



SLIIT

Discover Your Future



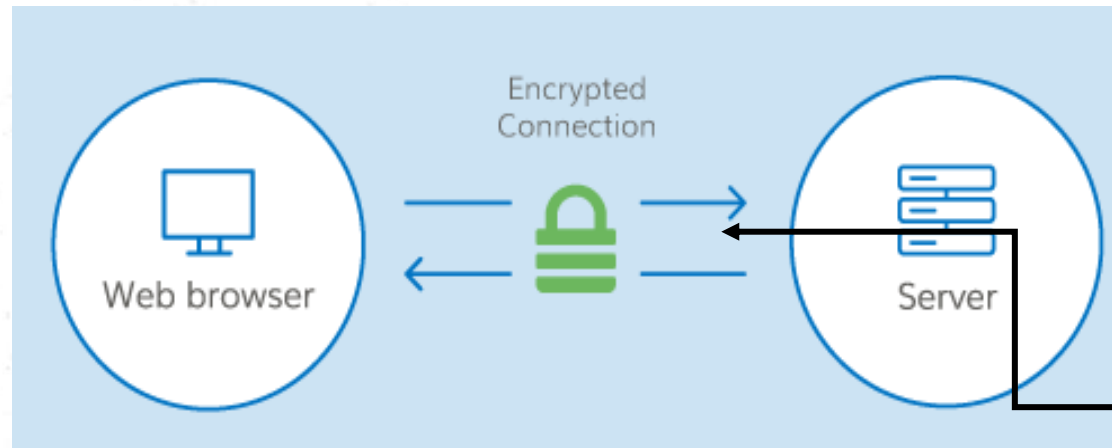
IE2062 – Web Security

Lecture 5 – Secure Socket Layer (SSL / TLS)



Concern of the SSL Certificate

- One of the most important components of online business is creating a trusted environment where potential customers feel confident in making purchases.
- SSL certificates create a foundation of trust by establishing a secure connection.




This link ensures that all data passed between the web server and browsers remain private and integral.

Concern of the SSL Certificate ctd..

- Secure Sockets Layer (SSL) certificates, sometimes called digital certificates, are used to establish an encrypted connection between a browser or user's computer and a server or website.
- The SSL connection protects sensitive data, such as credit card information, exchanged during each visit, which is called a session, from being intercepted from non-authorized parties.


Concern of the SSL Certificate ctd..

- More specifically, SSL is a security protocol. Protocols describe how algorithms should be used.
- In this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.
- All browsers have the capability to interact with secured web servers using the SSL protocol.
- However, the browser and the server need what is called an SSL Certificate to be able to establish a secure connection.

- 
- Internet users have come to associate their online security with the lock icon that comes with an SSL-secured website or green address bar that comes with an Extended Validation SSL-secured website.



• An Overview of One-Way SSL and Two-Way SSL


- **SSL (Secure Socket Layer)** is the standard technology used for enabling secure communication between a client and sever to ensure data security & integrity.
- SSL has evolved with time and several versions have been introduced to deal with any potential vulnerabilities.
- SSL V2 released in 1995 was the first public version of SSL followed by SSL V3 in 1996 followed by TLS V1.0 in 1999, TLS V1.1 in 2006 and TLS V1.2 in 2008.

- 
- TLS is the successor of SSL although is sometimes still referred to as SSL.
 - TLS has been evolving as time passes to keep up with more complex security requirements, to fix cryptographic flaws, etc.
 - For ensuring security of the data being transferred between a client and server, SSL can be implemented either one-way or two-way.

How One-Way SSL Works?

- In one way SSL, only client validates the server to ensure that it receives data from the intended server.
- For implementing one-way SSL, server shares its public certificate with the clients.
- Below is the high level description of the steps involved in establishment of connection and transfer of data between a client and server in case of one-way SSL.

- 
- 
1. Client requests for some protected data from the server on HTTPS protocol.
 2. This initiates SSL/TLS handshake process.
 3. Server returns its public certificate to the client along with server hello message.
 4. Client validates/verifies the received certificate. Client verifies the certificate through certification authority (CA) for CA signed certificates.

