draft-ietf-suit-mti-algorithms

ietf 117
July 2023
Summary

• Added authors
  • Thanks to Akira & Øyvind!
• Replaced HPKE with ECDH
• Added a CDDL profile for each algorithm
Purpose of suit-mti-algorithms

• Ensure that Manifest authors & Distributors can interoperate with Manifest Recipients.
• Focus is on Manifest Recipients that are:
  • On Constrained Networks
  • Implemented as Constrained Nodes
• Will track development of algorithms over time
• Algorithms may be deprecated and/or replaced as appropriate
HPKE vs ECDH-ES

• HPKE is gaining adoption
• HPKE may be used in upper-level protocols as well (e.g. TLS)
• Sharing code between SUIT Manifest Processors and other layers is desirable.
• HPKE is not adopted in COSE.
  • In the future we should consider HPKE, once a COSE+HPKE RFC is published.
• ECDH-ES is available now.
CDDL Profile

• Other specifications need to reference SUIT-MTI
• The SUIT MTI CDDL provides a COSE Envelope
  • CDDL intersection used to restrict algorithms to MTI algorithms
• Accepted algorithm IDs defined in the profile