SSL and TLS are commonly used by web browsers to protect connections between web applications and web servers. Many other TCP-based protocols use TLS/SSL as well, including email (SMTP/POP3), instant messaging (XMPP), FTP, VoIP, VPN, and others. Typically, when a service uses a secure connection the letter S is appended to the protocol name, for example, HTTP**S**, SMTP**S**, FTP**S**, SIP**S**. In most cases, SSL/TLS implementations are based on the OpenSSL library.

If you visit a website and receive a certificate that is signed by another entity, you might still feel uncertain about website security. You may be worried that the entity that signed the certificate is an impostor. This problem is addressed by the Public Key Infrastructure (PKI). The PKI includes everything that is needed to manage digital certificates and public key encryption.

There are several PKI entities that you can trust. They are called Certificate Authorities (CAs). They verify other entities (companies, organizations, individuals) and confirm that they are indeed who they say they are. Upon such verification, a CA signs the certificate using their own certificate. The certificate of a CA is called the root certificate.

The root certificates of all CAs (and therefore their public keys) are considered trusted. They are installed in all browsers such as Chrome, Firefox, and Edge and in operating systems (including Windows). Popular CAs include IdenTrust, Comodo, DigiCert, GoDaddy, GlobalSign, and Symantec. There are currently more than 200 root certificates that are trusted by browsers.

An SSL/TLS web connection requires a TLS/SSL certificate but that certificate can be signed by anyone. It can even be self-signed (signed by the entity that created the certificate). When visiting a website secured with SSL/TLS, the browser checks if that website has a valid certificate by checking if it is signed by a trusted root certificate. It also checks if the certificate is for the domain that you are visiting and displays information about the certificate owner for you to verify. If the certificate is not signed by a trusted root certificate, the web browser displays a clear warning. You can usually choose to ignore the warning (depending on web browser setup) but you cannot miss it.