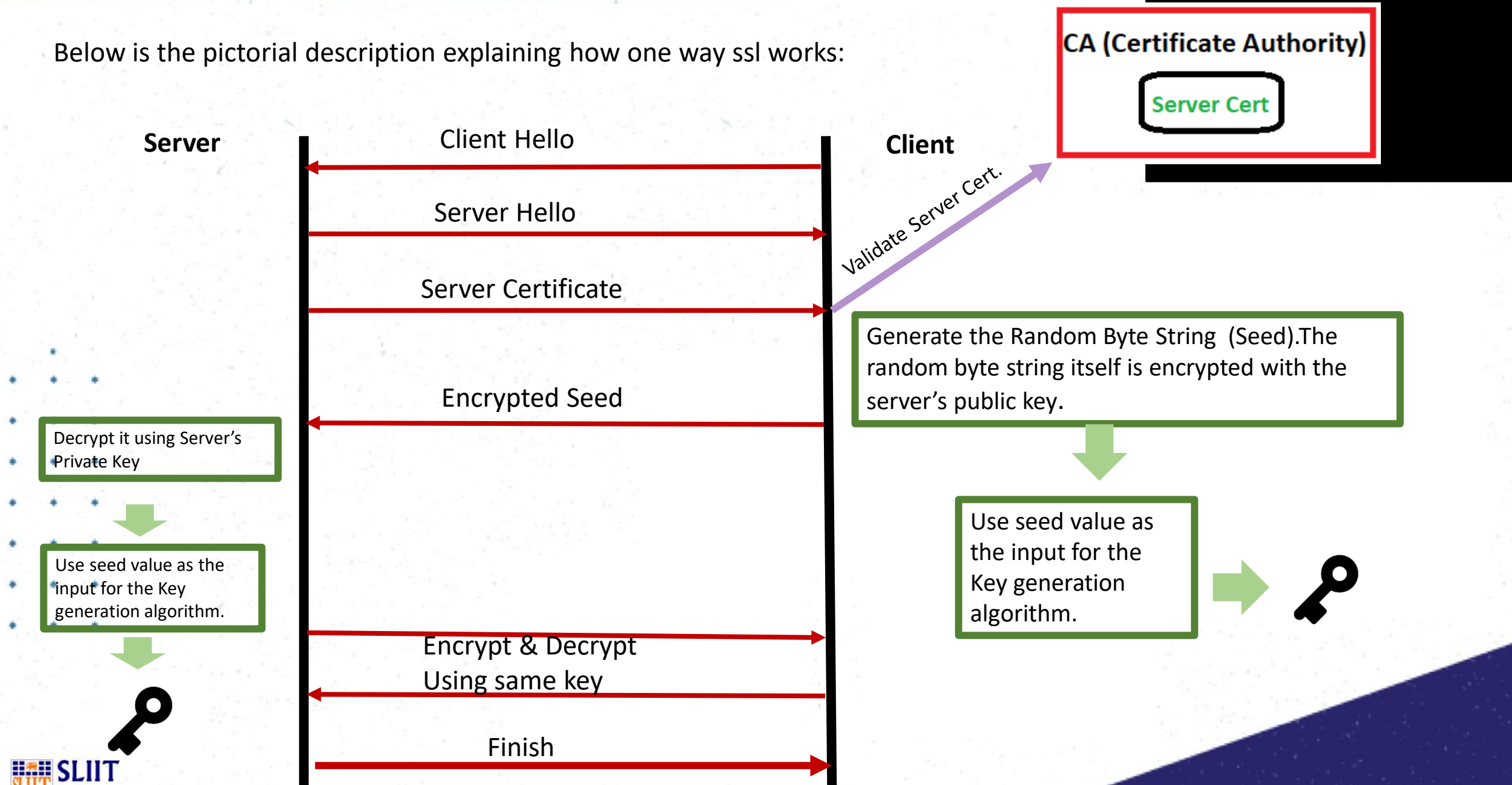


SSL/TLS client sends the random byte string that enables both the client and the server to compute the secret key to be used for encrypting subsequent message data.

The random byte string itself is encrypted with the server's public key.

After agreeing on this secret key, client and server communicate further for actual data transfer by encrypting/decrypting data using this key.

