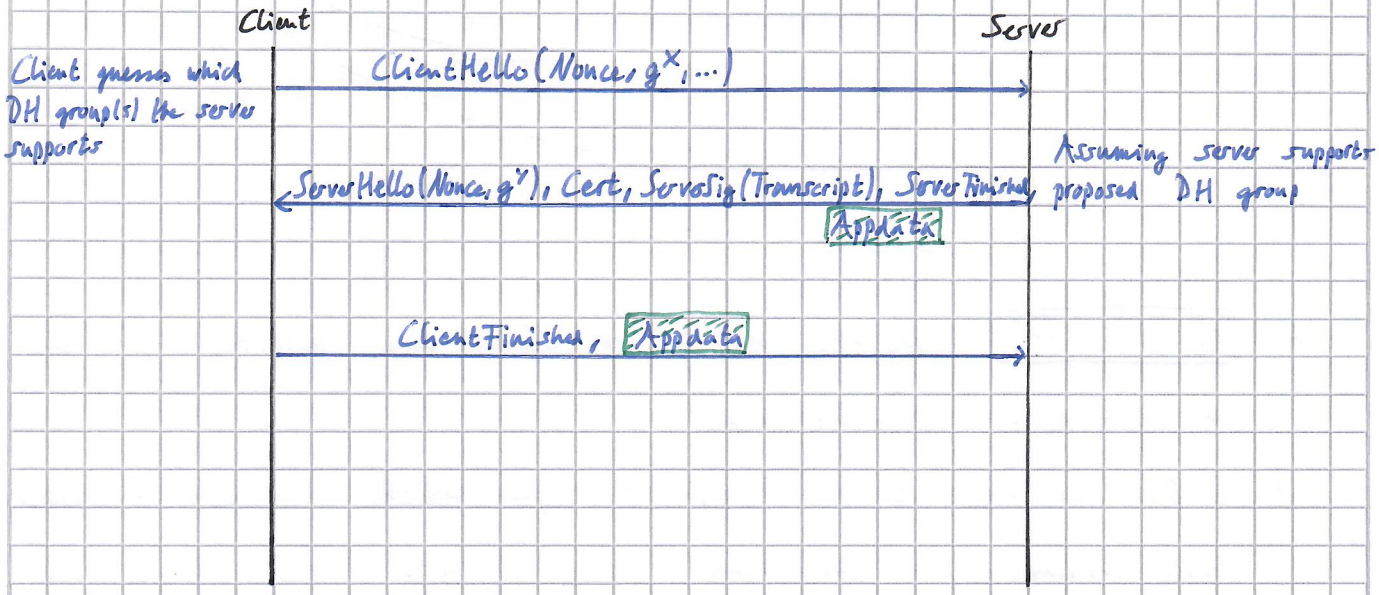
NetSec Exam prep

TLS

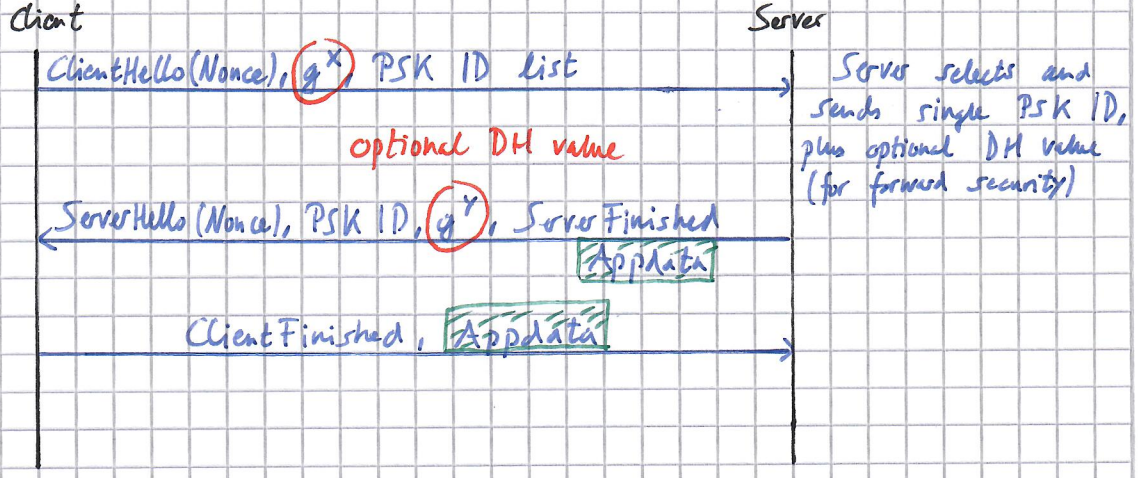
TLS 1.3

- 1-RTT handshake:



⇒ TLS 1.3: reduced set of key agreement options (no RSA, no user-defined DH parameters)

- TLS 1.3 handshake – Resumption



PSKs: Pre shared keys → established in prior handshake, each PSK has an identity

↳ Client sends list of PSK identities in its first flow, plus optional DH value (for forward security)

No server signature, authentication based on Finished messages.