Secure Socket Layer (SSL)

· SSL was originated by Netscape. It has been designed to provide **encryption and authentication** among web clients and servers.

· Widely used in the electronic commerce being implemented in the majority of web browsers and servers. It provides the following functions:

-Server authentication. It allows a user to confirm the server identiy.

-Client authentication. It allows a server to confirm the user identity.

- SSl session encrypted. All the information sent from the client and the server are encrypted by the sending software (browser or server)and decrypted by the receiving software (browser o server)

Handsake protocol

· The protocol allows the server and the client to authenticate each other and to negotiate an encryption and hash algorithm and criyptographic keys to be used to protect data sent in a SSL record.

·The handsake protocol is used before any application data is transmitted.

1.The client sends the highest SSL version and its preference for the kind of symmetric key algorithm to be used.

2.The server sends to the client the number of its SSL version, its preferences for the kind of symmetric key algorithm and **its digital certificate.**
The certificate contains the RSA public key of the server and it is signed with the private key of a CA.

3.The client knows the public key of some CA. It controls if the server CA is present in its list. In the positive case the client uses the CA public key in order to decrypt the certificate and obtain the server public key. (server authentication)

4. The client creates a session symmetric key, encrypts it with the server public key and sends it to the server.

5. The client sends a message to the server to comunicate that the following messages will be encrypted with the session key. Then, sends an encrypted message to indicate the conclusion of the client handsake.

6. The server sends a message to the browser to comunicate that the following messages will be encrypted with the session key. Then, sends an encrypted message to indicate the conclusion of the server handsake.

7. Client and server utilize the session key to encrypt and decrypt the sent messages and to validate their integrity.