Below is the pictorial description explaining how one way ssl works:

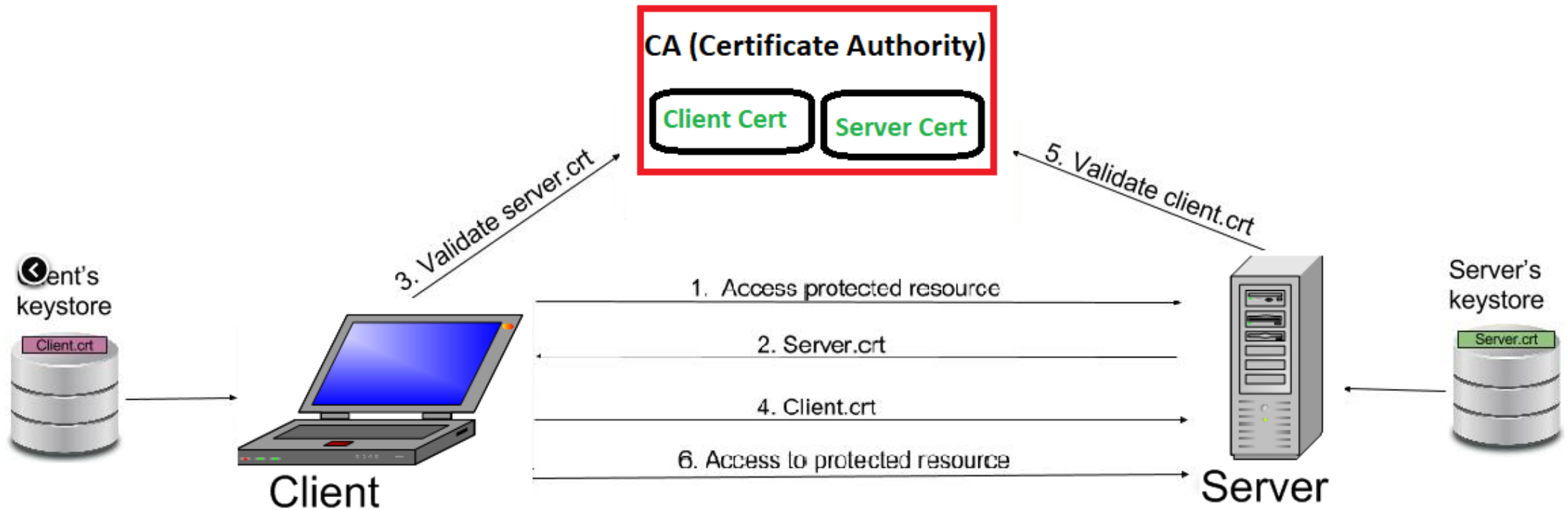


How Two-Way (Mutual) SSL works?

- Contrary to one-way SSL; in case of two-way SSL, both client and server authenticate each other to ensure that both parties involved in the communication are trusted.
- Both parties share their public certificates to each other and then verification/validation is performed based on that.

• Below is the high level description of the steps involved in establishing connection and transfer of data between a client and server in case of two-way SSL:

1. Client requests a protected resource over HTTPS protocol and the SSL/TLS handshake process begins.
2. Server returns its public certificate to the client along with server hello.
3. Client validates/verifies the received certificate. Client verifies the certificate through certification authority (CA) for CA signed certificates.
4. If Server certificate was validated successfully, client will provide its public certificate to the server.
5. Server validates/verifies the received certificate. Server verifies the certificate through certification authority (CA) for CA signed certificates.
6. After completion of handshake process, client and server communicate and transfer data with each other encrypted with the secret keys shared between the two during handshake.



Obtaining a Digital Certificate

- You get a digital certificate from a recognized Certificate authority (CA). Just like you get a passport from a passport office.
- In fact the procedure is very similar.
- You fill out the appropriate forms add your public keys (they are just numbers) and send it/them to the certificate authority. (this is a certificate Signing Request)

