Associated Parties: Sharing secrets with non-members

IETF 121

Use-cases

- SemiPrivateMessages
- Franking
- Other features that require shared key material with non-members

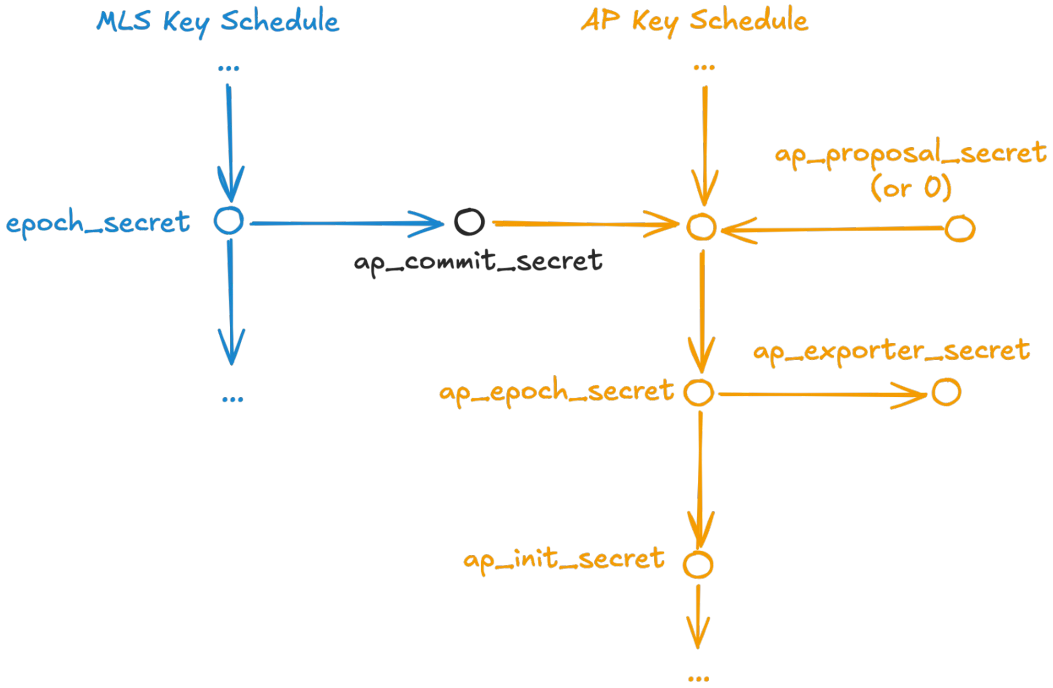
Overview

- Potential associated parties (AP) publish KeyPackage-like structs
- GroupContext: List of associated parties
- Manage APs using Add/Remove/Update proposals
- Each epoch, KEM an exported secret to each AP
- AP key schedules
- Allow APs to contribute randomness

AP Lifecycle

- Potential AP publishes “AssociatedPartyEntry”s
  - Credential
  - Signature Public Key
  - HPKE key
- List of AssociatedPartyEntries in GroupContext
- Group member manage list via
  - AddAssociatedParty
  - UpdateAssociatedParty
  - RemoveAssociatedParty

AP Key Schedule



New Group Members

- Welcomes contain last epoch's `ap_init_secret` for each AP
- External joiners set new `ap_init_secret` for each AP
  - KEM to respective AP and ExternalPub

Thanks!

Overview

- Potential associated parties (AP) publish KeyPackage-like structs
- GroupContext: List of associated parties
- Manage APs using Add/Remove/Update proposals
- Each epoch, KEM an exported secret to each AP
- AP key schedules
- Allow APs to contribute randomness