draft-moran-suit-mti-02

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.

Current Status

- Defines 4 MTI algorithms
- MTI algorithms are ALL mandatory to implement for manifest authors and intermediaries.
- Manifest Processors are required to implement at least one MTI.
- MTI is scoped to IoT Firmware Deployment use cases.

- QUESTION: Should we require all authors/intermediaries to implement symmetric algorithms as well?

SUIT MTI algorithms

- Symmetric
  - Hash: SHA-256
  - Authentication: KDF + HMAC
  - Key Exchange: KDF + AES-keywrap
  - Encryption: AES-GCM
- Classical asymmetric 1
  - Hash: SHA-256
  - Authentication: ES256
  - Key Exchange: HPKE
  - Encryption: AES-GCM
- Classical asymmetric 2
  - Hash: SHA-256
  - Authentication: EDDSA
  - Key Exchange: HPKE
  - Encryption: AES-GCM
- Hybrid PQC Asymmetric
  - Hash: SHA-256
  - Authentication: HSS-LMS
  - Key Exchange: HPKE
  - Encryption: AES-GCM

NOTE: AES-CTR or AES-CBC should be swapped in now that we have clarity from the COSE-WG

Other Algorithms

- Ed25519 specialization
- Chacha + Poly1305
- More?