JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

AES-GMAC For COSE

IETF 122 COSE WG

Brian Sipos
JHU/APL

Background

- The current IANA registry for COSE algorithms includes GCM-based AEAD

Name	Value	Description
A128GCM	1	AES-GCM mode w/ 128-bit key, 128-bit tag
A192GCM	2	AES-GCM mode w/ 192-bit key, 128-bit tag
A256GCM	3	AES-GCM mode w/ 256-bit key, 128-bit tag

Table 5: Algorithm Values for AES-GCM

- Part of GCM is a MAC behavior, and when used without any plaintext GCM behaves as a “nonce-based MAC” called GMAC
  - This means GMAC provides equivalent authentication to GCM on which it is based
- When used with the AES block cipher, this technique is called AES-GMAC
- As a nonce-based MAC, each use requires a unique key-and-IV combination
  - This needed IV parameter is unique among other MAC algorithms
- Because this is based on AES-GCM, it has wide support for hardware/firmware acceleration including in commodity hardware
  - Able to support high-rate and high-volume MAC processing

Proposed Registrations

- Personal draft in draft-sipos-cose-gmac-00 - AES-GMAC for COSE
- Registers fully specified COSE Algorithm entries to mirror existing AES-GCM entries

COSE Value	Algorithm	Key Length	IV Length	Tag Length
TBA1	AES-GMAC	128	96	128
TBA2	AES-GMAC	192	96	128
TBA3	AES-GMAC	256	96	128

Table 1: Registered AES-GMAC combinations

- Expected use of this algorithm is with COSE_MAC0 for an “inline authenticator”
  - Similar in form and concept with an “inline encryptor”
  - Will make use of existing COSE headers related to IV (5) and Partial IV (6)
- This was offered as a possibility to JOSE WG as well, but there was not any interest from that WG in high-rate, high-volume GMAC use

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY