Discussion of JOSE open issues

John Bradley @ve7jtb

5 Unclear instructions for key management

- draft-ietf-jose-json-web-encryption-09 adds clear instructions for using each key management mode. See the Key Management Mode definitions in the Terminology section (Section 2) and the uses of these definitions in the Encryption and Decryption instructions in Sections 5.1 and 5.2. I therefore believe that this issue should be closed.

- Recommendation: Closed as fixed

7 Algorithm identifiers/ parameters incompatible with WebCrypto

- As Discussed in Denver, it is up to Webcrypto working group to use the JWA identifiers or not.
- No Action needed on our part.
- Recommendation: Close

13 Enable AEAD key wrapping

- Draft 13 added AEAD key wrapping.
- Recommendation: Close as Fixed

14 Support longer wrapped keys than OAEP allows

- OAEP is limited by the size of the RSA Key.
- Minimum size is 2048 bits, larger keys can be used and will be required in future.
- All known symmetric keys can be wrapped with OAEP.
- Recommendation: Close, Theoretical problem

15 At least one key indicator should be mandatory

- Draft 11 incorporated the text agreed to at Denver F2F.
- Recommendation: Close as fixed.

18 Address MAC key lifetime concerns

- Recommendation:
  - Add security considerations that key lifetimes for JWS/JWE usages adhere to limitations in specs defining those key-types
  - Close after review

25 Detached content for the ALTO use case

- Can be done by applications by signing a digest of the detached content in the current spec.
- Recommendation: Close won't fix

26 Allow for signature payload to not be base64 encoded

- On last call there seemed to be agreement that this is a v2 feature and may depend on future serializations of JSON.
- Recommendation: Close Won't Fix

28 AES-GCM should not be allowed for content encryption in combination with Direct Encryption key management mode

- Draft 13 added the security considerations from NIST
- Recommendation: Close as fixed

29 Add an explicit "aad" field to JWE

- Added in Draft 13
- Recommendation: Close as Fixed

30 Align key usages with WebCrypto

- Single Key use is by design to prevent security issues.
- "alg" values can be used to restrict key usage when appropriate.
- Recommendation: Close won't Fix

31 Add extractability field for JWK

- Semantics under defined.
- Web Crypto can use the IANA registry to define and add the element.
- Recommendation: Close No Action needed.