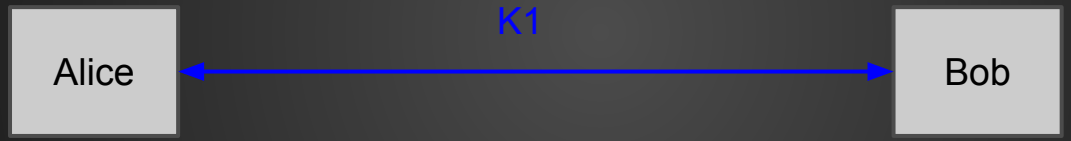
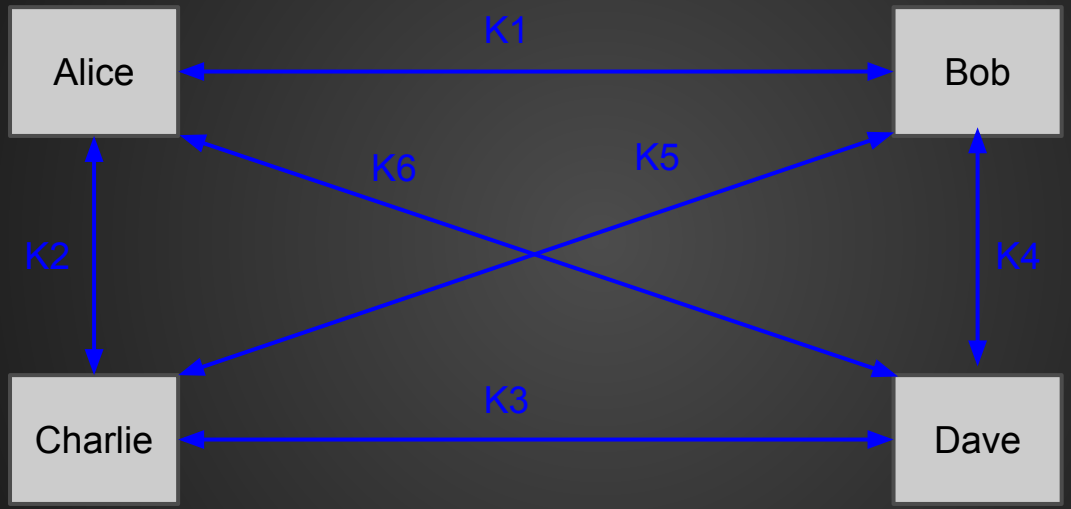
Secure Conferencing

