
Two party profile

IETF 125
MLS WG Meeting
Konrad Kohbrok

Why?

- Discussion in other WGs to use MLS in two-party context
 - Use MLS to power secure channel protocols (TLS, QUIC)
 - PCS useful in long-running connections
 - Benefit from extensive analysis of MLS
-

What?

- A way to use MLS specifically for two parties
 - Three phases:
 - Key establishment
 - Key updates (in-band)
 - Resumption
 - Commits in ping-pong ordering (for now)
 - Vanilla MLS (for now)
-

How?

