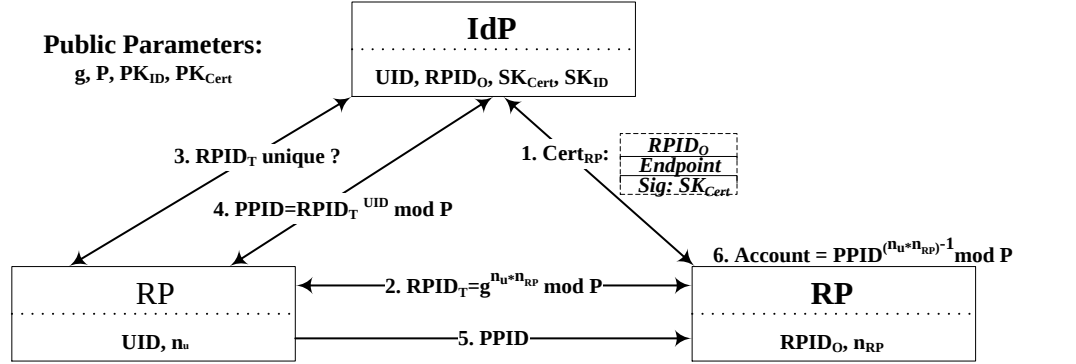
Public Parameters:
g, P, PK_ID, PK_Cert
IdP
UID, RPID_O, SK_Cert, SK_ID
3. RPID_T unique ?
1. Cert_RP:
RPID_O
Endpoint
Sig: SK_Cert
4. PPID=RPID_T UID mod P
6. Account = PPID^(n_u*n_RP)-1 mod P
RP
UID, n_u
2. RPID_T=g^(n_u*n_RP) mod P
5. PPID
RP
RPID_O, n_RP