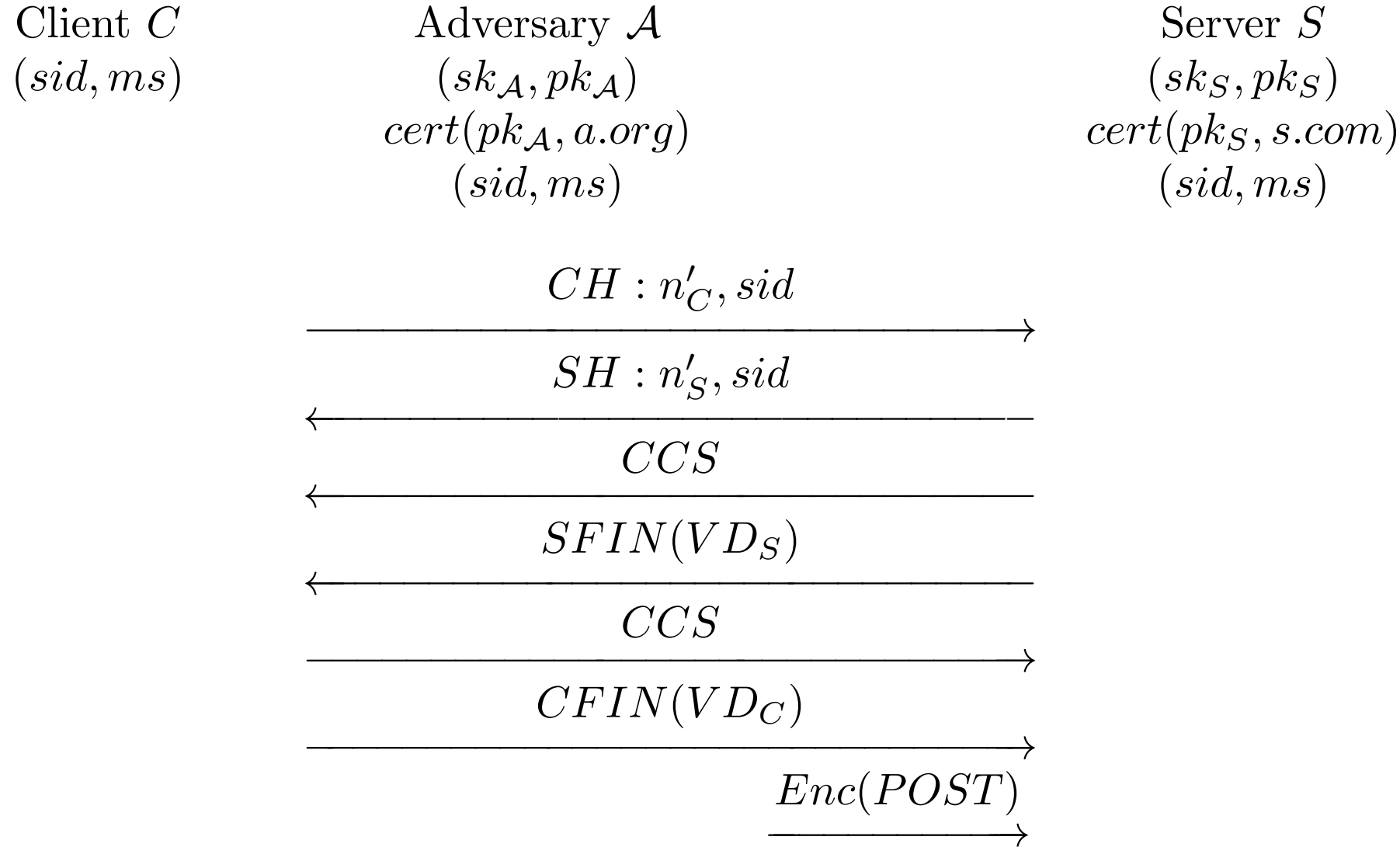
Client C
(sid, ms)
Adversary $\mathcal{A}$
$(sk_{\mathcal{A}}, pk_{\mathcal{A}})$
$cert(pk_{\mathcal{A}}, a.org)$
(sid, ms)
Server S
(sk_S, pk_S)
$cert(pk_S, s.com)$
(sid, ms)
$CH : n'_C, sid$
$SH : n'_S, sid$
CCS
$SFIN(VD_S)$
CCS
$CFIN(VD_C)$
$Enc(POST)$