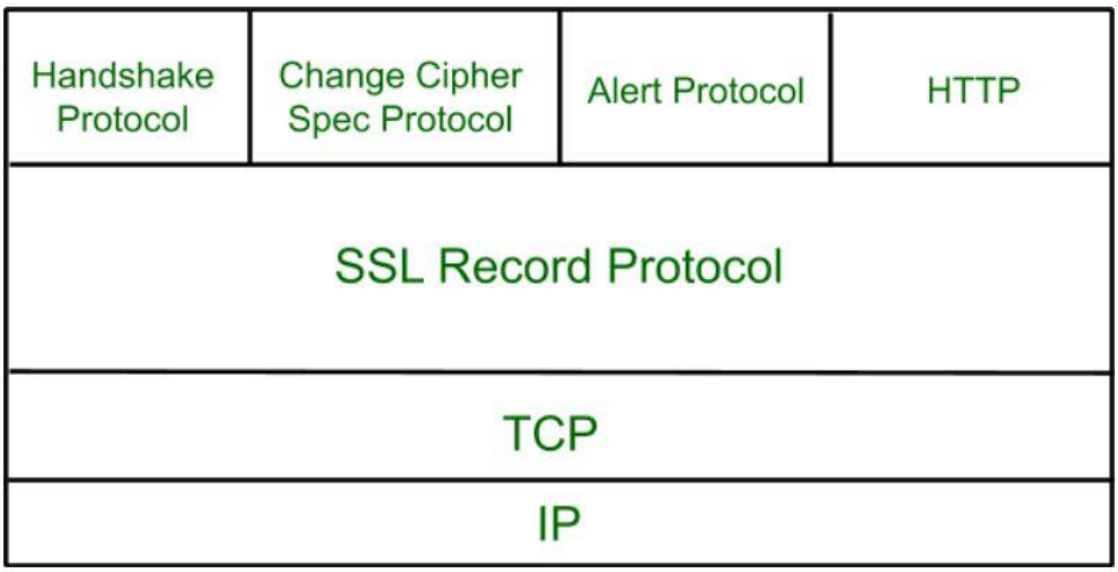
Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Protocol Stack:

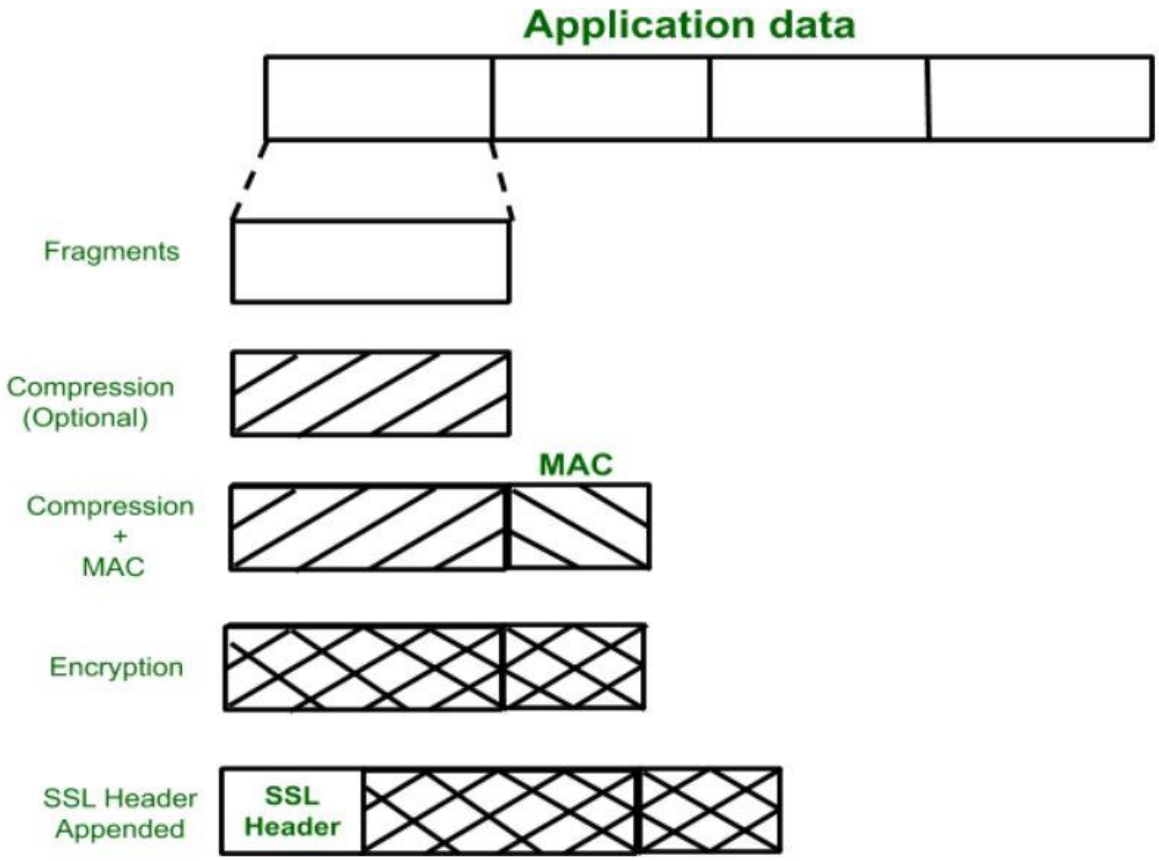


SSL Record Protocol:

