COSE Structure

JIM SCHAAD

IETF 106

DRAFT-IETF-COSE-RFC8152BIS-STRUCT

Document Status

- WGLC finished -- 16 Sept
  - Error uploading the document to the datatracker in -06
- All known issues addressed
- Shepherd writeup – next step

Interop Status

- Need to assess what the IESG wants to see
- Code review of 8 Different Implementations
- COSE_Sign1 and COSE_Sign are implemented in all
- Encryption and MAC are implemented in Mine and one other
- Almost all of the implementations have pointers back to the COSE Examples project for testing.

COSE Algorithms

JIM SCHAAD

DRAFT-IETF-COSE-RFC8152BIS-ALGS

Document Status

- WGLC finished -- 16 Sept
- One known issue to be addressed
- Shepherd writeup – next

Capabilities (1 of 2)

- Per the request from the chairs, I have added capabilities to the document
  - Algorithm based capabilities
    - If relevant will always have a key type
    - Deals with non-key based capabilities
  - Key based capabilities
    - Will always have a key type
    - Will have key based parameters such as curves
  - Attempted to minimize the overlap under the assumption that one will always specify both
  - Negotiation structures [*([AlgorithmCaps, *[KeyCaps]])]
    - AlgorithmCaps = [*any]
    - KeyCaps = [*any]

Capabilities (2 of 2)

- Need to get verification that this is what is desired
- Need to get verification on the capabilities desired for hash signatures
  - Ability to say I only do this hash or this number of levels?
- Issue a new document

Hash Algorithms

JIM SCHAAD

DRAFT-IETF-COSE-HASH-ALGS

Document Status

- WGLC Finished – Sept 24
- One known issue left – Define capabilities
- Shepherd writeup – not done

Capabilities

- Presumption is empty by default
- SHAKE could be the exception if max and min lengths should be specified.

X509 Certificates

JIM SCHAAD

DRAFT-IETF-COSE-X509

Document Status

- WGLC – Never started
- All issues have been addressed in the document or in email

Way Forward

- Ready for Working Group Last Call
- Do the early assignment of code points

More Algorithms

JIM SCHAAD

DRAFT-SCHAAD-COSE-MORE-ALGS

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?
    - AE conflicts with a MUST in the standard!!

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
- Adopt a document