How an SSL connection is established

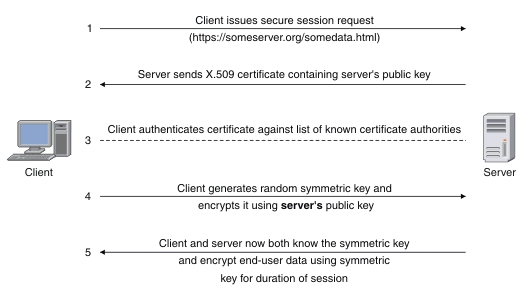
Last Updated: 2022-11-02

An SSL connection is established though a handshake (a series of communications exchanges) between the client and the server.

SSL handshake

The following diagram shows what happens during an SSL handshake:

Figure 1. SSL handshake



1. The client sends a request to the server for a secure session. The server responds by sending its X.509 digital certificate to the client.
2. The client receives the server's X.509 digital certificate.
3. The client authenticates the server, using a list of known certificate authorities.
4. The client generates a random symmetric key and encrypts it using server's public key.
5. The client and server now both know the symmetric key and can use the SSL encryption process to encrypt and decrypt the information contained in the client request and the server response.

CICS® Transaction Gateway supports the JSSE implementation of SSL. JSSE as supplied with the Java SDK is the only supported option. For more information, see [Security](https://www.ibm.com/docs/en/SSZHJ2_9.3.0/securing/topics/secure.html#secure).

Authentication

During server authentication, a connection is only established if the client trusts the server based on the information presented by the server to the client in its certificate.

During client authentication (if activated) the client sends its certificate information to the server. A connection is then only established if the client trusts the server *and* the server trusts the client, based on the information exchanged in both certificates.

* [**Transport Layer Security (TLS)**](https://www.ibm.com/docs/en/SSZHJ2_9.3.0/securing/topics/transportlayersecurity.html)  
  Network connections between a JEE client and CICS can be secured by the Secure Sockets Layer (SSL) protocol, or the Transport Layer Security (TLS) protocol.
* [**Encryption**](https://www.ibm.com/docs/en/SSZHJ2_9.3.0/securing/topics/ov2wnt.html)  
  Cryptography is the scientific discipline for the study and development of ciphers, in particular, encryption and decryption algorithms. These cryptographic procedures are the essential components that enable secure communication to take place across networks that are not secure. SSL encryption uses both symmetric and asymmetric keys.
* [**Digital signatures, certificates and key rings**](https://www.ibm.com/docs/en/SSZHJ2_9.3.0/securing/topics/ov2tsr.html)  
  SSL uses digital signatures and digital certificates for establishing a trusted relationship between a sender and a receiver of information sent over a network connection.
* [**Cipher suites**](https://www.ibm.com/docs/en/SSZHJ2_9.3.0/securing/topics/ssl_cipher.html)  
  A cipher suite is a set of ciphers (encryption algorithms) used for encrypting sensitive information. SSL uses cipher suites to ensure security and integrity of information transmitted over a network connection. Different cipher suites provide different levels of encryption.