Workgroup: Network Working Group
Published: 17 November 2019
Intended Status: Informational
Expires: 20 May 2020
Authors: J. Schaad
August Cellars

CBOR Object Signing and Encryption (COSE): Additional Algorithms

Abstract

The CBOR Object Signing and Encryption (COSE) syntax [I-D.ietf-cose-rfc8152bis-struct] allows for adding additional algorithms to the registries. This document adds one additional key wrap algorithm to the registry using the AES Wrap with Padding Algorithm [RFC5649].

Contributing to this document

This note is to be removed before publishing as an RFC.

The source for this draft is being maintained in GitHub. Suggested changes should be submitted as pull requests at https://github.com/cose-wg/X509 Editorial changes can be managed in GitHub, but any substantial issues need to be discussed on the COSE mailing list.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

1.1. Requirements Terminology

1.2. Open Issues

2. AES Key Wrap with Padding

2.1. Security Considerations for AES-KW with Padding

3. References

3.1. Normative References

Author's Address

1. Introduction

The CBOR Object Signing and Encryption (COSE) syntax [I-D.ietf-cose-rfc8152bis-struct] is defined to have an object based set of security primatives using CBOR [I-D.ietf-cbor-7049bis] for use in constrained environments. COSE has algorithm agility so that documents like this one can register algorithms which are needed.

In this document we add the AES Wrap with Padding algorithm to the registry and describe how to use it.

1.1. Requirements 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.

1.2. Open Issues

This section is to be removed before publishing as an RFC.

*A desire has been expressed to all for the use of AES Key Wrap with Padding as a content encryption algorithm. This is not

compatible with the requirement that all content encryption algorithms "support authentication of both the content and additional data." AES Key Wrap is an AE not an AEAD algorithm.

2. AES Key Wrap with Padding

The AES Key Wrap with Padding is defined in [RFC5649]. This algorithm uses an AES key to wrap a value that is a multiple of 8 bits. As such, it can be used to wrap not only the key sizes for the content encryption algorithms, but additionally it can be used to encrypt off size keys that can be used with the keyed hash functions or key derivation functions. The algorithm uses a single fixed parameter, the initial value. This value is fixed in section 3 of [RFC5649], this is a different value from that used for the AES Key Wrap algorithm of [RFC3394]. There are no public parameters that very on a per-invocation bases. This algorithm does not support additional data and thus the protected header field MUST be empty.

When using a COSE key for this algorithm, the following checks are made:

*The 'kty' field MUST be present, and it MUST be 'Symmetric'.

*If the 'alg' field is present, it MUST match the AES Key Wrap algorithm being used.

*If the 'key_ops' field is present, it MUST include 'encrypt' or 'wrap key' when encrypting.

*If the 'key_ops' field is present, it MUST include 'decrypt' or 'unwrap key' when decrypting.

Name	Value	Key Size	Description
A128KW-Pad	TBD1	128	AES Key Wrap w/padding and a 128-bit key
A192KW-Pad	TBD2	192	AES Key Wrap w/padding and a 192-bit key
A256KW-Pad	TBD3	256	AES Key Wrap w/padding and a 256-bit key

Table 1: AES Key Wrap Algorithm Values

2.1. Security Considerations for AES-KW with Padding

The shared secret needs to have some method to be regularly updated over time. The shared secret is the basis of trust.

3. References

3.1. Normative References

[I-D.ietf-cose-rfc8152bis-struct]

Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", Work in Progress, Internet-Draft, draft-ietf-cose-rfc8152bis-struct-06, 11 September 2019, <https://tools.ietf.org/html/draft-ietf-cose-rfc8152bis-struct-06>.

[I-D.ietf-cbor-7049bis]
Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", Work in Progress, Internet-Draft, draft-ietf-cbor-7049bis-07, 25 August 2019, <https://tools.ietf.org/html/draft-ietf-cbor-7049bis-07>.

[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>.

[RFC5649] Housley, R. and M. Dworkin, "Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm", RFC 5649, DOI 10.17487/RFC5649, September 2009, <https://www.rfc-editor.org/info/rfc5649>.

[RFC3394] Schaad, J. and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm", RFC 3394, DOI 10.17487/RFC3394, September 2002, <https://www.rfc-editor.org/info/rfc3394>.

Author's Address

Jim Schaad
August Cellars

Email: ietf@augustcellars.com