Registering algorithms for encryption without MAC?

COSE, IETF 110

Göran Selander

Encrypt without MAC in COSE?

- Current COSE IANA register only contains AE or AEAD algorithms

- E.g. section 8.3 Content Encryption Algorithms in https://tools.ietf.org/html/draft-ietf-cose-rfc8152bis-struct-15:

  "COSE restricts the set of legal content encryption algorithms to those that support authentication both of the content and additional data."

- But there are settings where COSE could be used in a secure way with encryption decoupled from MAC

- **Request for guidance from WG:**
  Shall we allow IANA registration of encryption algorithms without MAC for COSE?

Request from FIDO Alliance

- FIDO Alliance has requested COSE IANA registration of AES-128-CBC, AES-256-CBC, AES-128-CTR and COSE AES-256-CTR for supporting legacy hardware
  - https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-RD-v1.0-20201202.html
  - One instance of use: COSE_encrypt0 wrapped in COSE_MAC0

(This is the second request for COSE algorithm registration from FIDO Alliance. Previous request resulted in RFC 8812.)

Other use for COSE with encrypt without MAC

- EDHOC message_2
  - Not using COSE/AEAD because would increase overhead without improving security
  - SIGMA security proof only requires ENC without integrity

- Group OSCORE
  - Current use: AEAD || SIG(AEAD)
  - Would improve security and reduce overhead with: ENC || SIG(ENC + MAC)