XMPP E2E

Matthew Miller

IETF 84 - XMPP WG

Changes from -00

- Updated to latest JOSE drafts
- Use key wrapping
- Updates around CMK (and now SMK) usage concerns

Key Wrapping

- Encrypt (wrap) one key using another
- Content Message (CMK) encrypts content
- Session Message Key (SMK) encrypts CMK
- “Better” JOSE

Content Message Key

- Encrypts content
- included with encrypted data
- Generated for each stanza

Session Message Key

- Encrypts CMK
- Obtained via <keyreq/>
- Might be re-used for each <e2e/>

/todo

- Signing!
- Notes about sender offline
- Optimizations with <keyreq/>?