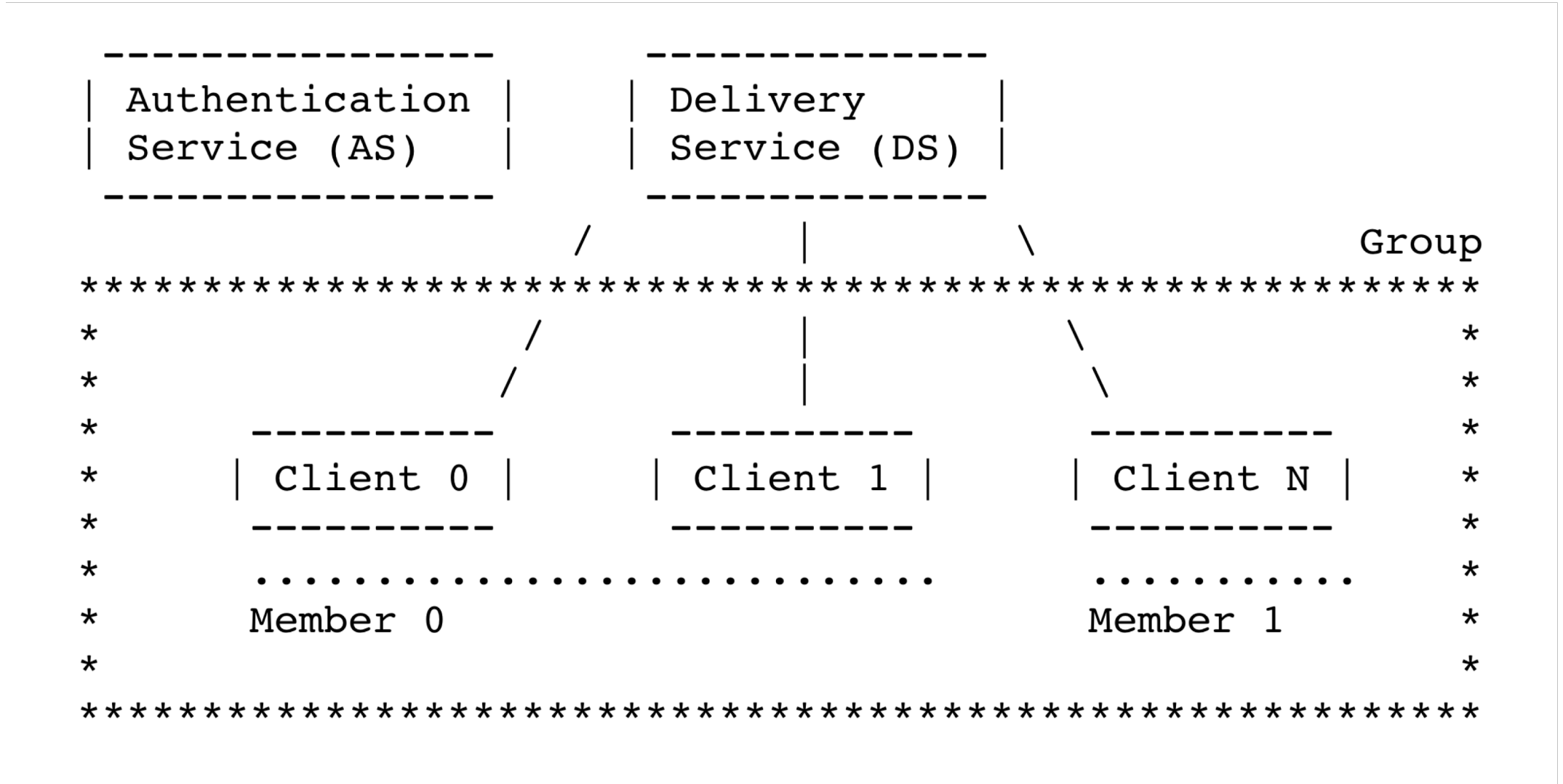
