End-to-End Object Encryption in XMPP

IETF 77

Matthew Miller

Why not 3923?

- “Square peg, round hole”: CPIM over MIME over XMPP
- SIMPLE Interop not as high-priority (e.g. MSRP)
- Different processing for different stanza kinds
- Little to no adoption; community has moved in other directions

Alternative #1
TLS over XMPP (XTLS)

- Encryption is based on a session between end-points
- “Stream within a stream”: Reuses TLS protocol with XMPP as transport layer
- Offline case not supported

Alternative #2
Object Encryption

- Each stanza (object) is encrypted stand-alone
- Supports offline case
- Mutual key exchange is through a different protocol

Object Encryption General Approach

- Start with a stanza (<iq/>, <message/>, <presence/>, etc)
- Serialize into UTF-8 octets, then encrypt
- Wrap in matching stanza kind in <e2e/>

Known Limitations

- Public-key operations for every message more resource intensive
- Stanza information (kind, type addressing) cannot be completely protected

Object Encryption Open Issues

- Key exchange (possibly Pubsub/PEP?)
- Object data size limitations (fixed in -02)
- Broadcast issues (e.g. Multi-User Chat)