# Secured Socket Layer

* The secured socket layer technology comprises the
  - secured sockets layer (SSL)
  - transport layer security (TLS)

These protocols provide authentication and encryption to secure transactions

* SSL and TLS are included in transaction methods to secure transactions, using encryption.

* SSL was created by the Netscape corporation, while TLS was created by the IETF network working group, using the SSL 3.0 specification
TLS is an open standard that is updated frequently.

* SSL and TLS are commonly used in browsers. They can be used to secure various types of network traffic, such as email, FTP or NNTP. SSL and TLS also can secure e-commerce transactions from custom created applications.
Additionally they can secure B2B and B2C transactions.

SSL and TLS offer services, such as authentication, data confidentiality and data integrity.

* PKI

Before using SSL and TLS to enable encryption, an organization needs a certificate. Therefore, an organization should participate in a Public Key Infrastructure (PKI)

A PKI is a collection of individuals, networks and computers that can authoritatively verify the identity of a person, host or organization.

ENCRYPTION begins once PKI establishes trust between two unknown parties

PKI comprises several elements

A Digital certificate.
B CA (certificate authority)
C RA (registration authority)
D Certificate server
E certification chain
F Entity

A **Digital certificate**

This is a signed publickey that checks a set of credentials connected with the public key of the CA
All SSL and TLS sessions need a valid certificate.
This certificate acts as a trusted third party, and enables unknown parties to authenticate with each other and begin encryption

B **CA**

a CA is a trusted third party that checks the identity of the person or company that has presented a certification request.
A CA is an organization that issues digital certificates, and validates the identity of a person, host or process

C **RA**

An RA is part of the CA. The RA is used if the CA is overburdened with various requests The RA only checks credentials, and the task of issuing certificates is performed only by the CA

D **Certificate server**

A certificate server is placed within the CA. This server is the computer that generates certificates. It is also referred to as an authentication service

certification chain

This defines the nature of trust in a PKI infrastructure. The CA establishes trust by establishing itself as as trustworthy authority that validates identity. The CA exists at the top of a tree hierarchy and creates a trust pattern

by vouching for each entity under it. A certificate ceases to be valid if its links to the CA is not trustworthy

F **Entity**

An Entity is a host that uses a certificate. A host that requests a certificate is also known as an entity

* **X.509**

Digital certificates used in PKI adhere to the International telecommunications union (ITU) X.509 standard.
The CA creates the X.509 certificate. Each time this certificate is used to secure a service, a different port is used.
For example, SSL and TLS enabled web traffic use TCP port 443 instead of port 80, the default ports

* Public Key Cryptography standards (PKCS) defines 15 methods for securely requesting transferring, and storing certificates.
PKCS * 1 Known as the Rivest Shamir Adleman (RSA) Cryptography standard, defines the use of the RSA algorithm and the format for RSA private and public keys.

* PKCS #6, known as the extended-certificate syntax standard, provides extensions to the X.509 standard.
PKCS #7, known as the cryptographic message syntax standard, is used for secure Multipurpose Internet Mail Extensions or Privacy enhanced Mail (PEM). It is used by end users to export public keys for encrypting e-mail sent to each other.

* PKCS #7 is also used to publish a Certificate Revocation List (CRL), or a Certification chain
PKCS #10, called the certification request syntax standard, defines the format for a certificate request.
The resulting file is formatted according to this standard.
PKCS #12, known as the personal information exchange syntax standard, defines the user based storage of private keys and certificates.

* All certificates generated through PKI have a specific life span. There are certain terms involved in the life cycle

- Certificate Policy refers to the guidelines for using digital certificates
- A Certificate Practice statement (CPS) is a document that describes the manner in which a CA verifies and manages certificates

* Certificate expiration refers to the invalidation of a certificate when it reaches its end date.
Certificate revocation occurs when a certificate ceases to be valid before its end date. Keys that have been revoked cannot be renewed. Reasons for revocation include termination or reassignment of an employee, renaming of a company or of a DNS server, or of a compromised CA.

* Certificate suspension is the temporary invalidation of a key for a certain time interval. The key can be reactivated. However, if the certificate expires during a period of suspension, a new key must be generated.
Certificate renewal refers to the revalidation of a key before it expires.
Keys that have been revoked or have already expired cannot be renewed.

* certificate destruction refers to the deletion of all public and private keys, resulting in the elimination of an identity from PKI
A CRL is a list of certificates that are no longer valid. Users need to manually download and check this list
Online Certificate Status protocol (OCSP) is a real time protocol that enables users to check for revoked certificates.

* Once a client and server are SSL enabled, they need to negotiate a connection by using an SSL or TLS handshake. This handshake negotiates which encryption algorithm, RSA or Digital Signature Algorithm (DSA) should be used.
The handshake also requires the server to always authenticate with a client using a certificate. The client can be forced to authenticate with the server.

* In the SSL and TLS handshake, the session key, which is a symmetric key shared between the client and the server, is also negotiated.
The session key is protected by asymmetric key encryption.
Specifically, the session key is protected by the client's public key.

* Encryption occurs after authentication, which is enabled by certificates AN SSL and TLS session can take place in a browser, as it contains public keys of several known CAs.
As most Web servers have certificates signed by the CAs, the session starts automatically.
However, a discrepancy can occur because of an attempted attack or improper server configuration.

* There are several common discrepancies that can result in a warning or a failed session. For Example, if the host name on the certificate is different from the name on the server, the web browser issues a warning. The user can then choose to continue the session or end it.
The problem occurs mainly due to a change in the server configuration or by hacker activity on the users connection.

* A WARNING is issued when the certificate presented by the server needs to be renewed, or the server is using a certificate that is not yet validated.
The session cannot continue when the certificate contains a fatal flaw that results in an invalid format.

* If a recognized CA does not sign the certificate the user receives a warning. The user can then cancel the session, accept the certificate for the current session, or install the certificate permanently.
The session may not continue if the browser cannot handle the encryption level required by the server. In this case, the user should upgrade the encryption level of the browser.