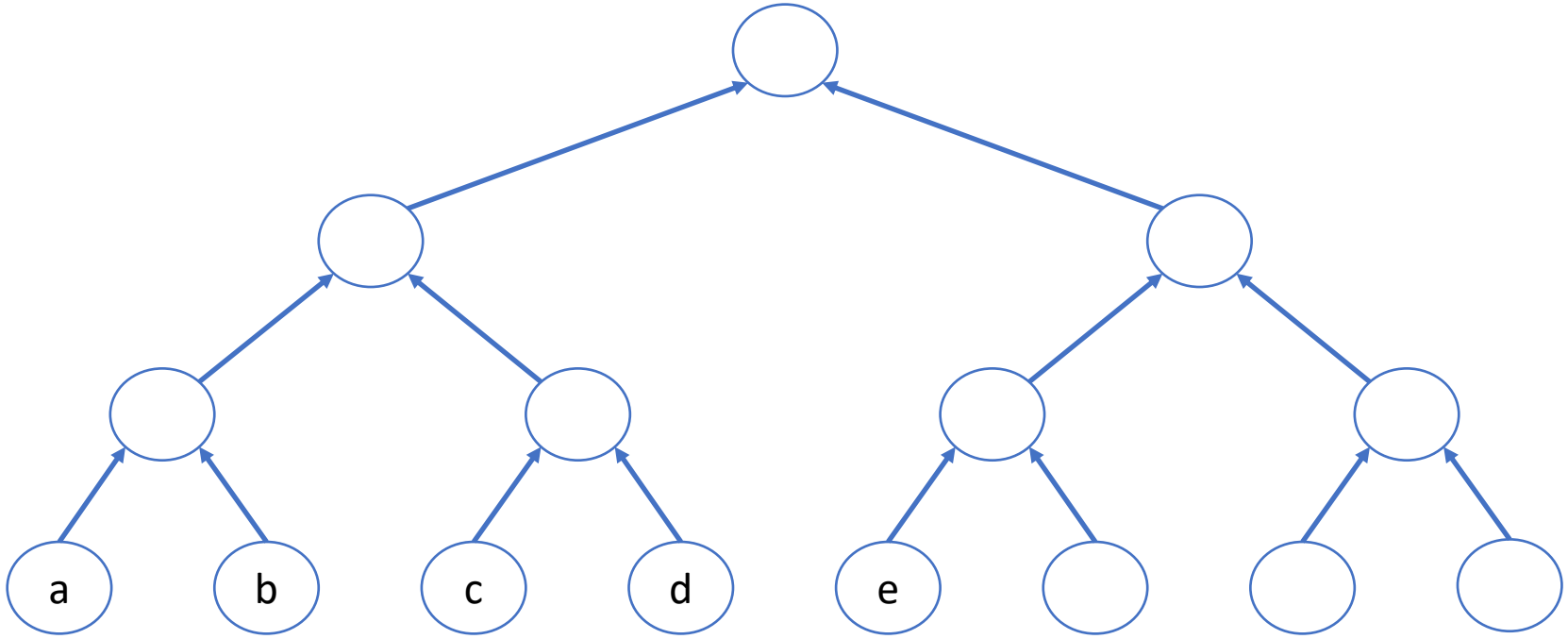
Threat Model and Security (Non-)Goals

