Protecting Keys in JOSE

Matt Miller
IETF 86
The Problem

• Transporting private keys
  – Ex: XMPP-E2E

• Might not involve a protocol
  – W3C WebCrypto
One Approach

• draft-miller-jose-jwe-protected-jwk
• JWK as content
• JWE as protection
• PBKDF2 for humans
To Wrap …

• Serialize JWK to UTF-8

• Normal JWE
  – Encrypt JWK with a CMK
  – Encrypt CMK with Agreed Key
... to Unwrap

• Normal JWE
  – Decrypt CMK with Agreed Key
  – Decrypt JWK with CMK

• Deserialize JWK from UTF-8
For Humans

• Derive a Key from a Password with PBKDF2
  – HMAC SHA-256/HMAC SHA-512

• Key wrapping CMK with PBES2
  – PBKDF2 as above
  – AES-128-KW/AES-256-KW
Next Steps

• Explore alternatives?
• Accept as WG Item?
• Incorporate into existing doc?