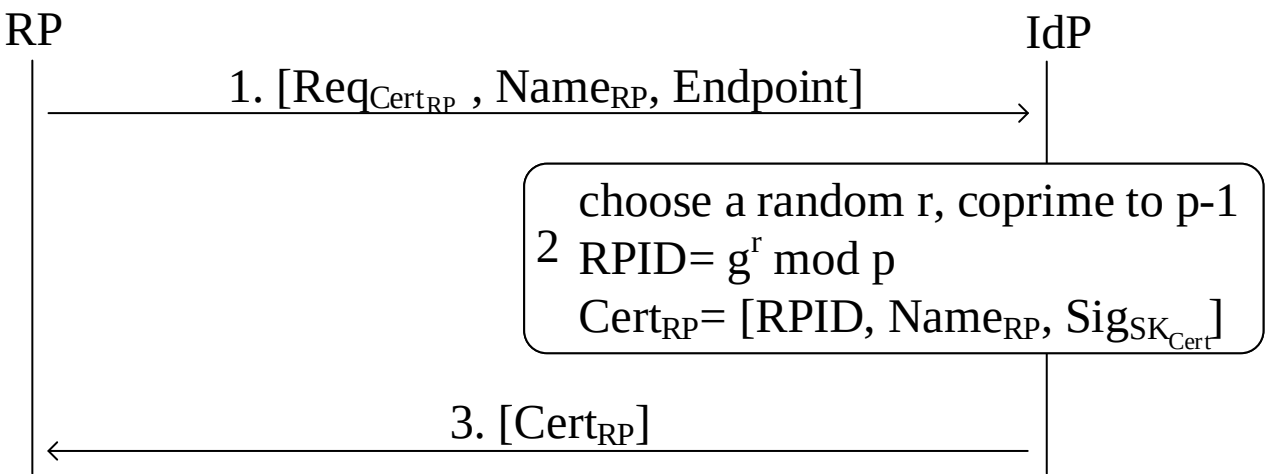
RP
IdP
1. [Req$_{Cert_{RP}}$, Name$_{RP}$, Endpoint]
2
choose a random r, coprime to p-1
RPID= g^{r} mod p
Cert$_{RP}$= [RPID, Name$_{RP}$, Sig$_{SK_{Cert}}$]
3. [Cert$_{RP}$]