COSE Structure

JIM SCHAAD

DRAFT-IETF-COSE-RFC8152BIS-STRUCT
Countersignatures

- Countersignature type – COSE_Signature / [+COSE_Signature]
  - Both options have an array as the first tag
  - Two opinions expressed both for elimination of the first option

- Countersignature0 context string
  - CounterSignature0 → CounterSignature1
  - My code base has just added countersignatures, but not generally released
  - This is an esthetic issue not a technical issue

- Document reorganization
  - Move Countersignature0 out of appendix
  - Make countersignatures a separate section

- CBOR Tag for countersignatures
Open Issues

IANA Considerations
- Need to get review of re-write
- Only lists the new changes for IANA to perform
- DE Instruction updates

Treatment of downref to RFC 7049 (CBOR)
- Should be going up in the near future as well.

CBOR Issues
- Treatment of canonical encoding in section 13 of this document
Interop Status

Need to assess what the IESG wants to see

What is known
  ◦ Three families of implementations exist
  ◦ All three families appear to implement the six basic message structures
  ◦ One implements counter signature
  ◦ Not all algorithms are implemented in all versions.
  ◦ All appear to run tests against the example repository based on eyeballs

Hackathon Results
Going Forward

Continue soliciting feedback from implementers
COSE Algorithms

JIM SCHAAD
DRAFT-IETF-COSE-RFC8152BIS-ALGS
Current State

- Github repository has pointer to diff RFC 8152 and this document
- Relatively few changes in the extracted text
Open Issues

- None known
- What I have missed?
Way Forward

- Clean up security considerations
- Grammar and spelling pass
- Check for missing pointers back to structure draft
- Be more specific about what protected/unprotected fields are populated?
List of requested algorithms

- Padded Key Wrap
  - Add as a Content or a key wrap algorithm?
  - First AE rather than AEAD algorithm as CE algorithm – is that where we want to go?
  - Integration level
List of Potential Algorithms

- What algorithms could be added
  - Hash Algorithms – SHA-2, SHA-3, SHAKE, BLAKE2
  - Signature Algorithms – SHA-3, SHAKE
  - Key Wrap Algorithms -- AES-SIV, KWF
  - MAC Algorithms – KMAC
  - KDF – HKDF w/ KMAC
  - Content Encryption Algorithms Adiantum
  - Key Agreement Algorithm – Add a shared secret
  - Password Based -- ????
Way Forward

- Establish the list of algorithms that are to be added
- Clear with AD on charter
- Set a time line for a new document
- Write document