Hash Algorithms

JIM SCHAAD

IETF 104

DRAFT-IETF-COSE-HASH-ALGS

Current State

- Has the following algorithms
  - SHA-1 – Tagged as deprecated
  - SHA-2 – 5 variants
    - SHA-256/64, SHA-256, SHA-384, SHA-512, SHA-512/256
  - SHA-3 – 2 variants
    - SHAKE128, SHAKE256

Open Issues

- What other hash algorithms are currently required?
  - > 256-bit SHA-3 hash functions
  - Truncated SHAKE functions
  - Lighter weight hash functions – KangarooTwelve
- Are the recommended values correct?
  - SHA-1 - Deprecated
  - SHA-256/64 – No
- Recommendations to the DE for assignment
  - Input on expected frequency of use
  - Which deserve 1 byte identifiers – Currently 23 unused

Open Issues (2)

- Should we provide CDDL for a Digest structure?
  - Would be an example
  - If yes, then what goes into it?
- What did I miss?

Going Forward

- Spell Checking and Grammar Pass
- Missing Security Considerations
- How close to last call
  - Does it need to wait for RFC 8152-bis?
- Early assignment of identifiers
  - Which are needed now and which can wait?