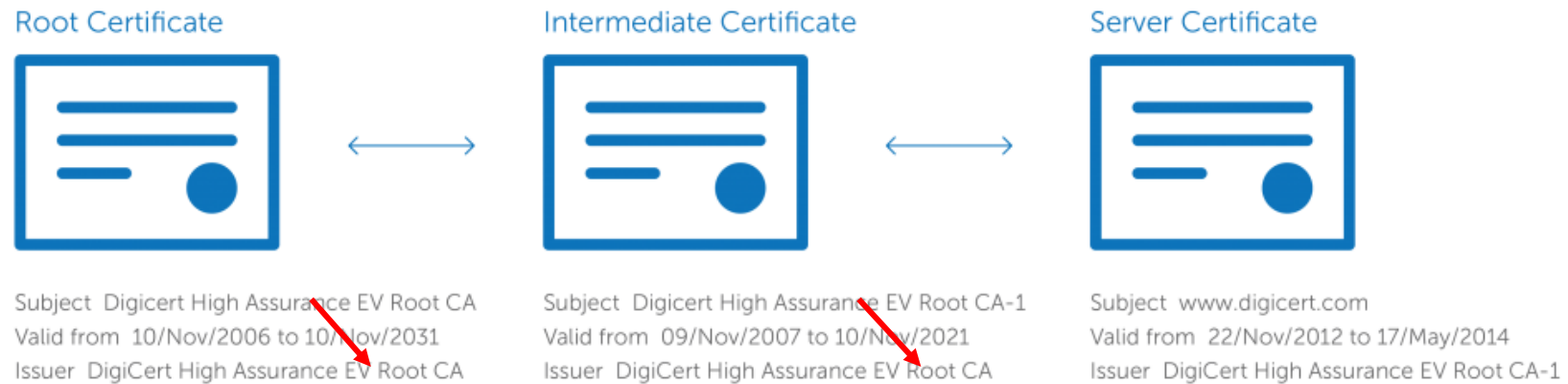


Obtaining a Digital Certificate ctd..

- The certificate authority does some checks (depends on authority), and sends you back the keys enclosed in a certificate.
- The certificate is signed by the Issuing Certificate authority, and this is what guarantees the keys.
- Now when someone wants your public keys, you send them the certificate, they verify the signature on the certificate, and if it verifies, then they can trust your keys

