

CMS Content Types for CBOR
draft-schaad-cbor-content-01

Abstract

CBOR is becoming a widely used method of doing content encoding. CMS is still a widely used method of doing message based security. This document defines a set of content types for CMS that hold CBOR content.

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 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

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 March 3, 2020.

Copyright Notice

Copyright (c) 2019 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 Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	CBOR Content Type	2
3.	CBOR Sequence Content Type	3
4.	ASN.1 Module	3
5.	IANA Considerations	4
6.	Security Considerations	5
7.	Normative References	5
	Author's Address	6

[1.](#) Introduction

CBOR [[CBOR](#)] is a compact self describing binary encoding formation that is starting to be used in many different applications. One of the primary uses of CBOR is in the Internet of Things where the constrained nature means that having minimal size of encodings becomes very important. The use of the Cryptographic Message System (CMS) [[CMS](#)] is still one of the most common method for providing message based security, although in many cases the CBOR Object Signing and Encryption (COSE) [[COSE](#)] message based security system is starting to be used. Given that CBOR is going to be transported using CMS, it makes sense to define CMS content types for the purpose of denoting that the embedded content is CBOR. This document defines two new content types: CBOR Content Type and CBOR Sequence Content Type [[CBOR-SEQ](#)].

[2.](#) CBOR Content Type

[CBOR] defines an encoded CBOR item. This section defines a new content type for wrapping an encoded CBOR item in a CMS object.

The following object identifier identifies the CBOR content type:

```
id-ct-cbor OBJECT IDENTIFIER ::= { iso(1) member-body(2) usa(840)
                                     rsadsi(113549) pkcs(1) pkcs9(9) smime(16) ct(1) TBD1 }
```

The CBOR content type is intended to refer to a single object encoded using the CBOR encoding format [[CBOR](#)]. Nothing is stated about the

specific CBOR object that is included. CBOR can always be decoded to a tree as the encoding is self descriptive.

The CBOR content type is intended to be encapsulated in the signed data and auth-enveloped data, but can be included in any CMS wrapper. It cannot be predicted if the compressed CMS encapsulation will provide compression as the content may be binary rather than text.

[RFC7193] defined an optional parameter "innerContent" to allow for identification of what the inner content is for an application/cms media type. This document defines the string "cbor" as a new value that can be placed here when a CBOR content type is used.

3. CBOR Sequence Content Type

[CBOR-SEQ] defines a CBOR Sequence as a concatenation of zero or more CBOR objects. This section defines a new content type for wrapping a CBOR Sequence in a CMS object.

The following object identifier identifies the CBOR Sequence content type:

```
id-ct-cborSequence OBJECT IDENTIFIER ::= { iso(1) member-body(2) usa(840)
    rsadsi(113549) pkcs(1) pkcs9(9) smime(16) ct(1) TBD2 }
```

The CBOR Sequence content type is intended to refer to a sequence of objects encoded using the CBOR encoding format. The objects are concatenated without any markers delimiting the individual CBOR objects. Nothing is stated about the specific CBOR objects that are included. CBOR can always be decoded to a tree as the encoding is self descriptive.

The CBOR Sequence content type is intended to be encapsulated in the signed data and auth-enveloped data, but can be included in any CMS wrapper. It cannot be predicted if the compressed CMS encapsulation will provide compression as the content may be binary rather than text.

[RFC7193] defined an optional parameter "innerContent" to allow for identification of what the inner content is for an application/cms media type. This document defines the string "cborSequence" as a new value that can be placed here when a CBOR Sequence content type is used.

4. ASN.1 Module


```

CborContentTypes { iso(1) member-body(2) usa(840)
    rsadsi(113549) pkcs(1) pkcs9(9) smime(16) 0 id-mod-cbor-2019(TBD3) }
DEFINITIONS EXPLICIT TAGS ::=
BEGIN
IMPORTS

CONTENT-TYPE
FROM CryptographicMessageSyntax-2010
    { iso(1) member-body(2) us(840) rsadsi(113549)
      pkcs(1) pkcs-9(9) smime(16) modules(0) id-mod-cms-2009(58) }
;

id-ct-cbor OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) ct(1) TBD1 }

id-ct-cborSequence OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) ct(1) TBD2 }

-- Content is encoded directly and does not have any ASN.1 structure
ct-Cbor CONTENT-TYPE ::= { IDENTIFIED BY id-ct-cbor }

-- Content is encoded directly and does not have any ASN.1 structure
ct-CborSequence CONTENT-TYPE ::= { IDENTIFIED BY id-ct-cborSequence }

END

```

5. IANA Considerations

In the "SMI Security for S/MIME Module Identifier" registry, create a new entry to point to this document.

Decimal	Description	References
TBD3	id-mod-cbor-2019	[[This Document

Table 1

In the "SMI Security for S/MIME Content Types" registry, add two new entries for id-ct-cbor and id-ct-cborSequence that point to this document.

Decimal	Description	References
TBD1	id-ct-cbor	[[This Document]]
TBD2	id-ct-cborSequence	[[This Document]]

Table 2

In the table "CMS Inner Content Types" add two new entries:

Name	Object Identifier	Reference
cbor	1.2.840.113549.1.9.16.1.TBD	[[This Document]]
cborSequence	1.2.840.113549.1.9.16.1.TBD2	[[This Document]]

Table 3

6. Security Considerations

This document only provides identification for content types, it does not introduce any new security issues by itself. The new content types does mean that id-data does not need to be used to identify these content types and thus can reduce confusion.

7. Normative References

- [CBOR] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", [RFC 7049](https://www.rfc-editor.org/info/rfc7049), DOI 10.17487/RFC7049, October 2013, <<https://www.rfc-editor.org/info/rfc7049>>.
- [CBOR-SEQ] Bormann, C., "Concise Binary Object Representation (CBOR) Sequences", [draft-ietf-cbor-sequence-01](https://www.ietf.org/archive/id/draft-ietf-cbor-sequence-01) (work in progress), August 30, 2019, <<https://www.ietf.org/archive/id/draft-ietf-cbor-sequence-01>>.
- [CMS] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, [RFC 5652](https://www.rfc-editor.org/info/rfc5652), DOI 10.17487/RFC5652, September 2009, <<https://www.rfc-editor.org/info/rfc5652>>.
- [COSE] Schaad, J., "CBOR Object Signing and Encryption (COSE)", [RFC 8152](https://www.rfc-editor.org/info/rfc8152), DOI 10.17487/RFC8152, July 2017, <<https://www.rfc-editor.org/info/rfc8152>>.

[RFC7193] Turner, S., Housley, R., and J. Schaad, "The application/cms Media Type", [RFC 7193](#), DOI 10.17487/RFC7193, April 2014, <<https://www.rfc-editor.org/info/rfc7193>>.

Author's Address

Jim Schaad
August Cellars

Email: ietf@augustcellars.com