



Private External Commits and External Proposals

draft-mahy-private-external—Changes since -00

- Clarify terminology around provisional commits
- Clarify the use of the next `epoch_secret`
- Added IANA section
- Expanded Security Considerations

draft-mahy-private-external—Wrap External Proposals

- Why do we need this? Make External Commits/Proposals private to the DS (when you use PrivateMessage handshakes).
- How does it work?
 - Defines new WireFormat: PrivateExternalMessage
 - New Joiner HPKE Encrypts its PublicMessage containing an External Add Proposal to the Group
 - The DS cannot see the KeyPackage or LeafNode inside
 - Members can decrypt the PublicMessage, then authenticate and authorize the External Add Proposal
- What has changed since -00
 - Clarify terminology around provisional commits
 - Clarify the use of the next `epoch_secret`
 - Added IANA section

draft-mahy-private-external—Advertise HPKE Public Key for group

- Advertise ExternalEncryptionInfo (of **future** epoch) in AAD of each Commit, containing
 - CipherSuite
 - HPKE (encryption) Public Key for group
 - Signature Public Key for the group
 - **HMAC of authentication key and these keys**
- Members can verify the contents of the AAD
- Members or DS can share this safely with potential new joiners

draft-mahy-private-external—Preventing attacks

- Attacker could flood the DS with ExternalProposals that members need to decrypt in order to validate.
- **Include an Argon 2di memory-hard hash to discourage abuse**
- **To prevent active attacks, HMAC the authentication_secret with public keys**