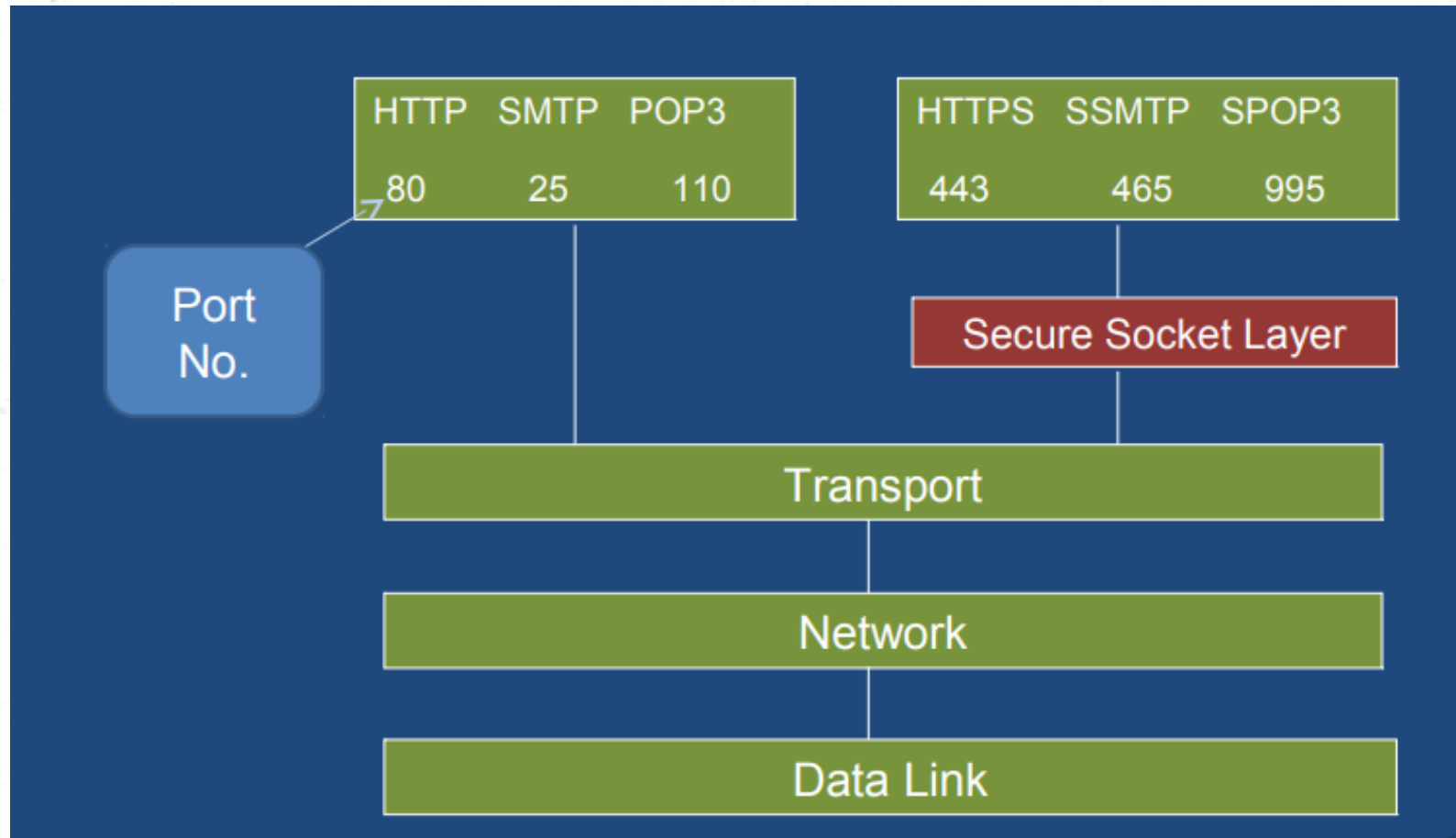
The Certificate Chain

It connects your server certificate to your CA's (in this case DigiCert's) root certificate through an intermediate certificate.

