End-to-End Object Encryption in XMPP

IETF 78

Stephen Ferrel / Matthew Miller

Object Encryption General Approach

- Start with a stanza (e.g. <message/>)
- Serialize into UTF-8 octets
- Encrypt stanza with a block cipher
- Encrypt cipher inputs with a PKI cipher
- Send with a matching stanza kind + type + addressing, with <e2e/> child containing data

Object Encryption Stage 1: Encrypt Stanza

- Input stanza is serialized UTF8, then Base64
- Wrapped with <plain/>, then UTF8
- Encrypted using a block cipher (e.g. AES), then Base64
- Generate MAC from encrypted data
- Wrapped in <data/> element

Object Encryption Stage 2: Encrypt Cipher

- Session key encrypted with recipient's public key, then Base64
- Wrapped in <key/> element

Object Encryption Coming Soon...

- Digital signatures
- Algorithm Details

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 (XEP-0189 one approach)
- Broadcast issues (e.g. Multi-User Chat)