

Klient

Server

TCP SYN

TCP SYN, ACK

TCP ACK

TCP Handshake

ClientHello

ServerHello
Certificate*

ServerKeyExchange*
CertificateRequest*
ServerHelloDone

TLS Handshake

Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished

[ChangeCipherSpec]
Finished

Čas

Čas