COSE Message

Jim Schaad

4 April 2016

Issue: Define a key parameter for IV

- Opened as a counter balance to Partial IV
  - Need to establish a base IV to XOR with the partial IV
  - Adding to CWK makes sense if that is going to be the distribution method
  - Potential security problems on re-issue of same base IV

- Potentially harmful depending on the use of a partial IV rather than the base IV for dividing the nonce space between multiple entities.

- Discuss

Issue: COSE Padding for Encryption

- Raised in early January
- TLS decided that the ability to pad was worth processing cost
- Currently no “free” way to do this for non-padded cases

- Resolution: Treat as a security consideration and no general solution.

Issue: Publicly Visible Specifications Required

- Pro:
  - Not needed for closed environments
  - Compatibility with first-come first-serve IANA policy?

- Con:
  - Company proprietary in multiple supplier environments
  - JOSE provides a similar feature with private name space.

- Discuss

Issue: Remove “operation time”

- Pro:
  - This is a content creation time in disguise and should be part of the content
- Con:
  - Not all contents are structured and thus have a place for this
  - Defined for use with Counter Signatures
  - Defined as operation not content creation time
- Discuss

Issue: Add ECDH and EdDSA for Curve25519

- These algorithms were deferred because it was thought that this document would finish first.
- ECDH is now completed as RFC 7748
- ECDSA as completed RG last call

- Should we move these algorithms back into the main document?

Issue: Make “alg” field optional

- New appendix is addressing this issue
- Francesca et al requested this be included here
- Mike has objected to it being here

- Discuss

Issue: Define ‘bstr’ Counter Signature

- New appendix is addressing this issue
- Francesca et al requested this be included here
- Mike has objected to it being here

- Discuss