Internet Engineering Task Force (IETF)
Request for Comments: 8769
Category: Informational
ISSN: 2070-1721

J. Schaad
August Cellars

March 2020

Cryptographic Message Syntax (CMS) Content Types for Concise Binary Object Representation (CBOR)

Abstract

Concise Binary Object Representation (CBOR) is becoming a widely used method of doing content encoding. The Cryptographic Message Syntax (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.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8769.

Table of Contents

1. Introduction

Concise Binary Object Representation (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, the constrained nature of which means that having minimal size of encodings becomes very important. The Cryptographic Message Syntax (CMS) [CMS] is still one of the most common methods 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) 44 }
```

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 it can be included in any CMS wrapper. It cannot be predicted whether the compressed CMS encapsulation will provide compression, because 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 in this parameter 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)
        45 }
```

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, because the encoding is self descriptive.

The CBOR Sequence content type is intended to be encapsulated in the signed data and auth-enveloped data, but it can be included in any CMS wrapper. It cannot be predicted whether the compressed CMS encapsulation will provide compression, because 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 in this parameter 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) modules(0)
        id-mod-cbor-2019(71) }
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)
        44 }

    id-ct-cborSequence OBJECT IDENTIFIER ::= { iso(1) member-body(2)
        us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) ct(1)
        45 }

    -- 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

IANA has registered the following in the "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)" subregistry within the SMI Numbers registry:

Decimal	Description	References
71	id-mod-cbor-2019	RFC 8769

Table 1

IANA has registered the following in the "SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)" subregistry within the SMI Numbers registry:

Decimal	Description	References
44	id-ct-cbor	RFC 8769
45	id-ct-cborSequence	RFC 8769

Table 2

IANA has registered the following in the "CMS Inner Content Types" subregistry within the "MIME Media Type Sub-Parameter Registries":

Name	Object Identifier	Reference
cbor	1.2.840.113549.1.9.16.1.44	RFC 8769
cborSequence	1.2.840.113549.1.9.16.1.45	RFC 8769

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 mean that id-data does not need to be used to identify these content types; they can therefore reduce confusion.

7. Normative References

[CBOR] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[CBOR-SEQ] Bormann, C., "Concise Binary Object Representation (CBOR) Sequences", RFC 8742, DOI 10.17487/RFC8742, February 2020,

            <https://www.rfc-editor.org/info/rfc8742>.

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

   [COSE]   Schaad, J., "CBOR Object Signing and Encryption (COSE)",
              RFC 8152, 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