

# **AES-CMAC For COSE**

**IETF 125 COSE WG**

Brian Sipos  
JHU/APL

# Background

- The current IANA registry for COSE algorithms includes AES-based CBC MAC

Name	Value	Key Length	Tag Length	Description
AES-MAC 128/64	14	128	64	AES-MAC 128-bit key, 64-bit tag
AES-MAC 256/64	15	256	64	AES-MAC 256-bit key, 64-bit tag
AES-MAC 128/128	25	128	128	AES-MAC 128-bit key, 128-bit tag
AES-MAC 256/128	26	256	128	AES-MAC 256-bit key, 128-bit tag

Table 4: AES-MAC Algorithm Values

- These algorithms, while functionally fine, are not approved by FIPS-140
  - This limitation creates a barrier to use in systems which either mandate or benefit from FIPS approval
- Use of AES block cipher with CMAC (NIST SP 800-38B) is FIPS approved
  - AES-CMAC is already supported in [IPsec](#), [IEEE 802.16](#), and the baseline mode of [CCSDS SDLS](#)
- Earlier COSE mailing list discussion mentioned alternative use of CMAC but did not reach any conclusion, so CBC MAC was the registered family
  - In 2018: <https://mailarchive.ietf.org/arch/msg/cose/yiLtOdsw6RXC-iHdNHJKGWgfUEs/>
  - In 2015: [https://mailarchive.ietf.org/arch/msg/cose/GwP\\_6EgbzTkzXGh36WhX0nomhT8/](https://mailarchive.ietf.org/arch/msg/cose/GwP_6EgbzTkzXGh36WhX0nomhT8/)

# Proposed Registrations

- Personal draft in [draft-sipos-cose-cmac-00](#)
- Registers fully specified COSE Algorithm entries to mirror existing non-truncated-tag AES-MAC entries

COSE Value	Algorithm	Key Length	Tag Length
TBA1	AES-CMAC	128	128
TBA3	AES-CMAC	256	128

Table 1: Registered AES-CMAC combinations

- AES-CMAC 256/128 also conforms to CNSA 1.0 and 2.0
- Expected use of this algorithm is with COSE\_Mac0 for an “inline authenticator”
  - Similar in form and concept with an “inline encryptor”
- Because this family is based on AES block cipher, it has wide support for hardware/firmware acceleration including in commodity hardware
  - Able to support high-rate and high-volume MAC processing
- This family was offered as a possibility to the JOSE WG as well, but there was not any interest from that WG in high-rate, high-volume MAC use

# Next Steps

- Registration of COSE algorithms is Standards Action for values between -256 and 255
  - This small encoded size (1+1) is desirable for MAC algorithms
  - Values 35-255 are currently unregistered
- Pursuing this registration through COSE WG seems natural
- No algorithm customization is done with this registration
  - No security analysis seems necessary
- Thoughts about WG adoption?