# Bringing the JOSE WG Specifications to WGLC

Nat Sakimura

November 7, 2012

# JOSE Status by Specification

- JWS
  - Very stable since March 2011
  - Well over a dozen known implementations
- JWE
  - Open issues largely closed since IETF 84
  - At least 5 known implementations
- JWK
  - Semantically very stable – a few syntax changes
  - Also over a dozen known implementations
- JWA
  - Open issues largely closed since IETF 84
  - Used in JWS, JWE, JWK implementations

# Conclusions

- The specs are fairly mature and implemented
- Most issues have been closed
- We're ready for WGLC
- Options:
  - Go to WGLC with the current specs
  - Close issues we can quickly close, then go to WGLC

# Remaining Open Issues

- Default RSA-OAEP parameters
- Criticality of understanding header fields
- Define nonce, timestamp, and/or uninterpreted string parameter(s)?

# Default RSA-OAEP parameters

- SHA-1 (and mgf1SHA1) are the default OAEP parameters in RFC 3447
  - They are also the parameters specified in JWA
- Many libs don't support other OAEP parameters
  - Interop argues for keeping things as-is
- Previous results:
  - 7 YES – keep the current default OAEP parameters
  - 2 NO – change the default parameters
  - 4 DISCUSS

# Criticality of understanding header fields

- Currently implementations must understand all header fields
- Security argues for the current behavior
- Extensibility argues for allowing not-understood fields or specifically identified fields
- Previous results:
  - 9 YES – all header fields are critical
  - 1 NO – all header fields are non-critical
  - 4 MAYBE – criticality should be specified per field
  - 3 DISCUSS

# Define nonce, timestamp, and/or uninterpreted string parameter(s)?

- Previous results:
  - 7 YES – Define nonce/timestamp parameter
  - 1 NO – Do not define nonce/timestamp parameter
  - 14 DISCUSS
- DISCUSS likely dominated because there were no concrete proposals
- One possibility is to defer decision(s) until concrete proposals are made