Layer Security (TLS) , ранее известный как Secure Sockets Layer (SSL), — это протокол, используемый приложениями для безопасного взаимодействия в сети, предотвращающий подделку и подслушивание электронной почты, просмотра веб-страниц, обмена сообщениями и других протоколов. И SSL, и TLS представляют собой протоколы клиент/сервер, которые обеспечивают конфиденциальность связи за счет использования криптографических протоколов для обеспечения безопасности в сети. Когда сервер и клиент взаимодействуют с использованием TLS, это гарантирует, что никакая третья сторона не сможет подслушать или подделать какое-либо сообщение.

Все современные браузеры поддерживают протокол TLS, требуя от сервера предоставления действующего цифрового сертификата, подтверждающего его личность, для установления безопасного соединения. И клиент, и сервер могут взаимно аутентифицировать друг друга, если обе стороны предоставляют свои собственные индивидуальные цифровые сертификаты.