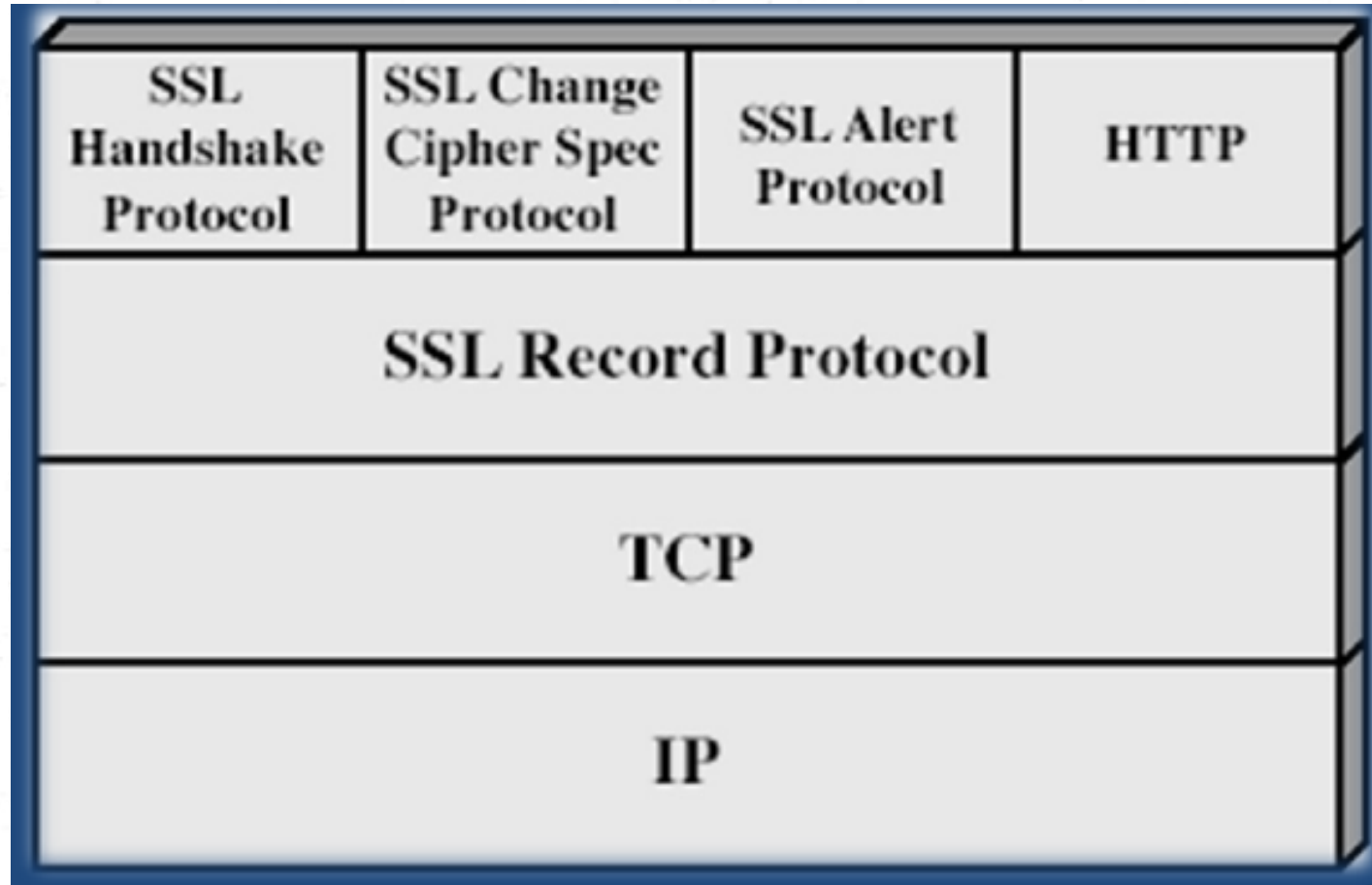


- The most important part of an SSL certificate is that it is digitally signed by a trusted CA, like DigiCert.
- Anyone can create a certificate, but browsers only trust certificates that come from an organization on their list of trusted CAs.
- Browsers come with a pre-installed list of trusted CAs, known as the Trusted Root CA store.
- In order to be added to the Trusted Root CA store and thus become a Certificate Authority, a company must comply with and be audited against security and authentication standards established by the browsers.

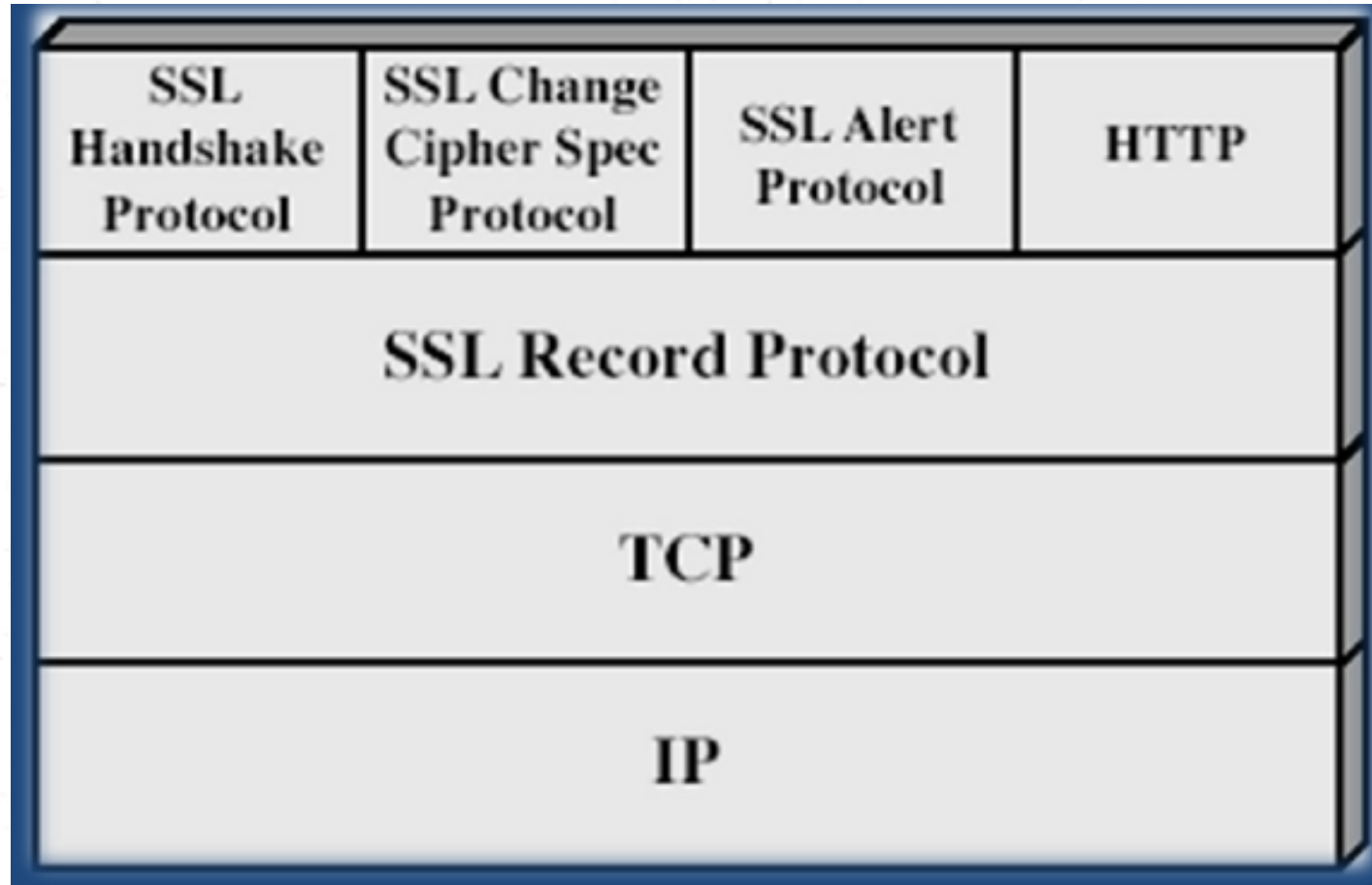
Where SSL Fits ??



