CBOR Object Signing and Encryption
Internet-Draft
Intended status: Informational
Expires: 2 July 2026

B. Sipos
JHU/APL

29 December 2025

AES-CMAC for COSE
draft-sipos-cose-cmac-00

Abstract

This document registers COSE algorithm code points for using the Advanced Encryption Standard (AES) in Cipher-based Message Authentication Code (CMAC) mode for use in CBOR Object Signing and Encryption (COSE) messages. The CMAC mode of operation is an alternative to AES-CBC-MAC which is approved by US NIST FIPS 140.

Table of Contents

1. Introduction

The base CBOR Object Signing and Encryption (COSE) specification [RFC9052] defines a container for Message Authentication Code (MAC) parameters and results. This container is parameterized on an algorithm identifier used to verify the MAC result. This document defines new fully specified algorithm identifiers for the use of Advanced Encryption Standard (AES) in Cipher-based Message Authentication Code (CMAC) mode to generate an authentication tag as defined by US NIST [SP800-38B].

These COSE algorithm identifiers are "fully specified" meaning they rely on no extra parameters (_e.g._, key length or tag length) to determine their exact operation. The COSE algorithm code point along with the shared secret key is suffient to generate or verify the MAC tag.

The use of CMAC is an alternative to the Hash-based Message Authentication Code (HMAC) family of algorithms which relies exclusively on a block cipher instead of a cryptographic hash function. For some implementations, cipher-based MAC can enable the use of hardware acceleration of its processing. The CMAC mode of AES is approved by US NIST FIPS 140 [FIPS-140].

1.1. Scope

This document does not define any new algorithms it only defines code points in a COSE registry so that the AES-CMAC can be used in that security environment with fully specified combinations of parameters.

To avoid confusion, the AES-CMAC algorithm family specified in this document is distinct from the "AES-MAC" (also known as "AES-CBC-MAC") algorithm family from Section 3.2 of [RFC9053]. That algorithm family is not approved by FIPS 140.

1.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. The AES-CMAC Family

While the CMAC mode [SP800-38B] can be used with any underlying encryption block cipher, this document focuses on its use with the AES cipher referred to as AES-CMAC.

For the sake of adhering to COSE best practice about fully specifying what gets assigned a COSE "algorithm" code point, AES-CMAC will be treated as an _algorithm family_ with a single code point referring to the algorithm itself along with a specific set of parameter values. The parameters associated with AES-CMAC are: key length and tag length.

This document restricts the allocated code points to the commonly used key lengths of 128 and 256 bits and restricts the use of a single tag length of 128 bits, which happens to be the longest possible tag length, as indicated in Table 1. These tag lengths are consistent with the COSE use of AES-CBC-MAC in Section 3.2 of [RFC9053]. Future allocations can define the use of AES-CMAC with shortened tag lengths.

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

Table 1: Registered AES-CMAC combinations

When using a COSE key for these algorithms, the following checks are made:

* The "kty" field MUST be present with a value of "Symmetric".

* The "k" field MUST match the key length for the algorithm being used.

* If the "alg" field is present, it MUST match the algorithm being used.

* If the "key_ops" field is present, it MUST include "MAC create" when creating an authentication tag.

* If the "key_ops" field is present, it MUST include "MAC verify" when verifying an authentication tag.

3. Security Considerations

This document does not define any new behavior of the AES-CMAC family, and so does not introduce any new security considerations. All of the applicable considerations from NIST [SP800-38B] apply when the algorithm is used in COSE.

4. IANA Considerations

This section provides guidance to the Internet Assigned Numbers Authority (IANA) regarding registration of code points in accordance with BCP 26 [RFC8126].

4.1. COSE Algorithms

A new set of entries have been added to the "COSE Algorithms" registry [IANA-COSE] with the following parameters.

Name: AES-CMAC 128/128

Value:
// TBA1

Description: AES-CMAC with 128-bit key and 128-bit tag

Capabilities: [kty]

Change controller: IETF

Reference: [This document]

Recommended: Yes

Name: AES-CMAC 256/128

Value:
// TBA3

Description: AES-CMAC with 256-bit key and 128-bit tag

Capabilities: [kty]

Change controller: IETF

Reference: [This document]

Recommended: Yes

// Note to IANA: The reqested COSE algorithm code points are in the
// positive less-than-256 range.

5. References

5.1. Normative References

[IANA-COSE] IANA, "CBOR Object Signing and Encryption (COSE)", <https://www.iana.org/assignments/cose/>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/info/rfc9052>.

[SP800-38B] US National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", NIST SP 800-38B, May 2005, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf>.

5.2. Informative References

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/info/rfc9053>.

[FIPS-140] US National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules", FIPS 140-3, March 2019, <https://doi.org/10.6028/NIST.FIPS.140-3>.

Author's Address

Brian Sipos
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Rd.
Laurel, MD 20723
United States of America
Email: brian.sipos+ietf@gmail.com