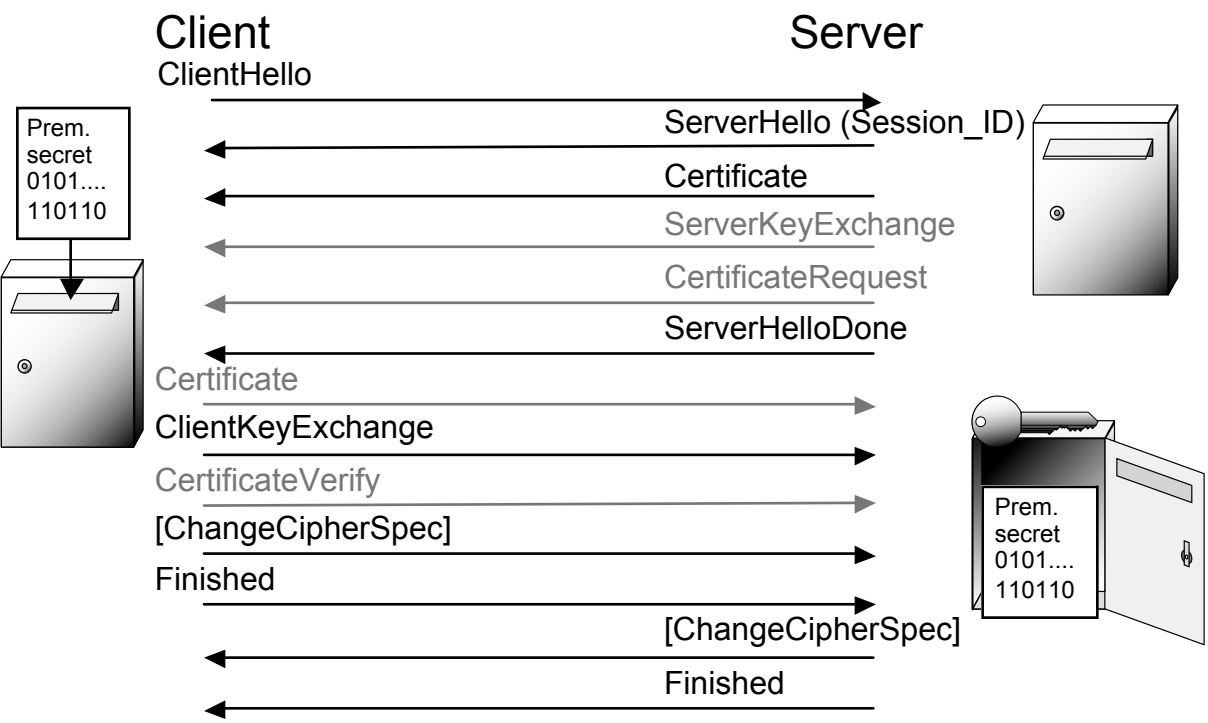
Client
Server
ClientHello
Prem.
secret
0101....
110110
ServerHello (Session_ID)
Certificate
ServerKeyExchange
CertificateRequest
ServerHelloDone
Certificate
ClientKeyExchange
CertificateVerify
[ChangeCipherSpec]
Finished
Prem.
secret
0101....
110110
[ChangeCipherSpec]
Finished