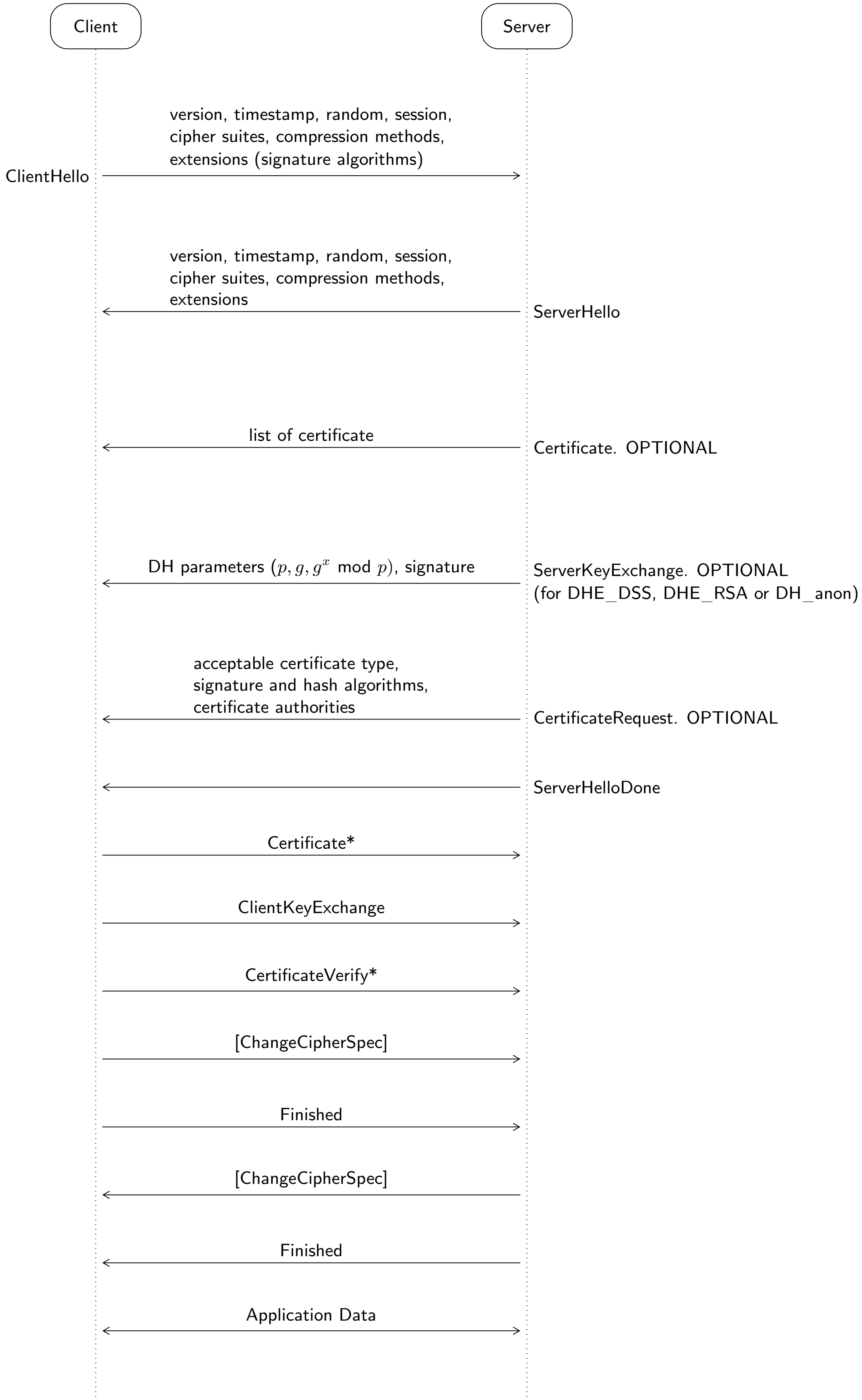
Client
Server
version, timestamp, random, session, cipher suites, compression methods, extensions (signature algorithms)
ClientHello
version, timestamp, random, session, cipher suites, compression methods, extensions
ServerHello
list of certificate
Certificate. OPTIONAL
DH parameters $(p, g, g^x \bmod p)$, signature
ServerKeyExchange. OPTIONAL (for DHE_DSS, DHE_RSA or DH_anon)
acceptable certificate type, signature and hash algorithms, certificate authorities
CertificateRequest. OPTIONAL
ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished
[ChangeCipherSpec]
Finished
Application Data