SSL Architecture



SSL Architecture



Functions of SSL Protocol Components

The four sub-components of the SSL protocol handle various tasks for secure communication between the client machine and the server.

Record Protocol

- The record layer formats the upper layer protocol messages.

- It fragments the data into manageable blocks (max length 16 KB). It optionally compresses the data.

- Encrypts the data.

- Provides a header for each message and a hash (Message Authentication Code (MAC)) at the end.

Hands over the formatted blocks to TCP layer for transmission.

SSL Handshake Protocol

It is the most complex part of SSL.

It is invoked before any application data is transmitted.

It creates SSL sessions between the client and the server.

- Establishment of session involves Server authentication, Key and algorithm negotiation, Establishing keys and Client authentication (optional).

- A session is identified by unique set of cryptographic security parameters.

- Multiple secure TCP connections between a client and a server can share the same session.

Handshake protocol actions through four phases. These are discussed in the next section.

ChangeCipherSpec Protocol

Simplest part of SSL protocol. It comprises of a single message exchanged between two communicating entities, the client and the server.

- As each entity sends the ChangeCipherSpec message, it changes its side of the connection into the secure state as agreed upon.
- The cipher parameters pending state is copied into the current state.
- Exchange of this Message indicates all future data exchanges are encrypted and integrity is protected.

SSL Alert Protocol

This protocol is used to report errors – such as unexpected message, bad record MAC, security parameters negotiation failed, etc.

It is also used for other purposes – such as notify closure of the TCP connection, notify receipt of bad or unknown certificate, etc.

Working of HTTPS

HTTPS application protocol typically uses one of two popular transport layer security protocols - SSL or TLS. The process of secure browsing is described in the following points.

- You request a HTTPS connection to a webpage by entering https:// followed by URL in the browser address bar.

- Web browser initiates a connection to the web server. Use of https invokes the use of SSL protocol.

- An application, browser in this case, uses the system port 443 instead of port 80 (used in case of http).

Working of HTTPS ctd..

The SSL protocol goes through a handshake protocol for establishing a secure session as discussed in earlier sections.

- The website initially sends its SSL Digital certificate to your browser. On verification of certificate, the SSL handshake progresses to exchange the shared secrets for the session.

- When a trusted SSL Digital Certificate is used by the server, users get to see a padlock icon in the browser address bar. When an Extended Validation Certificate is installed on a website, the address bar turns green.

- Once established, this session consists of many secure connections between the web server and the browser.



The END