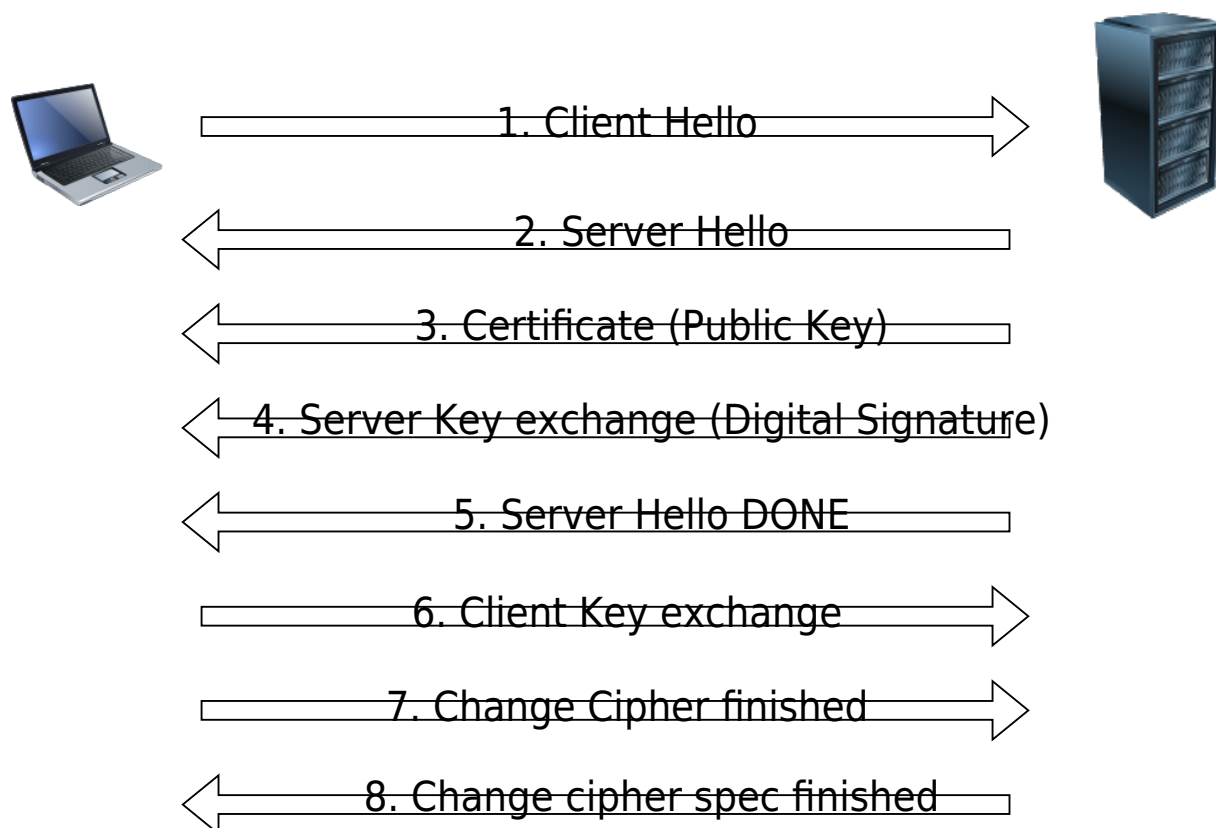


Security: Schemat działania TLS 1.2

TLS 1.2 handshake



Shared Secret (e.g. Elliptic Curve Diffie-Hellman Ephemeral - ECDHE)

Server Authenticity (e.g. Rivest-Shamir-Adleman - RSA)

Mechanism to make sure nobody tampered with the message

From:

<https://wiki.ostrowski.net.pl/> - Kacper's Wiki

Permanent link:

https://wiki.ostrowski.net.pl/doku.php?id=notatki:tls_1.2_explained&rev=1747835996

Last update: **2025/05/21 15:59**