COSE Message Issues

Jim Schaad
August Cellars
IETF 94
Issues in COSE-WG/Cose-Issues

• CFRG Issue with doing key derivation
• Assign Integer Keys to all Algorithms
• Add RSA v1.5 signature algorithm
Issues in COSE-WG/cose-spec

- Add MAC-OPS to key ops
- Usage of strict mode CBOR encoder/decoders
Document Issues – Editorial & Structural

• Changes from JOSE
• Document Terminology
• Verify we only refer to item defined in document as examples in document
• Change examples to be both more numerous and better pretty-print
• Moving CDDL to appendix
• Clarity of field transportation in the KDF context
Document Issues - Mime Types

• Registration of application/cose vs application/cose+cbor
  – Do we need to have both or is one sufficient.
  – CBOR currently the only sensible encoding (unless one wants ASN.1)

• Addition of smime-type style parameter to application/cose
  – RFC 2633
  – Allow for a method of identifying security features

• Addition of encapsulating and inner types ala RFC 7193
  – Not recommending
Document Issues

- Application Guidance (Mandatory to Implement)
  - Expand to be guidance rather than current statement
Document Issues - ACE

• Security Creation time
• Anti-Replay fields (Sequence Number)
• Algorithm Optionality