Transport Layer Security

The TLS (Transport Layer Security) handshake is the process by which a secure connection is established between a web browser and a web server. During this handshake, the browser and server authenticate each other, negotiate encryption algorithms, and establish a shared session key for secure communication.

The handshake typically follows these steps:

1. Client Hello: The browser sends a Client Hello message to the server, indicating its supported TLS versions, encryption algorithms, and other parameters.
2. Server Hello: The server responds with a Server Hello message, selecting the highest TLS version and encryption algorithm supported by both the client and server. It also sends its digital certificate, which contains its public key.
3. PKI Verification: The browser verifies the server's digital certificate using the Public Key Infrastructure (PKI). PKI is a system of trusted authorities that issue and manage digital certificates. The browser checks if the certificate is valid, trusted, and not expired. It verifies the certificate's digital signature using the public key of the certificate authority (CA) that issued the certificate. If the verification fails, the browser displays a warning.
4. Key Exchange: The browser generates a random session key (also known as the pre-master secret) and encrypts it using the server's public key obtained from the certificate. It sends this encrypted pre-master secret to the server.
5. Session Key Derivation: Both the browser and server independently derive the session key from the pre-master secret. This ensures that only the client and server possess the same session key without explicitly transmitting it over the network.

6. Server Authentication: The server decrypts the pre-master secret using its private key. It uses the pre-master secret, along with other random values exchanged during the handshake, to compute a shared session key.
7. Symmetric Encryption: From this point onward, the client and server switch to symmetric encryption, which is faster than asymmetric encryption used for key exchange. They use the shared session key to encrypt and decrypt the data exchanged during the secure session.
8. Completion: Both the client and server send messages to confirm that the handshake is complete. They indicate their readiness to start securely transmitting application data.

Throughout the TLS handshake, the PKI plays a crucial role. The server's digital certificate, signed by a trusted CA, is used to authenticate the server's identity. The browser verifies the certificate's authenticity using the CA's public key. This ensures that the browser is communicating with the genuine server and not an impostor. The use of asymmetric encryption during the handshake provides secure key exchange, while symmetric encryption using the session key ensures efficient and secure communication for the rest of the session.

Step 3 in detail: PKI Verification and Certificate Validation Certificate Authority (CA): A Certificate Authority is a trusted entity that issues and manages digital certificates. CAs are responsible for verifying the identity of individuals, organizations, or servers and issuing digital certificates that bind public keys to these identities.

Digital Certificate: A digital certificate is an electronic document that contains information about the identity of an entity (such as a web server) and its corresponding public key. It is signed by the CA to ensure its authenticity.

The certificate includes the following components:

a. Subject: The entity's name and other identifying information.
b. Public Key: The entity's public key used for encryption and verifying digital signatures. Certificate Expiration Date: The date when the certificate is no longer considered valid. Issuer: The CA that issued the certificate.
c. Digital Signature: A cryptographic signature generated by the CA using its private key, which guarantees the authenticity and integrity of the certificate.
d. Trust Anchors: Trust anchors are the root certificates of trusted CAs that are pre-installed or manually added to the client's trust store. These trust anchors serve as the starting point of trust in the PKI hierarchy. Browsers and operating systems have a list of trusted CAs and their root certificates.
e. Certificate Chain: A certificate chain is a sequence of certificates that link the server's certificate to a trusted root certificate. The chain establishes a trust path from the server's certificate to a trust anchor. The server's certificate is usually signed by an intermediate CA, which, in turn, is signed by a root CA.
f. Server Certificate: The certificate provided by the server during the TLS handshake.
g. Intermediate Certificates: Additional certificates that form the chain between the server certificate and the root certificate.
h. Root Certificate: The trusted CA's certificate that is included in the client's trust store.

Now, let's dive into the PKI verification process during the TLS handshake:

- Client Hello: The browser initiates the handshake by sending a Client Hello message to the server. The message contains information about the supported TLS versions, encryption algorithms, and other parameters.

- Server Hello: The server responds with a Server Hello message. In addition to selecting the TLS version and encryption algorithm, the server sends its digital certificate to the client.

Certificate Validation: The client begins the PKI verification process by performing the following steps:

1. Extract Server's Public Key: The client extracts the server's public key from the received digital certificate.
2. Verify Certificate Signature: The client verifies the signature of the server's certificate to ensure its authenticity. It uses the public key of the CA that issued the certificate (the intermediate CA) for this verification. The client checks the CA's digital signature on the certificate using the CA's public key, obtained from its own trust store.
3. Certificate Chain Validation: The client verifies the certificate chain starting from the server's certificate and going up to a trusted root certificate. It checks the signatures of each certificate in the chain until it reaches a trusted root certificate.
4. Intermediate Certificates: The client verifies the signature of each intermediate certificate in the chain using the public key of the next certificate in the chain.
5. Root Certificate: Finally, the client checks if the root certificate is present in its trust store and whether it is valid and not expired. If the root certificate is trusted and the entire chain is successfully validated, the server's certificate is considered authentic.
6. Certificate Revocation Check: The client may also perform a revocation check to ensure that the server's certificate has not been revoked by the issuing CA. This involves verifying the certificate's revocation status against Certificate

Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) responses.

7. Trust Decision: After the validation process, the client makes a trust decision based on the results. If the server's certificate is trusted and valid, the handshake proceeds. If the certificate fails validation or the trust chain cannot be established, the client displays a warning or terminates the connection.

By verifying the server's digital certificate using the PKI, the client can ensure that it is communicating with a legitimate and trusted server, establishing a secure and authenticated connection for the subsequent steps of the TLS handshake.