

simplified and one-way authentication

TLS 1.2 (2008)









Na

N

$$N_B, DH_B, \text{Cert}_B, \text{sign}(H(N_A \parallel N_B \parallel DH_B)))$$



DH_A

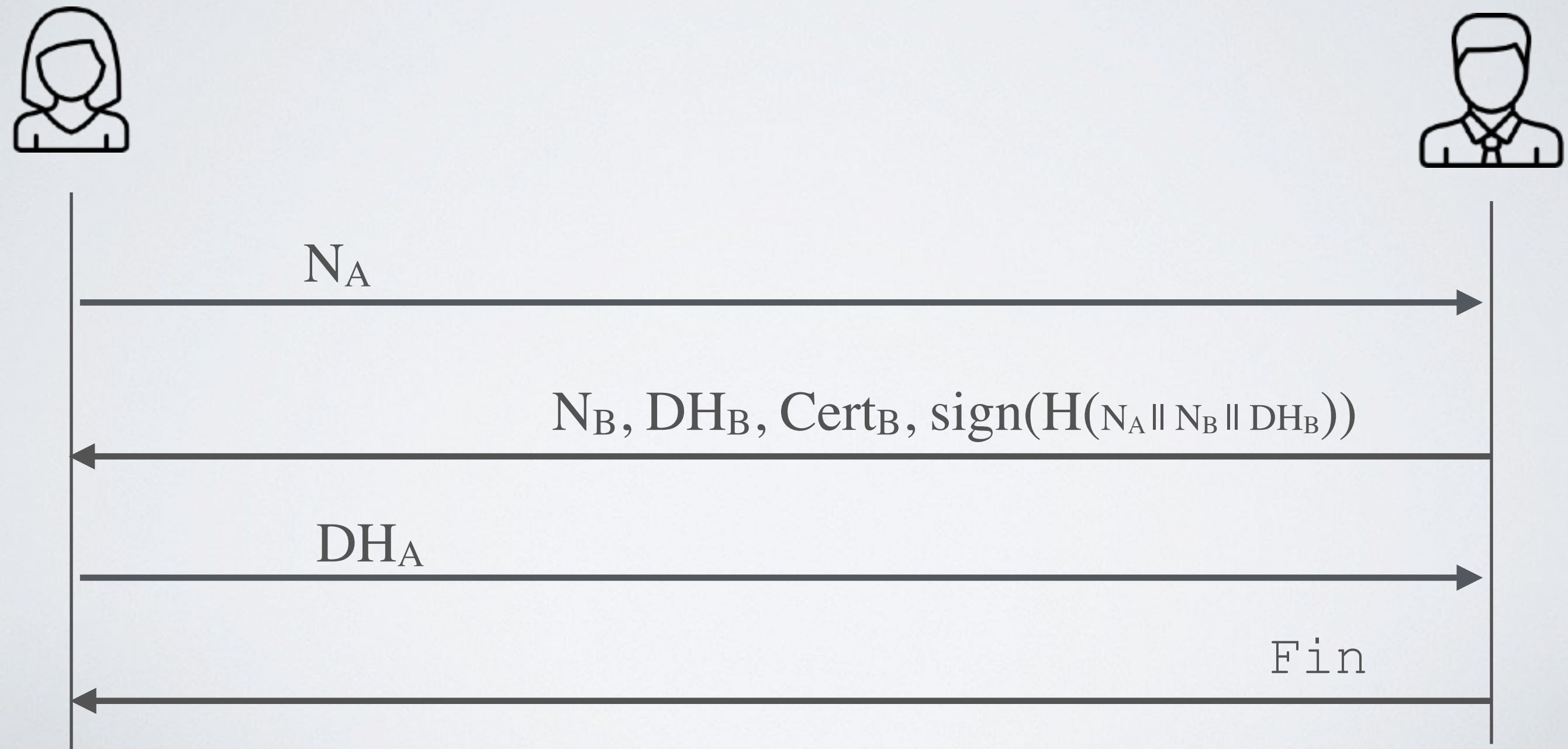


Fin



simplified and one-way authentication

TLS 1.2 (2008)



simplified and one-way authentication

TLS 1.3 (2018)

