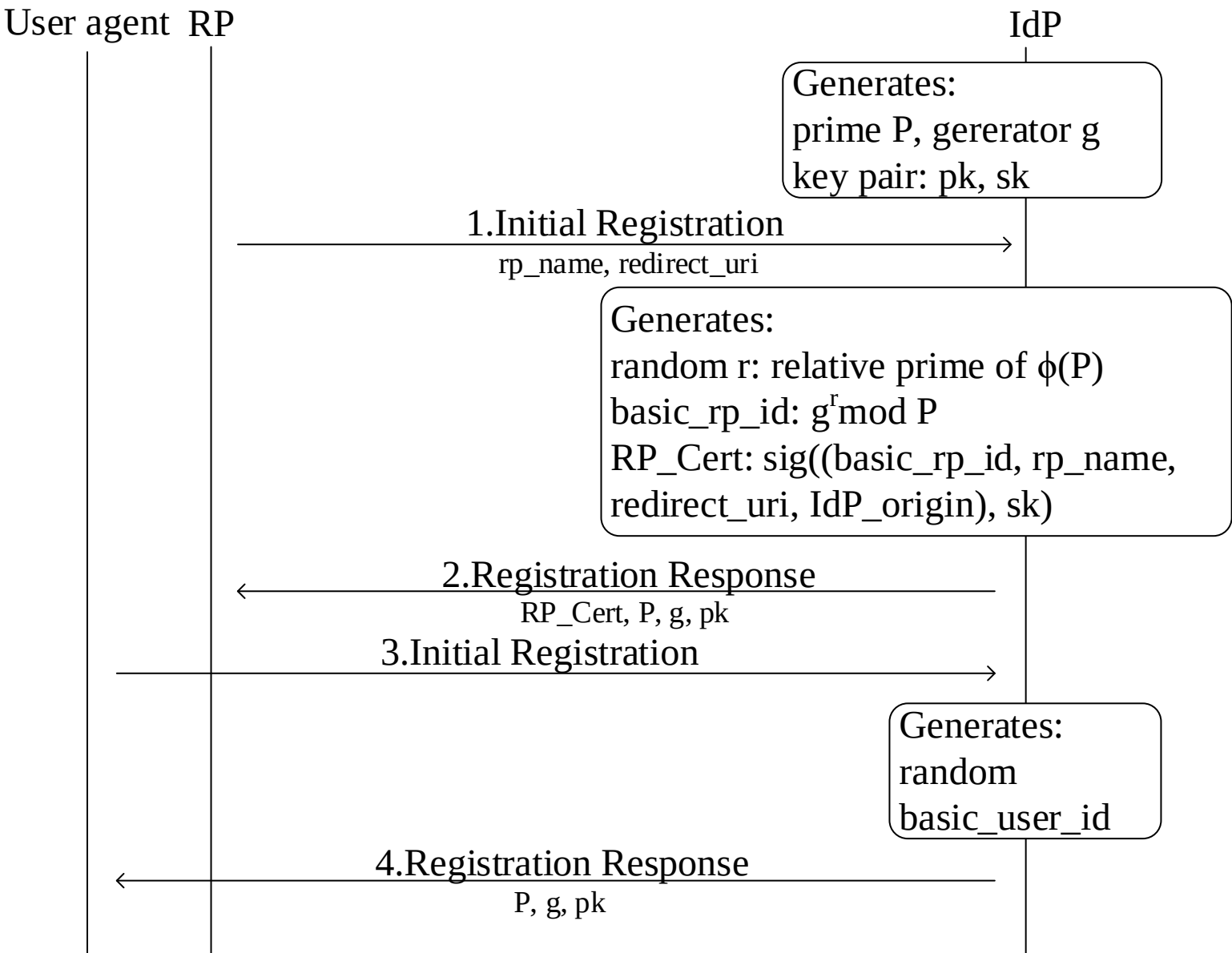
User agent
RP
IdP
Generates:
prime P, gererator g
key pair: pk, sk
1.Initial Registration
rp_name, redirect_uri
Generates:
random r: relative prime of ϕ(P)
basic_rp_id: g^r mod P
RP_Cert: sig((basic_rp_id, rp_name,
redirect_uri, IdP_origin), sk)
2.Registration Response
RP_Cert, P, g, pk
3.Initial Registration
Generates:
random
basic_user_id
4.Registration Response
P, g, pk