Crypto issues for JOSE

Eric Rescorla

ekr@rtfm.com

IETF 83

Algorithm Definitions and Key Lengths (JWA)

- Want to specify some minimum values

Algorithm	Key Length	
RSA	1024? 2048?	1024 is weak but common
ECDH	160 bits	
HMAC	Size of output	

- The other algorithms have fixed-length keys
- What about entropy?
  - Recommend a minimum of 128 bits of entropy
- Algorithms should be used with matching strengths where possible

Initialization Vector Generation

- Required for all the symmetric encryption algorithms
- CBC
  - MUST be a multiple of the block size (technical reqt.)
  - $>$ block size adds no value
- GCM
  - FIPS-800-38D allows 1-2^{64} bits.
  - ...but recommends 96 bits
  - Recommend we use 96 bits
  - MUST be generated via RFC 1750

Carrying the IV

- Current draft is kind of unclear
- Example 3.1 shows AES-GCM with a separate IV
- Section 8.2 describes it as “prepended”
- Proposal: IV is carried separately in “iv” field
  - And make it mandatory

Key Wrapping

- We currently specify RFC 3394
  - This requires 64-bit aligned inputs
- RFC 5649 allows arbitrary aligned inputs
  - In case you have something like that
- Not clear this is needed but also seems harmless
- Proposal: Specify both