Discussion

Architecture: Who to Trust?



Participants: What to Authenticate?



Protocol State

Full group membership

Group's messaging key

Leaf KEM keys? Subgroup keys?

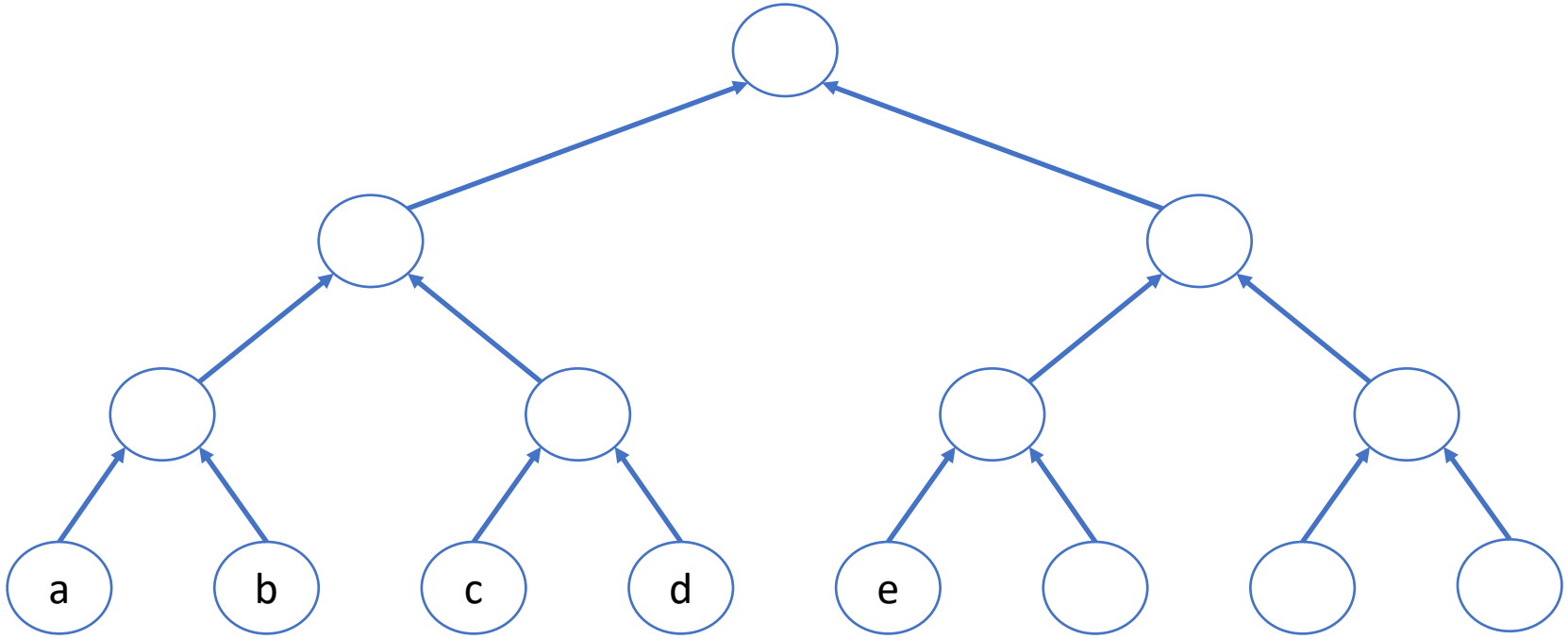
Message Authenticaiton

Sender's identity

Sender's knowledge of leaf KEM key?

Sender's knowledge of its leaf key?

Malicious Participants?

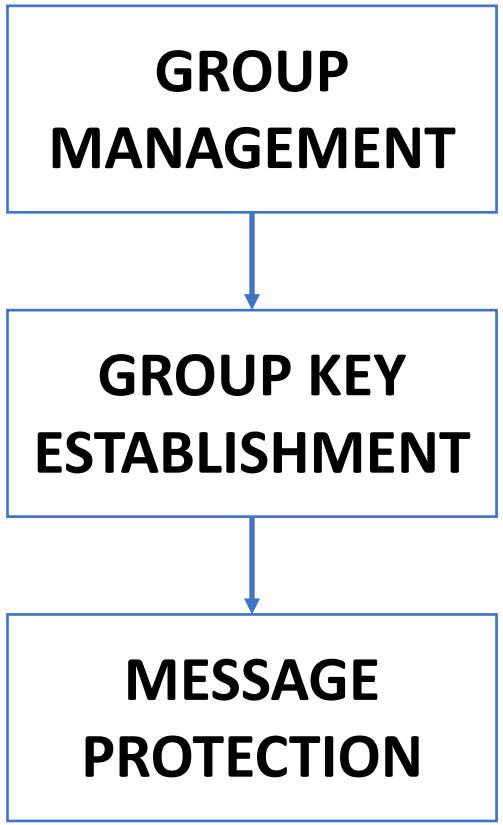


Protocol State
Prevent malicious participant
from creating inconsistent state

Message Authentication
Prevent malicious participant
from impersonating another node

MLS Components

- Manages subgroup tree
- Manages epoch_secret
- Secrecy and Authentication of all tree keys



- Establishes (private?) membership
- Publishes leaf + auth keys
- Authentication (privacy?) of leaf/auth keys

- Manages messaging chains
- Secrecy and authentication of messages