draft-moran-suit-mti-00
draft-moran-suit-mti-01

IETF 114 Philadelphia
The goal

• To ensure interoperability with a minimal crypto-suite
• This is an asymmetric problem
  • Manifest authors can afford to operate multiple crypto-suites
  • Many recipients can only support a single crypto-suite
  • MTI may be problematic for recipients
  • SUIT does not involve constrained-to-constrained crypto
• Recipients should have appropriate choices available for MTI
  • If an appropriate choice isn’t available, devices will simply not comply with MTI.
Which Authentication Algorithms?

• Symmetric?
  • Definitely Quantum-resistant
  • Key & tag distribution is a pain

• Asymmetric?
  • Classical is small
  • Hash-based is large, stateful private key
    • May be difficult to justify in some applications
  • Other options, but not standardized yet (winners announced)

• This is a moving target
What about Key Distribution

• Symmetric solutions exist
  • KDF from common root for MAC & KEK

• Classical Asymmetric
  • Well known, but may become broken

• PQC Asymmetric
  • No standardized algorithms yet (winners announced)

• This is a moving target
So what about SUIT MTI?

• **Symmetric**
  - Hash: SHA-256
  - Authentication: KDF + HMAC
  - Key Exchange: KDF + AES-keywrap
  - Encryption: AES-GCM

• **Classical asymmetric**
  - Hash: SHA-256
  - Authentication: ES256
  - Key Exchange: HPKE
  - Encryption: AES-GCM

• **Hybrid PQC Asymmetric**
  - Hash: SHA-256
  - Authentication: HSS-LMS
  - Key Exchange: HPKE
  - Encryption: AES-GCM

NOTE: AEAD is not ideal for streaming decryption
Streaming decryption is an intended SUIT use-case.
What about...

• EdDSA
• ChaCha/Poly?
• Curve25519

• Implementors requiring FIPS algorithms need a path...
Please Help!

• Certain to have wrong choices
• Please contribute!