Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 19, 2019

J. Schaad
August Cellars

February 15, 2019

# CBOR Object Signing and Encryption (COSE): Hash Algorithms
## draft-schaad-cose-hash-algs-00

## Abstract

The CBOR Object Signing and Encryption (COSE) syntax [I-D.ietf-cose-rfc8152bis-struct] does not define any direct methods for using hash algorithms. There are however circumstances where hash algorithms are used: Indirect signatures where the hash of one or more contents are signed. X.509 certificate or other object identification by the use of a thumbprint. This document defines a set of hash algorithms that are identified by COSE Algorithm Identifiers.

## Note

The source for this draft is being maintained in GitHub. Suggested changes should be submitted as pull requests at TBD. Editorial changes can be managed in GitHub, but any substantial issues need to be discussed on the COSE mailing list.

## Status of This Memo

Table of Contents

1. . . . . 2
1.1. . . . . 3
1.2. . . . . 3
2. . . . . 3
2.1. . . . . 3
3. . . . . 3
3.1. . . . . 3
4. . . . . 4
5. References . . . . . 4
5.1. Normative References . . . . . 4
5.2. Informative References . . . . . 4
Author's Address . . . . . 4

1.

The CBOR Object Signing and Encryption (COSE) syntax does not define any direct methods for the use of hash algorithms. It also does not define a structure syntax that is used to encode a digested object structure along the lines of the DigestedData ASN.1 structure in [RFC5652]. This omission was intentional as a structure consisting of jut a digest identifier, the content, and a digest value does not by itself provide any strong security service. Additional, an application is going to be better off defining this type of structure so that it can add any additional data that needs to be hashed as well as methods of obtaining the data.

While the above is true, there are some cases where having some standard hash algorithms defined for COSE with a common identifier makes a great deal of sense. Two of the cases where these are going to be used are:





Indirect signing of content is a paradigm where the content is not directly signed, but instead a hash of the content is computed and that hash value, along with the hash algorithm, is included in the content that will be signed. Doing indirect signing allows for the a signature to be validated without first downloading all of the content associated with the signature. This capability can be of even grater importance in a constrained environment as not all of the content signed may be needed by the device.

The use of hashes to identify objects is something that has been very common. One of the primary things that has been identified by a hash function for secure message is a certificate. Two examples of this can be found in [RFC2634] and the newly defined COSE equivalents in [I-D.ietf-cose-x509].

### 1.1.

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.

### 1.2.

## 2.

### 2.1.

The family of SHA-2 hash algorithms [FIPS-180-4] was designed by the United States National Security Agency and published in 2001. Since that time some additional algorithms have been added to the original set to deal with length extension attacks and some performance issues. While the SHA-3 hash algorithms has been published since that time, the SHA-2 algorithms are still broadly used.

There are a number of different parameters for the SHA-2 hash functions. The set of hash functions which have been chosen for inclusion in this document are based on those different parameters and some of the trade-offs involved.

3.

3.1.

IANA is requested to register the following algorithms in the "COSE Algorithms" registry.





4.

There are security considerations:

## 5. References

### 5.1. Normative References

[FIPS-180-4] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-4, August 2015.

[I-D.ietf-cose-rfc8152bis-struct] Schaad, J., "CBOR Object Signing and Encryption (COSE) - Structures and Process", draft-ietf-cose-rfc8152bis-struct-01 (work in progress), February 2019.

[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>.

### 5.2. Informative References

[RFC2634] Hoffman, P., Ed., "Enhanced Security Services for S/MIME",

RFC 2634, DOI 10.17487/RFC2634, June 1999,
<https://www.rfc-editor.org/info/rfc2634>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70,
RFC 5652, DOI 10.17487/RFC5652, September 2009,
<https://www.rfc-editor.org/info/rfc5652>.

## Author's Address

Jim Schaad
August Cellars

Email: ietf@augustcellars.com