Network Working Group
Internet-Draft
Intended status: Informational
Expires: 27 September 2019

J. Schaad
August Cellars

26 March 2019

CMS Content Types for CBOR
draft-schaad-cbor-content-00

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

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 27 September 2019.

Copyright Notice

provided without warranty as described in the Simplified BSD License.

Table of Contents

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 the most common method for providing message based security, although in many cases the CBOR Object Signing and Encryption (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.

2. CBOR Content Type

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) pkcs7(7) (x) TBD }
```

The CBOR content type is intended to refer to a single object encoded using the CBOR encoding format. 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.

3. CBOR Sequence Content Type

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) TBD }
```

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.

4. ASN.1 Module

```
CborContentTypes
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) TBD }

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

    -- 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.

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.

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, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[CMS] 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