**What is SSL, What is One-Way SSL & Two-Way SSL?**

**What is SSL?**

* SSL stands for “Secure Sockets Layer”.
* SSL has been developed by Netscape.
* The first released version 2.0 was declared in 1995.
* It is Security technology used to encrypt the data between clients and server or website on browser, mails, etc.

**What is TLS?**

* TLS stands for “Transport Layer Security” protocol.
* Later the SSL v3.0 has been replaced by TLS1.0
* The TLS1.0, TLS1.1, TLS 1.2 is available, the TLS 1.3 is the newer version protocol released in 2018.

**SSL works on “three basic principles”:**

* **A.       Encryption.**
* **B.       Authentication.**
* **C.       Data Integrity.**

**A) Encryption**: The data which is transferred between two or more Clients and Server should be encrypted. Since the attacker or hacker would unable to understand.

**B) Authentication**: The data to be transferred must be to the correct person or user.

**C)** **Data Integrity**: The data over transmission should not be tampered or changed.

**SSL works on  “a key pair”:**

**a)       Public Key.**

**b)       Private Key.**

**a) Public Key:**

* As the name says public, means it is available to all people.
* A public key is basically used for Authentication purpose (The Right Person/User).
* A CSR (Certificate Signing Request) contains the user detail which is encrypted using the public key.

**b) Private Key:**

* As the name says Private, means it is kept secret only available to the owner.
* This key is having both functionalities of encrypting and decrypting the data during transmission.
* The private key is generated while creating CSR in an encrypted format.

**Public key infrastructure (PKI) produces public and private keys.**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**SSL (Secure Sockets Layer) HANDSHAKE :**  
  
**Basically, the browser works on One-Way SSL authentication mechanism, Where the Client verifies/validates the server certificate with the list of CA's certification authority.**  
**There are three keys are used to set up the SSL connection: (a)the public, (b) private, and (c) session keys.**

**The SSL connection can be made in two different ways:**  
 **A) One-Way SSL: In this method only client going to verifies, server certificates with the List of CA's certification authority.**  
 **B) Two-Way SSL:** **In this method, both client and server verify, each other certificates with the list of CA's certification authority.**

**A) One-Way SSL authentication:**

1. Client requests for data on HTTPS protocol to the server. That going to initiates the SSL/TLS handshake process.

2. Server returns with its public certificate and public key to the client along with the server hello message.

3. The client validates/verifies the received server certificates with CA’s certification authority including certificate expiration, unrevoked and Common Name (CN – name).

4. The client sends back with a symmetric session key using the server’s public key.

5. The server decrypts the symmetric session key using its private key and sends back an encrypted session key to start the encrypted session.