Eric Rescorla
Mozilla
ekr@rtfm.com

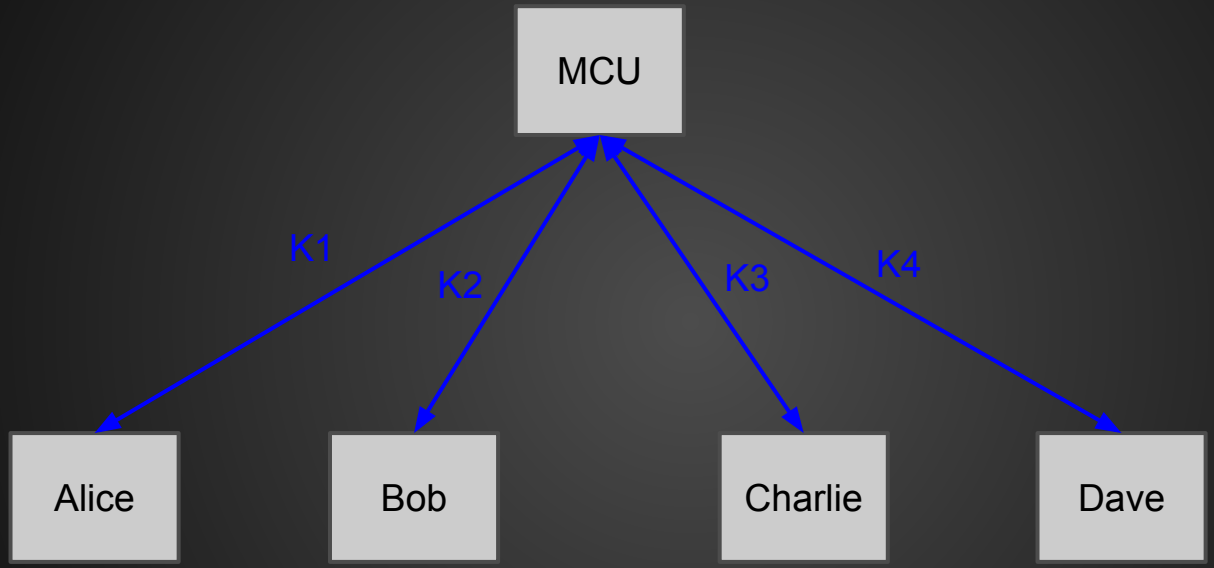
1-1 Calling



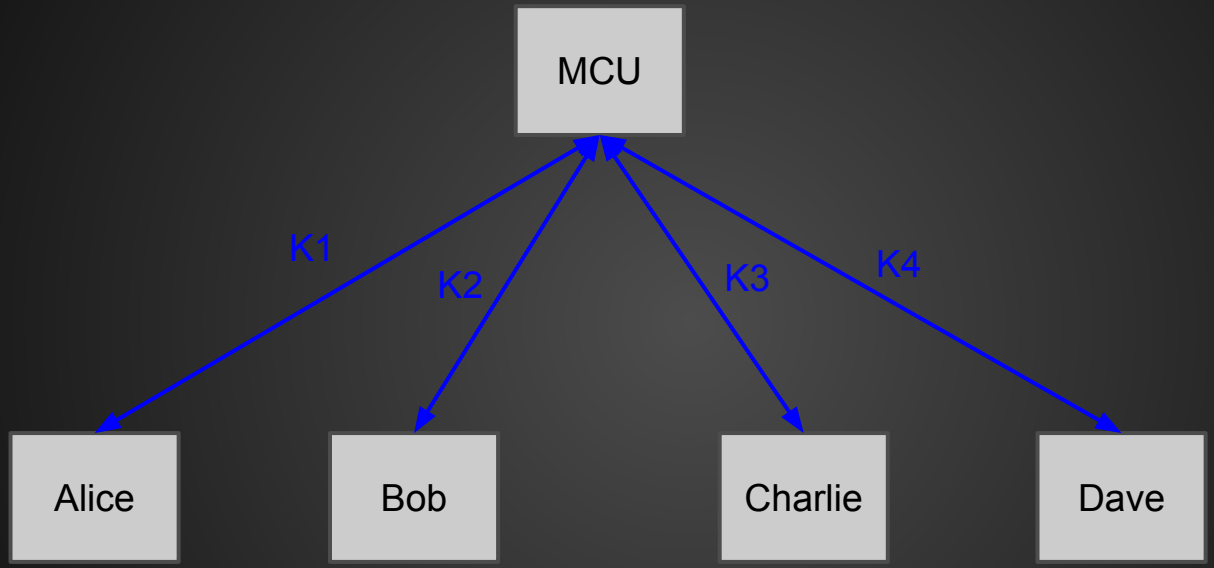
Mesh Conference Calling



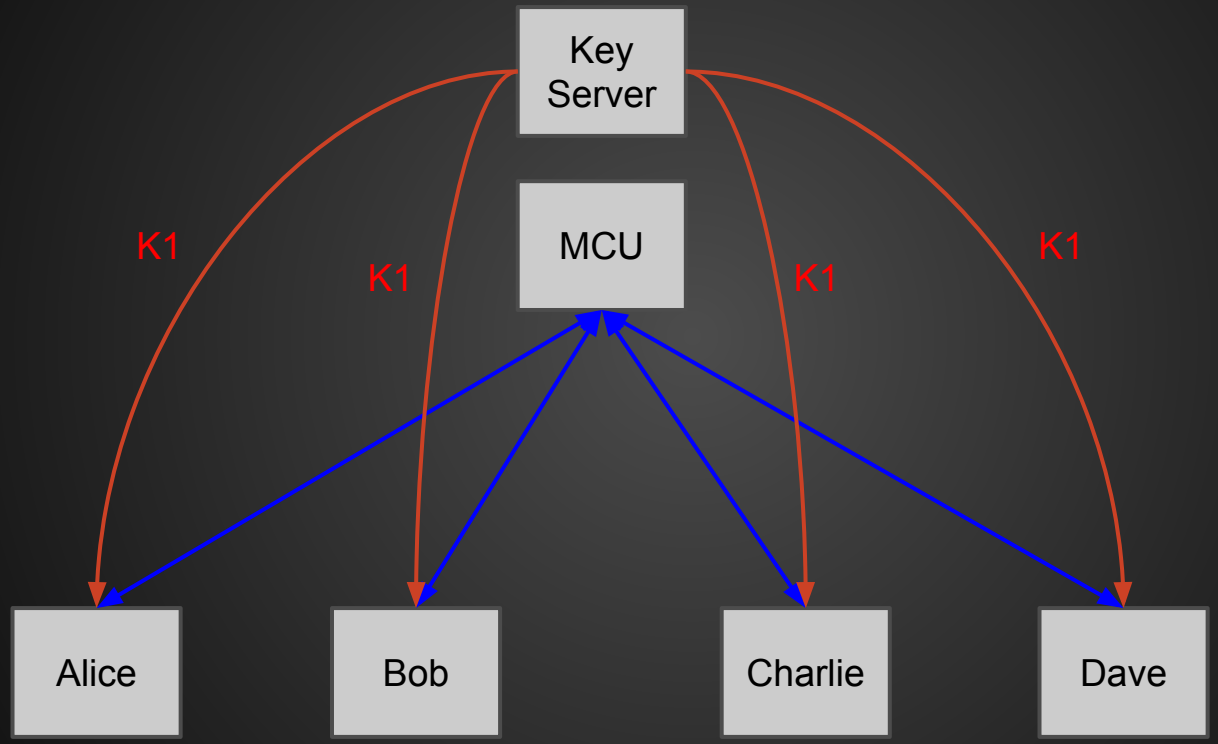
Central pairwise keying



Central pairwise keying



Secure Conferencing (Naive)



Work items

- Threat model
- Key establishment (DTLS + EKT)
- SRTP modifications needed
  - Both hop-by-hop and end-to-end keys

- Expecting to form a different WG in RAI
- Security attention needed