

Client C

Adversary \mathcal{A}
 $(sk_{\mathcal{A}}, pk_{\mathcal{A}})$
 $cert(pk_{\mathcal{A}}, a.org)$

Server S
 (sk_S, pk_S)
 $cert(pk_S, s.com)$

