



Legend



Public Key of Server



Private Key of Server



CA Signature



Private Shared Key



Data Encrypted with a private key



Unencrypted data

SSL Operation

This outlines the order of operations when a client connects to a secure website using SSL through HTTPS

