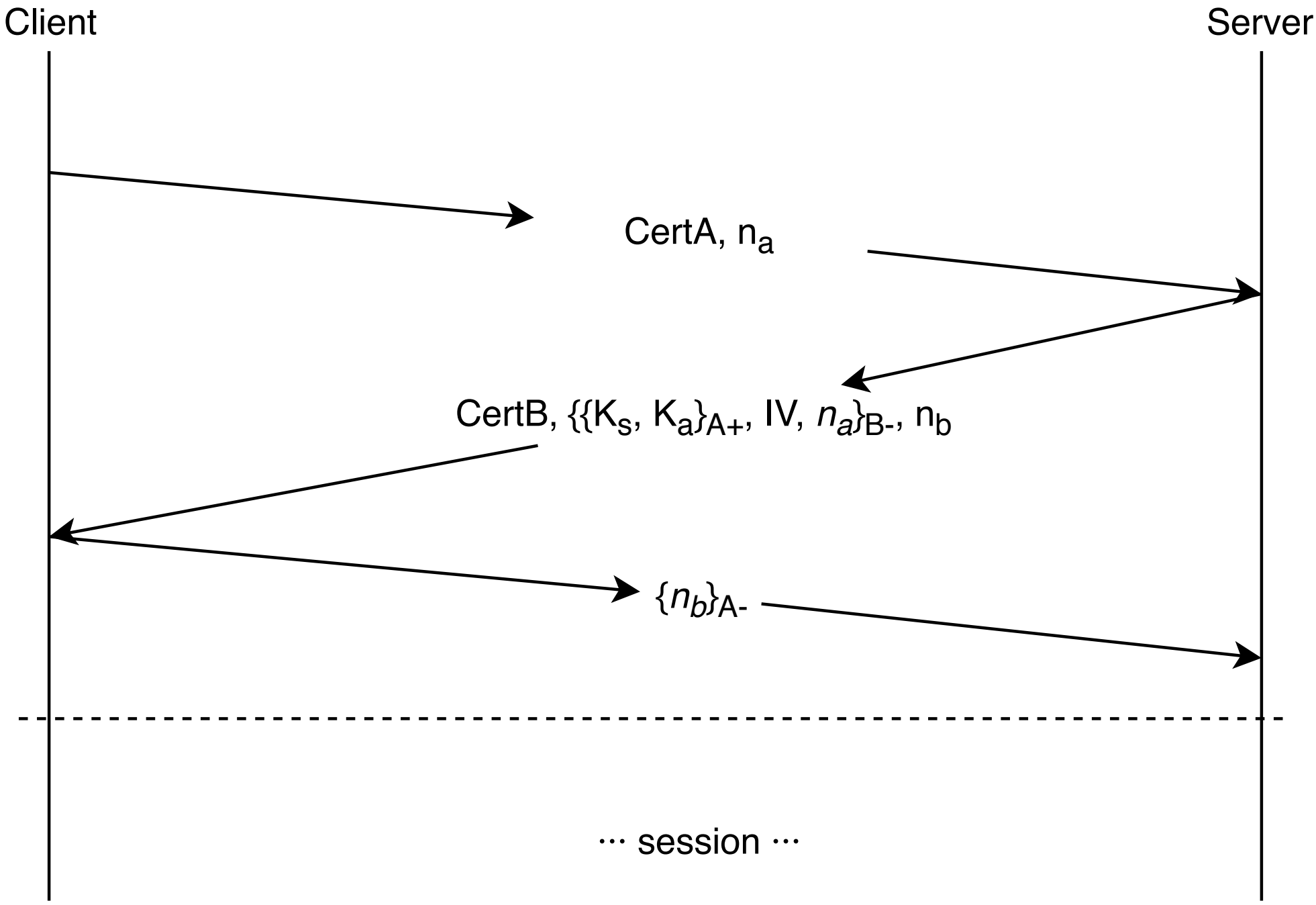
Client
Server
CertA, n_a
CertB, $\{\{K_s, K_a\}_{A+}, IV, n_a\}_{B-}, n_b$
$\{n_b\}_{A-}$
··· session ···