draft-ietf-suit-mti-06

ietf 120

Status

- No major changes
- No known issues

Changes

- Change summary
  - Corrected error in MTI number assignment
  - When ECDH-ES+HKDF was changed to ECDH-ES+A128KW, the algorithm identifier was not changed. This change corrects the algorithm identifier.

Summary

- Defines 6 algorithm profiles in 4 groups:
- Symmetric (very constrained)
  - SHA256 + HMAC + A128KW + A128CTR
- Current
  - SHA256 + ES256 + ECDH-ES + A128KW + A128CTR
  - SHA256 + EDDSA + ECDH-ES + A128KW + A128CTR
- Current-AEAD
  - SHA256 + ES256 + ECDH-ES + A128KW + A128GCM
  - SHA256 + EDDSA + ECDH-ES + A128KW + ChaCha20/Poly1305
- Future Asymmetric (constrained)
  - SHA256 + HSS-LMS + A128KW + A256CTR