JOSE in Action: XMPP E2E
(draft-miller-xmpp-e2e-02)

Matthew Miller
IETF 84 - JOSE WG
Requirements

- Encrypt whole stanzas
- Support multiple end-points
- COMING SOON: Non-optimistic Signing...
About Addressing

- “example.com” ==> server
- “user@example.com” ==> account
- “user@example.com/desk” ==> end-point
Example Topology

- juliet@capulet.lit/balcony
- capulet.lit
- montegue.lit
- romeo@montegue.lit/ye_face_scrolls
- romeo@montegue.lit/court
- romeo@montegue.lit/chambers
- romeo@montegue.lit/garden
Encrypting

- Generate keying material
- Encrypt stanza (alg=keywrap,enc=*)
- Send to user
  - no public key yse (yet)
Delivery

• Sender indicates recipient
• Server determines which end-point
• Might be multiple (e.g. forking)
Key Request

- Exchanges SMK
- Uses PKI from recipient
- Sender can reject
Benefits

• PKI limited to interested end-points
• Compatible with groupchat
Liabilities

- Simultaneously online ... at some point
- Potential for keyreq flooding
JOSE Considerations

- Keyreq feels too custom
- Base64url is slightly awkward