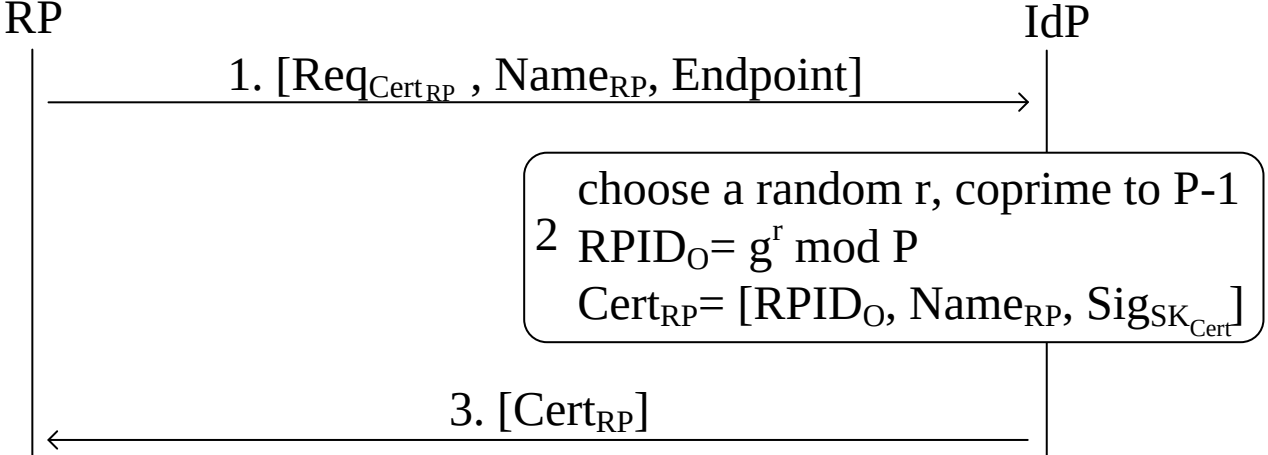
RP
IdP
1. [Req$_{Cert_{RP}}$, Name$_{RP}$, Endpoint]
2
choose a random r, coprime to P-1
RPID$_O$= g^r mod P
Cert$_{RP}$= [RPID$_O$, Name$_{RP}$, Sig$_{SK_{Cert}}$]
3. [Cert$_{RP}$]