**SSL/TLS Operation Technical Blog**

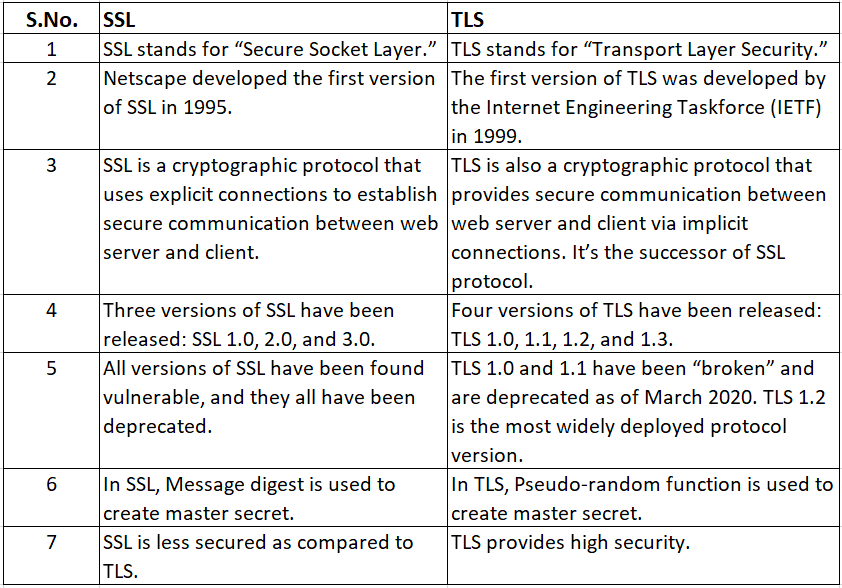
1. **What is SSL?**

SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. The two systems can be a server and a client (for example, a shopping website and browser) or server to server (for example, an application with personally identifiable information or with payroll information).

**2. What is TLS?**

TLS (Transport Layer Security) is just an updated, more secure, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term, but when you are [buying SSL](https://www.websecurity.digicert.com/ssl-certificate?inid=infoctr_buylink_sslhome) from DigiCert you are actually buying the most up to date TLS certificates with the option of [ECC, RSA or DSA encryption](https://www.websecurity.digicert.com/security-topics/how-ssl-works).

**3. Difference between SSL and TSL?**



**4. How SSL works?**

When an Internet user visits a secure web site, an SSL certificate provides Identification information about the web server and establishes an encrypted connection. This process happens in a fraction of a second.

##### **What Happens Between the Web Browser and Server**

* A browser attempts to connect to a web site secured with **SSL**. The browser requests that the web server identify itself.
* The server sends the browser a copy of its **SSL certificate**.
* The browser checks whether it trusts the SSL certificate. If so, it sends a message to the server.
* The server sends back a digitally signed acknowledgement to start an SSL encrypted session.
* Encrypted data is shared between the browser and the server.

##### **SSL Fundamentals**

There are 3 essential elements at work in the process described above: a protocol for communications (SSL), credentials for establishing identity (the SSL certificate), and a third party that vouches for the credentials (the certificate authority).

* Computers use protocols to allow different systems to work together. Web servers and web browsers rely on the **Secure Sockets Layer (SSL) protocol** to enable encrypted communications.
* **Credentials** for establishing identity are common to our everyday lives: a driver’s license, a passport, a company badge. An SSL certificate is a type of digital certificate that serves as a credential in the online world.
* Our trust of a credential depends on our confidence in the organization that issued it. **Certificate authorities** have a variety of methods to verify information provided by individuals or organizations.

At the end of the SSL certificate’s validity period **(1-5 years, depending on the certificate type and your selection)**, you have the option to renew your SSL certificate.

### **5. What is a digital certificate?**

A digital certificate is an electronic document issued by a Certificate Authority (CA). It contains the public key for a digital signature and specifies the identity associated with the key, such as the name of an organization. The certificate is used to confirm that the public key belongs to the specific organization. The CA acts as the guarantor. Digital certificates must be issued by a trusted authority and are only valid for a specified time. They are required in order to create a digital signature.

**6. What is open SSL.**

Open SSL is an all-around cryptography library that offers open-source application of the TLS protocol. First released in 1998, it is available for Linux, Windows, macOS, and BSD systems. OpenSSL allows users to perform various SSL related tasks, including CSR (Certificate Signing Request) and private keys generation and SSL certificate installation.

**7. Chain of trust.**

The Chain of Trust refers to your SSL certificate and how it is linked back to a trusted **Certificate Authority**. In order for an SSL certificate to be trusted it has to be traceable back to the trust root it was signed off of, meaning all certificates in the chain – server, intermediate, and root, need to be properly trusted. There are 3 parts to the chain of trust:

**Root Certificate** – A root certificate is a digital certificate that belongs to the issuing Certificate Authority. It comes pre-downloaded in most browsers and is stored in what is called a “trust store.” The root certificates are closely guarded by the Certificate Authorities.

**Intermediate Certificate** – Intermediate certificates branch off of root certificates like branches off of trees. They act as middle-men between the protected root certificates and the server certificates issued out to the public. There will always be at least one intermediate certificate in a chain, but there can be more than one.

**Server Certificate** – The server certificate is the one issued to the specific domain the user needs coverage.

**8. What is TLS?**

When browsing the internet, users and web applications regularly encounter multiple possible security problems. These include authenticating the identity of the other party, data tampering, and third-party monitoring. TLS uses cryptographic techniques to authenticate the client or server in a connection, help ensure the integrity of the data being transferred, and provide protection throughout the browsing session.

Users typically recognize TLS from secure web browsing, in which online transactions are protected from hackers and eavesdroppers. Secure browsing sessions are indicated by the padlock icon at the top left corner of the web browser. TLS is also used in applications such as email, file transfers, video and audio conferencing. TLS is also compatible with a significant number of protocols including HTTP, SMTP, FTP, XMPP, and many more. Users should note that TLS isn’t designed to secure data on end systems, only data transferred over the internet.