Fully-Specified Algorithms for JOSE and COSE

draft-ietf-jose-fully-specified-algorithms

Mike Jones and Orie Steele
IETF 119, Brisbane
March 18, 2024
Why and What

- See Introduction in draft-ietf-jose-fully-specified-algorithms
- Or IETF 118 slides
Progress Since IETF 118

• At IETF 118 in Prague, presented draft-jones-jose-fully-specified-algorithms, which incorporated feedback received since IETF 117

• There was support for working group adoption at IETF 118

• Successful call for adoption held in January 2024
  • With useful feedback from working group members

• draft-ietf-jose-fully-specified-algorithms-00 published in January

• Updates in -01 & -02, incorporating WG feedback during adoption
  • Text on fully-specified computations using multiple algorithms
  • Text on KEMs and encapsulated keys
  • Updated instructions to designated experts
Open Question on ECDH-ES

- ECDH-ES, ECDH-ES+A128KW, etc. take ephemeral key as a parameter
  - Meaning that they are polymorphic

- Should we create fully-specified algorithm identifiers?
  - Such as ECDH-ES-ES256, ECDH-ES-ES256+A128KW, etc.

- Some on the list are saying that we should do the whole job

- Brian Campbell and Ilari Liusvaara wrote on-list that there would be 10 or 12 new algorithms for combinations that make sense

- Let’s discuss
Next Steps

• Ask ECDH-ES question on-list?
• Once resolved, publish updated draft incorporating resolution
• Then working group last call?