

---

---

# Fewer Signature (Single Signature KPs)

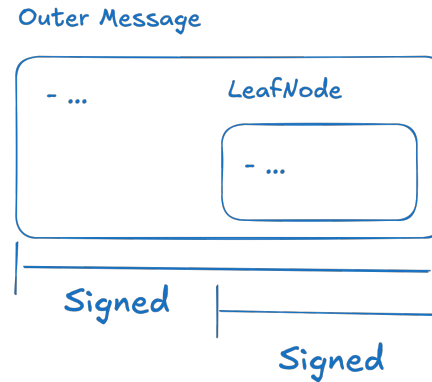
IETF 125  
MLS WG Meeting  
Konrad Kohbrok

---

---

# Reminder

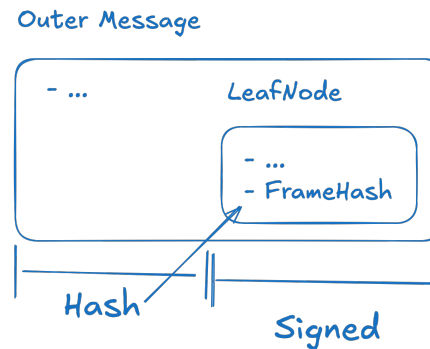
- KeyPackages, Commits and Update Proposals require nested signatures



---

## Reminder cont'd

- Omit one signature by including hash over outer TBS in LeafNode
- Useful when using ML-DSA



---

# What has changed

- Added specification for Commits with UpdatePath and Update Proposals
- Changed name to “Fewer signatures in MLS”

## Caveat:

- Works only if signature key is unchanged
  - Changes to transcript computation required
-

---

---

# ToDo

- Reviews welcome!
  - Update security proofs?
-