# End-to-End Object Encryption & Signing

IETF 81

Matthew Miller

# Current Status

- Existing documents have lapsed...
- ...Waiting on WOES...
- ...and figuring out some problems.

# Problems?

- Dealing with multiple end-points
- Exchanging keys

# Big Ideas

- Key Distribution and Discovery
- Encryption for multiple end-points
- Signatures with/without Encryption

# Discovering Support

- CAPS (XEP-0115)
- supported if any resource announced e2e

# Distributing Keys

- PEP (XEP-0163)
  - node for all keys; one item per key
  - change notification; offline retrieval

# Encrypting...

- Start with stanza
- Serialize to UTF-8 octet string

# ...Still Encrypting...

- Generate block cipher key
- encData == BlockCipher(blockKey, stanzaStr)
- For each recipient public key:
  - encKey[i] = PkiEncrypt(pubKey[i], blockKey)

# ...Encrypted!

- Package encKeys, encData into container
  - stanza with matching kind + type + addressing to original
  - <e2e/> child with packaged data

# Decrypting...

- Pick encKey that matches relevant keypair
- blockKey = PkiDecrypt(privKey, encKey)

# ...Still Decrypting...

- stanzaStr = BlockCipher(blockKey, encData)
- stanza parsed from UTF8 octet string

# ...Decrypted!

- Validate with signature
- “kind + type + addressing ~= container” might be good enough?

# Signing...

- Start with stanza
- serialize to UTF8 octets

# ...Still Signing...

- Choose privKey for published pubKey
- signature = PkiSign(privKey, stanzaStr)

# ...Signed!

- Package signature, stanzaStr, pubKey info into container
  - stanza with matching kind + type + addressing
  - child <e2e/> with packaged data

# Verifying...

- With appropriate pubKey in hand
- PkiVerify(pubKey, stanzaStr)

# ...Verified!

- parse UTF8 octet string for stanza
- Possibly match kind + type + addressing with container?

# Mix-n-Match

- Sign and Encrypt within same package
- Supports multiple resources
- Supports multiple entities

# Caveat Emptor

- Some trust in PEP implied
- Public-key ops more resource intensive
- Stanza info not completely protected

# Open Issues

- Semantic Key Identifiers?
- Key Distribution Syntax?
- Crypto Packaging Syntax?

# References


- XEP-0030: Service Discovery <http://xmpp.org/extensions/xep-0030.html>
- XEP-0060: Publish-Subscribe <http://xmpp.org/extensions/xep-0060.html>
- XEP-0115: Entity Capabilities <http://xmpp.org/extensions/xep-0115.html>
- XEP-0163: Personal Eventing Protocol <http://xmpp.org/extensions/xep-0163.html>