Wrapped Keys

Matt Miller, Richard Barnes

IETF 85

Specific Problem

- Want to send protected content
- Recipient's key not yet known
- Unwilling to cache content

More Generally

- JOSE has a key distribution model
  - Key Encryption/transport
  - Key agreement
- Want to re-use without protected content

An Example – XMPP-E2E

< draft-miller-xmpp-e2e-02 >

- alice@example.com/desktop Generate CMK
- Enc(CMK, content) → bob@example.com
- bob@example.com/laptop keyreq(pubkey)
  - And bob@example.com/mobile
  - And bob@example.com/tablet …
- alice@example.com/desktop wraps CMK in public key
- Send wrapped CMK → bob@example.com/laptop
  - Repeat for each interested end-point …

Solutions?

- #1 – JWE, key as content
- #2 – separate JWE key fields into another object

#1 Proposal

- Use “alg” algorithms for “enc” instances
  - { “alg”:”dir”, “enc”:”RSA1_5”,…}
- Encrypted Key is left empty
- Content is encrypted with public key

#1 Proposal Example

base64url({

"alg":"dir",

"enc":"RSA-OAEP",

"jwk": { ... }

})...base64url(enc(pubkey, cmk)).

#2 Proposal

- Encapsulate the key w/ existing fields
  - "alg" = [enc]
    - kid | epu | epv
  - "alg" = [trans]
    - kid | jwk | jku | x5t | x5u | x5c
  - "alg" = [agree]
    - kid | epk | apu | apv
- Exchange as new top-level object

#2 Proposal Example (Agreement)

```
{
   "typ":"agree",
   "alg":"ECDH-ES+A128KW",
   "epk":{ ... },
   "key":base64url(enc(epk, cmk))
}
```

#2 Proposal Example (Transport)

```
{
   "typ":"trans",
   "alg":"RSA-OAEP",
   "jwk":{ ... },
   "key":base64url(enc(pubkey, cmk))
}
```

Next Steps?

- Is this a problem we want to address?
- Proposal #1
  - Allow “alg” values for “enc” in limited instances
  - Integrity checking?
- Proposal #2
  - Extend JWK with symmetric wrapped keys
  - Move key management fields from JWE to JWK