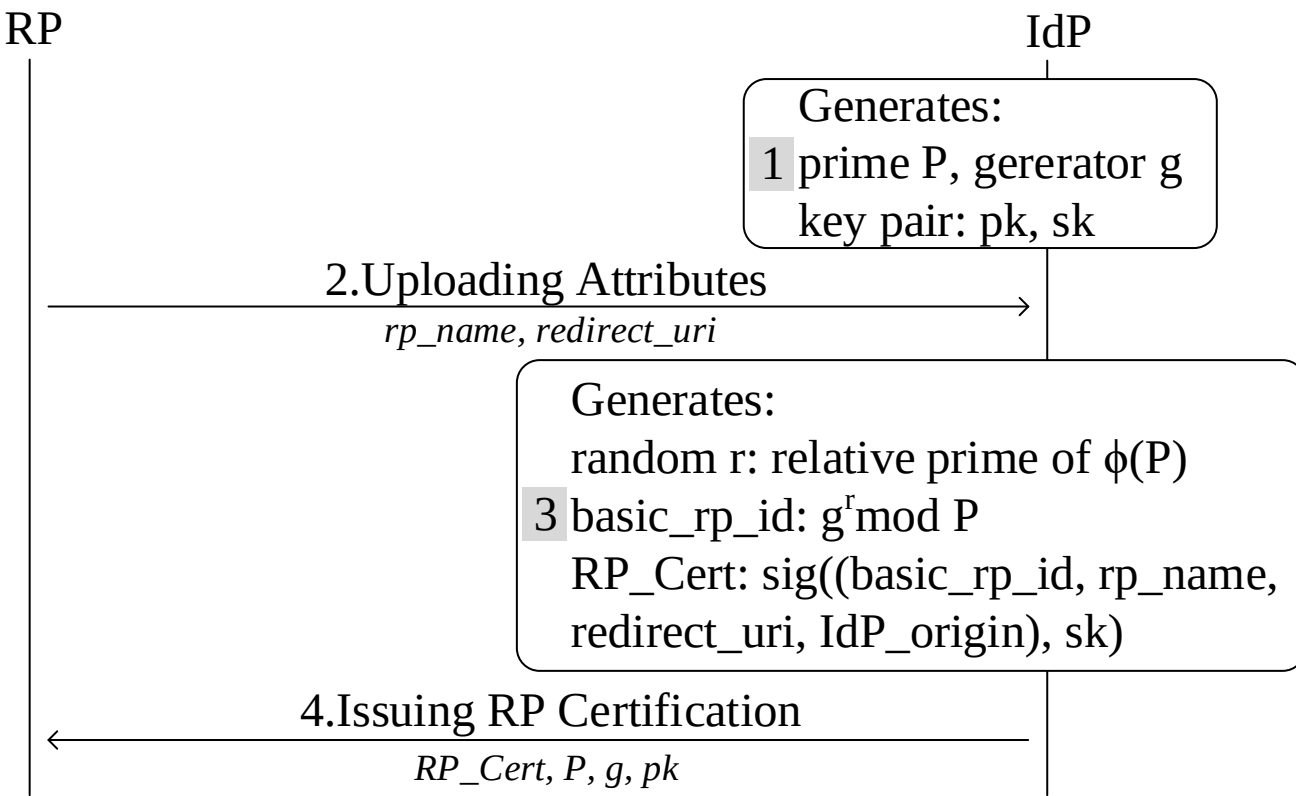
RP
IdP
Generates:
1 prime P, gererator g
key pair: pk, sk
2.Uploading Attributes
rp_name, redirect_uri
Generates:
random r: relative prime of ϕ(P)
3 basic_rp_id: g^r mod P
RP_Cert: sig((basic_rp_id, rp_name, redirect_uri, IdP_origin), sk)
4.Issuing RP Certification
RP_Cert, P, g, pk