draft-ietf-suit-manifest-16

ietf 112

Brendan Moran
Summary of changes

• Split draft into four documents:
  • draft-ietf-suit-manifest-16
  • draft-ietf-suit-firmware-encryption
  • draft-moran-suit-update-management
  • draft-moran-suit-trust-domains

• Integrated element keys

• URI definition
What is covered

• Authentication
• Flow Control
  • Try Each
  • Multiple components
• Parameter setting
  • Only Override Parameters
• Severable Members
• Text description
What is not covered

• Delegation
• Dependency manifests
  • Integrated dependencies
• Multiple SUIT Processors
• Payload transforms:
  • Encrypted Firmware/Manifests
  • Generic Compression
  • Differential Compression

• Conditions for managing updates
  • Version number match
  • Battery level
  • Use Before
  • Image not match
  • Check Authorization

• Directives for managing updates
  • Wait for event

• Metadata for non-recipient devices
  • CoSWID / CoRIM
Integrated Element Keys

- Integrated payloads (and manifests) are encoded in the envelope with tstr keys.
  - This simplifies the URI->integrated key conversion logic.
  - For short tstr keys, the encoding is smaller than equivalent numeric encoding
  - Enables a new use-case, where an intermediary embeds the payload in the envelope
    - Still allows a failover to fetching from URI
URIs

• Changed requirement for URI parameter to URI Reference
Open issues: MTI Signature alg

• IETF111:
  • Need more information on implementation overhead for HSS-LMS
    • Verification time: Verification time is $\approx 1/3$ ECDSA
      • Possible reason: most libraries are optimized for 1 long hash, not many small hashes.

• Summary:
  • Signature:
    • ECDSA:
      • Mature Tooling
      • Not quantum resistant
      • Long verification time
    • HSS-LMS:
      • Immature Tooling
      • Private key requires maintenance
      • Fixed number of signatures possible => key rotation may be necessary
      • Signatures are $>1kB$
      • Verification time is $\approx 1/3$ ECDSA
Open issues

• Optional-to-implement algorithms
  • RSA
    • Expected time horizon for quantum annealing vulnerability is 2030 (RSA-768) to 2035 (RSA-4096)
  • SHA-512?
  • SHA3?

• Recommendations for crypto agility in constrained devices?