CBOR Object Signing and Encryption
Internet-Draft
Intended status: Informational
Expires: 11 October 2026

B. Sipos
JHU/APL

9 April 2026

AES-CMAC for COSE
draft-sipos-cose-cmac-02

Abstract

The CBOR Object Signing and Encryption (COSE) specification defines structures for generating, conveying, and verifying Message Authentication Code (MAC) tags. This document registers code points for using the Advanced Encryption Standard (AES) block cipher in Cipher-based Message Authentication Code (CMAC) mode within those COSE structures. Specifically, these uses are for computing MAC tag values with no additional parameters.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 11 October 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The base CBOR Object Signing and Encryption (COSE) specification [RFC9052] defines two message types for Message Authentication Code (MAC) parameters and results: COSE_Mac and COSE_Mac0. These messages are parameterized on an algorithm identifier used to generate and verify the MAC tag. This document defines new fully specified COSE algorithm code points for the use of Advanced Encryption Standard (AES) block cipher [FIPS-197] in Cipher-based Message Authentication Code (CMAC) mode [SP800-38B] to compute a MAC tag.

These COSE algorithm code points are "fully specified" in accordance with [RFC9864], meaning they rely on no extra parameters to determine their exact operation. The COSE algorithm code point along with the shared secret key is sufficient 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 registered by the base COSE specification in Section 3.1 of [RFC9053]. CMAC relies exclusively on a block cipher instead of the HMAC use of a cryptographic hash function. For some implementations, cipher-based MAC can be hardware accelerated.

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].

1.1. Scope

This document does not define any new cryptographic algorithms or functions. It only defines code points in a COSE registry so that the AES-CMAC algorithm family can be used in COSE messages.

This document does not address the use of CMAC for any other purposes than to compute a fixed-length MAC tag. These registered code points are not to be used as a pseudorandom function (PRF) or key-derivation function (KDF).

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 [RFC9864] about fully specifying what gets assigned a COSE "algorithm" code point, AES-CMAC will be treated as an _algorithm family_ with a single COSE code point referring to the algorithm family along with a specific set of parameter values. The parameters associated with AES-CMAC family are: key length and tag length.

This document registers code points for the commonly used key lengths of 128 and 256 bits and tag lengths of 96 and 128 bits. The 128-bit tag happens to be the longest possible tag length while the 96-bit tag is a truncated form. These tag lengths are consistent with the use cases for single-use keys and limited-use keys (see Section 3.1) and with the use of AES-CMAC in IPsec [RFC4494].

Name	COSE Value	Algorithm Family	Key Length	Tag Length
AES-CMAC 128/96	// TBA1	AES-CMAC	128	96
AES-CMAC 256/96	// TBA2	AES-CMAC	256	96
AES-CMAC 128/128	// TBA3	AES-CMAC	128	128
AES-CMAC 256/128	// TBA4	AES-CMAC	256	128

Table 1: Registered algorithm code points

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, so all of the applicable considerations of AES [FIPS-197] and CMAC [SP800-38B] apply when the algorithm family is used in COSE.

The CMAC mode of AES is approved by US NIST FIPS 140 [FIPS-140]. The pre-existing uses of AES-CBC-MAC in COSE [RFC9053] are not approved by FIPS 140.

3.1. Key Overuse Limit

From analysis of Appendix B of [SP800-38B] performed in 2024 [Ericsson], an "effective tag length" in bits can be computed for the 128-bit AES block length as

T_eff = 128 - 2 * log2(q)

where the factor "q" is the message span of each key (number of messages for which a tag is generated).

This means that only for single-use keys is the effective tag length is the actual tag length. For the NIST recommended limit of q = 2^48, the effective tag length becomes shortened to only 48 bits.

The analysis itself [Ericsson] recommends an effective tag length no less than 64 bits (_i.e._, equivalent to a 64-bit ideal MAC). This translates to a message span limit of q < 2^32, meaning a single key is limited to generate MAC tags for fewer than 2^32 messages. For a 96-bit effective tag length, the limit becomes fewer than 2^16 messages.

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 128/96

Value:
   // TBA1

Description: AES-CMAC with 128-bit key and 96-bit tag

Capabilities: [kty]

Change controller: IETF

Reference: [This document]

Recommended: Yes

Name: AES-CMAC 256/96

Value:
// TBA2

Description: AES-CMAC with 256-bit key and 96-bit tag

Capabilities: [kty]

Change controller: IETF

Reference: [This document]

Recommended: Yes

Name: AES-CMAC 128/128

Value:
// TBA3

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 requested COSE algorithm code points are in the
// positive less-than-256 range.

5. References

5.1. Normative References

[FIPS-197] US National Institute of Standards and Technology, "The Advanced Encryption Standard (AES)", FIPS 197, 26 November 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[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

[Ericsson] Mattsson, J. P., "Comments on SP 800-38B and SP 800-38C", 14 September 2024, <https://emanjon.github.io/NIST-comments/2024%20-%20SP%20800-38B%20and%20800-38C.pdf>.

[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>.

[RFC4494] Song, JH., Poovendran, R., and J. Lee, "The AES-CMAC-96 Algorithm and Its Use with IPsec", RFC 4494, DOI 10.17487/RFC4494, June 2006, <https://www.rfc-editor.org/info/rfc4494>.

[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>.

[RFC9864] Jones, M.B. and O. Steele, "Fully-Specified Algorithms for JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE)", RFC 9864, DOI 10.17487/RFC9864, October 2025, <https://www.rfc-editor.org/info/rfc9864>.

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