

IdP

UID, RPID_O, SK_{Cert}, SK_{ID}

Public Parameters:

g, P, PK_{ID}, PK_{Cert}

3. RPID_T unique ?

4. PPID = RPID_T^{UID} mod P

1. Cert_{RP}:

$\frac{RPID_O}{Endpoint}$
 $Sig: SK_{Cert}$

6. Account = PPID^{(n_u*n_{RP})⁻¹ mod P}

2. RPID_T = RPID_O^{n_u*n_{RP}} mod P

User

UID, n_u, RPID_O

RP

RPID_O, n_{RP}

5. PPID