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

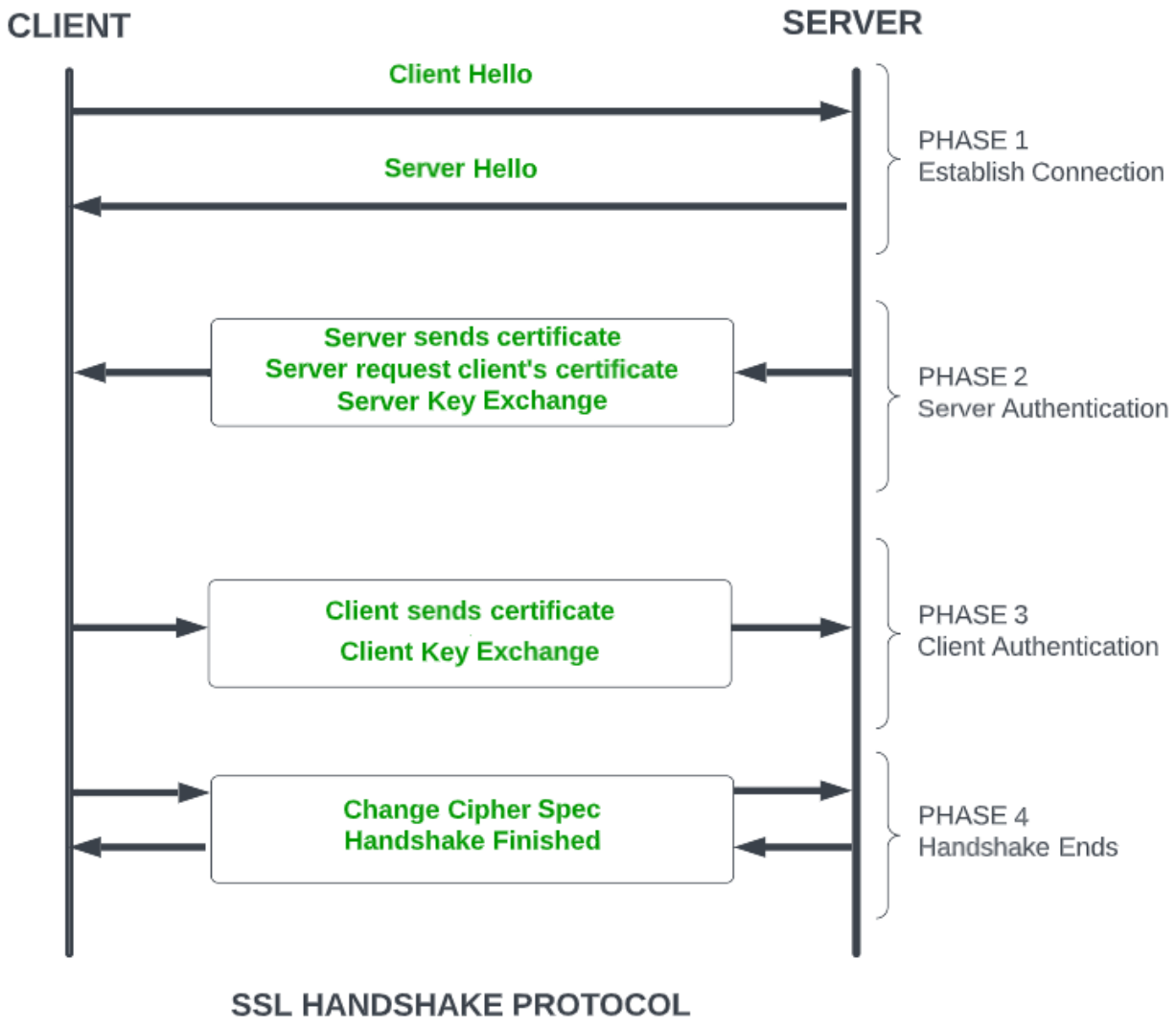
In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



Handshake Protocol:

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.



SSL Handshake Protocol Phases diagrammatic representation

Change-cipher Protocol:

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state. Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol:

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.

The level is further classified into two parts:

Warning (level = 1):
This Alert has no impact on the connection between sender and receiver. Some of them are:

- **Bad certificate:** When the received certificate is corrupt.
- **No certificate:** When an appropriate certificate is not available.
- **Certificate expired:** When a certificate has expired.
- **Certificate unknown:** When some other unspecified issue arose in processing the certificate, rendering it unacceptable.
- **Close notify**: It notifies that the sender will no longer send any messages in the connection.

Fatal Error (level = 2):
This Alert breaks the connection between sender and receiver. The connection will be stopped, cannot be resumed but can be restarted. Some of them are:

- **Handshake failure:** When the sender is unable to negotiate an acceptable set of security parameters given the options available.
- **Decompression failure**: When the decompression function receives improper input.
- **Illegal parameters:** When a field is out of range or inconsistent with other fields.
- **Bad record MAC:** When an incorrect MAC was received.
- **Unexpected message:** When an inappropriate message is received. The second byte in the Alert protocol describes the error.

Salient Features of Secure Socket Layer:

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.

- This is a two-layered protocol.

Versions of SSL:

SSL 1 – Never released due to high insecurity.
SSL 2 – Released in 1995.
SSL 3 – Released in 1996.
TLS 1.0 – Released in 1999.
TLS 1.1 – Released in 2006.
TLS 1.2 – Released in 2008.
TLS 1.3 – Released in 2018.