RATS Working Group H. Birkholz
Internet-Draft Fraunhofer SIT
Intended status: Standards Track N. Cam-Winget
Expires: September 10, 2020 Cisco Systems
C. Bormann
Universitaet Bremen TZI
March 09, 2020

A CBOR Tag for Unprotected CWT Claims Sets
draft-birkholz-rats-uccs-00

Abstract

CBOR Web Token (CWT, RFC 8392) Claims Sets sometimes do not need the protection afforded by wrapping them into COSE, as is required for a true CWT. This specification defines a CBOR tag for such unprotected CWT claims sets (UCCS) and discusses conditions for its proper use.

Table of Contents

1. Introduction

A CBOR Web Token (CWT) as specified by [RFC8392] is always wrapped in a CBOR Object Signing and Encryption (COSE, [RFC8152]) envelope. COSE provides - amongst other things - the integrity protection mandated by RFC 8392 and optional encryption for CWTs. Under the right circumstances, though, a signature providing proof for authenticity and integrity can be omitted from the information in a CWT without compromising the intended goal of authenticity and integrity. If a secure channel is established in an appropriate fashion between two remote peers, and if that secure channel provides the correct properties, it is possible to omit the protection provided by COSE, creating a use case for unprotected CWT Claims Sets.

This specification allocates a CBOR tag to mark Unprotected CWT Claims Sets (UCCS) as such and discusses conditions for its proper use.

This specification does not change [RFC8392]: A true CWT does not make use of the tag allocated here; the UCCS tag is an alternative to using COSE protection and a CWT tag.

1.1. Terminology

The terms Claim and Claims Set are used as in [RFC8392].

UCCS: Unprotected CWT Claims Set

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.

2. Characteristics of a Secure Channel

A Secure Channel for the conveyance of UCCS needs to provide the security properties that would otherwise be provided by COSE for a CWT.

Secure Channels are often set up in a handshake protocol that agrees a session key, where the handshake protocol establishes the authenticity of one of both ends of the communication as well as confidentiality. The session key can then be used to protect confidentiality and integrity of the transfer of information inside the secure channel. A well-known example of a such a secure channel setup protocol is the TLS [RFC8446] handshake; the TLS record protocol can then be used for secure conveyance.

If only authenticity/integrity is required, the secure channel needs to be set up with authentication of the side that is providing the UCCS. If confidentiality is also required, the receiving side also needs to be authenticated.

3. IANA Considerations

In the registry [IANA.cbor-tags], IANA is requested to allocate the tag in Table 1 from the FCFS space, with the present document as the specification reference.

Tag	Data Item	Semantics
TBD601	map	Unprotected CWT Claims Set [RFCthis]

Table 1: Values for Tags

4. Security Considerations

The security considerations of [RFC7049] and [RFC8392] apply.

{#secchan} discusses security considerations for secure channels, in which UCCS might be used.

5. References

5.1. Normative References

[IANA.cbor-tags]
IANA, "Concise Binary Object Representation (CBOR) Tags", <http://www.iana.org/assignments/cbor-tags>.

[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>.

[RFC7049] 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>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[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>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

5.2. Informative References

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

Appendix A. Example

The example CWT Claims Set from Appendix A.1 of [RFC8392] can be turned into an UCCS by enclosing it with a tag number TBD601:

```
<TBD601>(
  {
    / iss / 1: "coap://as.example.com",
    / sub / 2: "erikw",
    / aud / 3: "coap://light.example.com",
    / exp / 4: 1444064944,
    / nbf / 5: 1443944944,
    / iat / 6: 1443944944,
    / cti / 7: h'0b71'
  }
)
```

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295
Germany

Email: henk.birkholz@sit.fraunhofer.de

Nancy Cam-Winget
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
USA

Email: ncamwing@cisco.com

Carsten Bormann
Universitaet Bremen TZI
Bibliothekstrasse 1
Bremen 28369
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.de