MLS Protocol

draft-ietf-mls-protocol-16

Richard Barnes, Raphael Robert,
Benjamin Beurdouche

Since IETF 113...

May 3-17 - WGLC I

May 19 - Interim
May 26 - Interim
Jun 9 - Interim
Jun 15 - draft-15

Jun 16-30 - WGLC II

July 11 - draft 16

July 29 - YOU ARE HERE

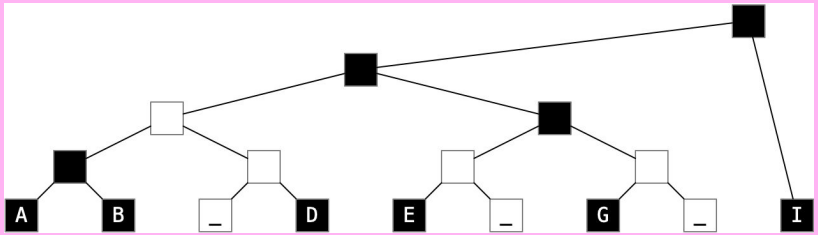
DRAFT-15

Change Log

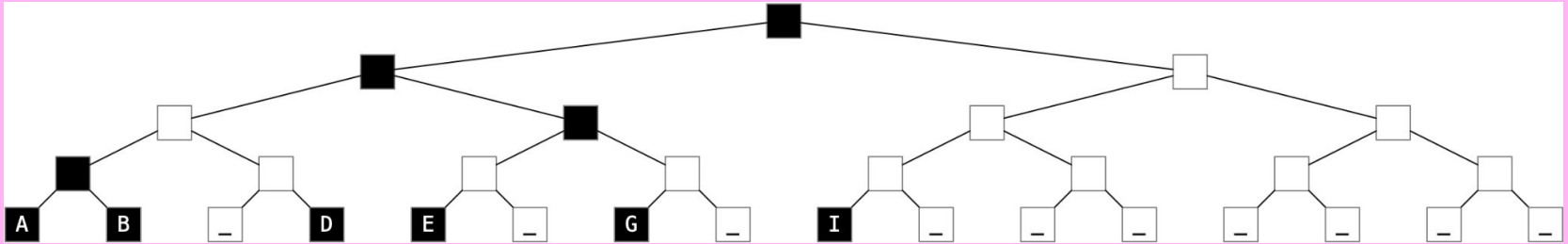
Lots of good WGLC feedback!

- Always use a full tree
- Include ciphersuite in group context
- Add new new_proposal_member SenderType
- Change KeyPackage identifier extension to be LeafNode identifier
- Use new tree for context in path secret encryption
- Use a hash function for hash identifiers
- Add a marker byte to tree hash input structs
- Recommend that group ids are generated randomly
- Update external senders extension to have SignaturePublicKey and Credential
- Replace LeafNodeRef with leaf index
- Remove AppAck proposal
- Make padding arbitrary-size and all-zeroRequire that unmerged_leaves be ordered
- Derive the commit secret from the end of the UpdatePath, not the root
- Specify the precise points in the protocol where credential validation must be done
- Make PSK provisions more uniform, e.g., always generating a fresh random nonce
- Improve parent hash guarantees with stricter checks on tree correctness
- Streamline some structs, e.g., folding GroupContext into GroupInfo
- Provide clearer rules for validating and applying commits
- Clarify tree hash and parent hash, and correct examples
- Clean up struct names and references to outdated structs
- Cite AEAD limits draft

Always use a full tree



- Tree only changes size by doubling or halving the number of leaves (changing height)
- Much simpler tree math (esp. For parent hash)
- Extra nodes are all **virtual** – guaranteed to be blank by "no redundant nodes" PR
- Only perf impact is in tree hashing…
- … and even that can be pre-computed



DRAFT-16

Not interesting

Added a missing field in GroupInfoTBS

Moved a reference from normative -> informative


Onward!
To the IESG!