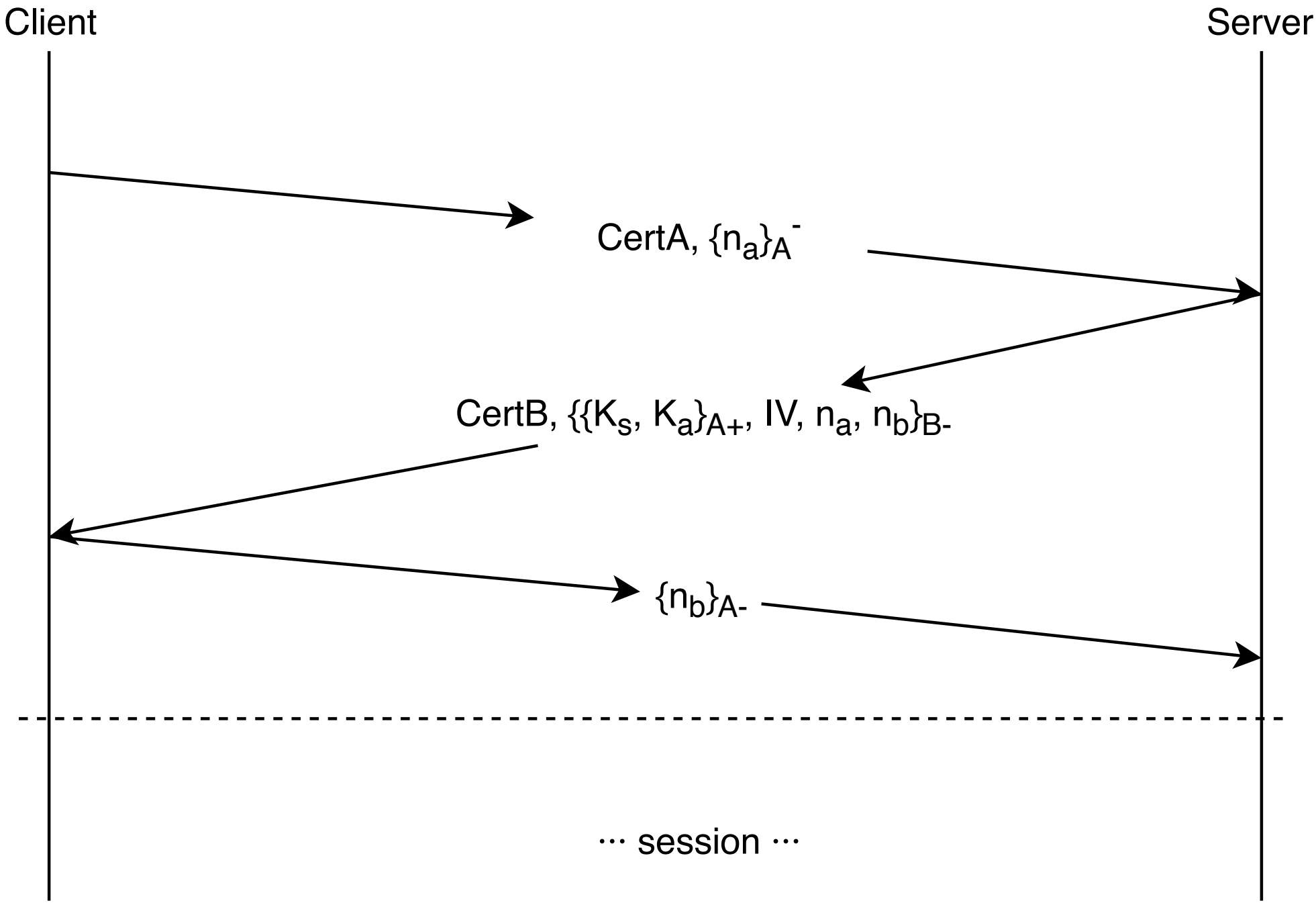
Client
Server
CertA, {n_a}_A^-
CertB, {{K_s, K_a}_A+, IV, n_a, n_b}_B-
{n_b}_A-
··· session ···