COSE Structure

JIM SCHAAD

DRAFT-IETF-COSE-RFC8152BIS-STRUCT

Open Issues

- IANA Considerations - DONE
  - 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) - DONE
  - Should be going up in the near future as well.
- CBOR Issues - DONE
  - Treatment of canonical encoding in section 13 of this document

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.

Going Forward

- Should be ready for Working Group Last Call

COSE Algorithms

JIM SCHAAD

DRAFT-IETF-COSE-RFC8152BIS-ALGS

Way Forward

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

- Should be ready for WGLC

TBD: New Algorithms

JIM SCHAAD

NO CURRENT DRAFT

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
- If this is the only one then it will be fast – so far nobody has spoken up about other algorithms to be added.

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

X509 Certificates

JIM SCHAAD

DRAFT-IETF-COSE-X509

Decisions

- What is missing? – Nothing has been raised.
- Define a CBOR (sorted?) array of certificates media-type – Nobody has asked for it – Don't do
- Define any of the media types as CBOR content types? – Nobody has asked for it – Don't do
- Do anything about revocation information? CRLs, OCSP – Nobody has asked for it – Don't do
- Early assignment of numbers – This has been asked for.
- Is there a need for any examples in the document? – Examples have not been pushed due to OpenSSL problems with certificate generation – If the examples are on the github repository they are probably not needed in the document.
- Define a new key type for COSE_Key? I have implemented this differently in my system and no longer think that this is needed.

Way Forward

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