XMPP E2E

IETF 86 ..?

Matt Miller

Latest Changes

- Tracking to latest JOSE
- Better SMK transport/exchange
- Signatures

Signing

- S’ = UTF-8(Stanza)
- JOSE-JWS(S’, PK)
- Wrap in <e2e/>
  - <sigheader/> versus <encheader/>

Meanwhile…

- Effort to RFC-ize OTR
  - Protocol-agnostic
- Yabasta
  - OTR-like for XMPP only
- Differs from OTR
  - Fixed algorithms (SMP, AES-128-CTR)
  - Reputability emphasized

Next Steps

- Adopt as WG Item?
- Persue OTR?