

COSE  
Internet-Draft  
Intended status: Standards Track  
Expires: 2 September 2022

T. Looker  
Mattr  
M. Jones  
Microsoft  
1 March 2022

CBOR Web Token (CWT) Claims in COSE Headers  
draft-looker-cose-cwt-claims-in-headers-00

## Abstract

This document describes how to include CBOR Web Token (CWT) claims in the header parameters of any COSE structure. This functionality helps to facilitate applications that wish to make use of CBOR Web Token (CWT) claims in encrypted COSE structures and/or COSE structures featuring detached signatures, while having some of those claims be available before decryption and/or without inspecting the detached payload.

## Discussion Venues

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

Source for this draft and an issue tracker can be found at <https://github.com/tplooker/draft-looker-cose-cwt-claims-in-headers>.

## 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 2 September 2022.

## Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Representation . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Privacy Considerations . . . . .	<a href="#">3</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">3</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">3</a>
<a href="#">7.</a>	Normative References . . . . .	<a href="#">3</a>
<a href="#">8.</a>	Informative References . . . . .	<a href="#">3</a>
<a href="#">Appendix A.</a>	Document History . . . . .	<a href="#">4</a>
	Authors' Addresses . . . . .	<a href="#">4</a>

## [1.](#) Introduction

In some applications of COSE, it is useful to have a standard representation of CWT claims [[RFC8392](#)] available in the header parameters. These include encrypted COSE structures, which may or may not be an encrypted CWT and/or those featuring a detached signature.

[Section 5.3](#) of the JWT RFC [[RFC7519](#)] defined a similar mechanism for expressing selected JWT based claims as JOSE header parameters. This JWT feature was motivated by the desire to have certain claims, such as Key ID values, be visible to software processing the JWT, even though the JWT is encrypted. No corresponding feature was standardized for CWTs, which was an omission that this specification corrects.

Directly including CWT claim values as COSE header parameter values would not work, since there are conflicts between the numeric header parameter assignments and the numeric CWT claim assignments. Instead, this specification defines a single header parameter registered in the IANA "COSE Header Parameters" registry that creates

a location to store CWT claims in a COSE header parameter.

## [2.](#) Terminology

## [3.](#) Representation

This document defines the following COSE header parameter:

Name	Label	Value Type	Value Registry	Description
cwt claims	TBD (requested assignment 11)	map	[ <a href="#">IANA.CWT</a> ]	location for CWT claims in COSE headers

Table 1

## [4.](#) Privacy Considerations

Some of the registered CWT claims may contain privacy-sensitive information. Therefore care must be taken when expressing CWT claims in COSE headers.

## [5.](#) Security Considerations

In cases where CWT claims are both present in the payload and the header, an application receiving such as structure **MUST** verify that their values are identical, unless the application defines other specific processing rules for these claims.

## [6.](#) IANA Considerations

IANA is requested to register the new COSE Header parameter in the table in [Section 3](#) in the "COSE Header Parameters" registry [[IANA.COSE](#)].

## 7. Normative References

[IANA.COSE]

IANA, "COSE Header Parameters",  
<<https://www.iana.org/assignments/cose/cose.xhtml#header-parameters>>.

[IANA.CWT] IANA, "CBOR Web Token (CWT) Claims",

<<https://www.iana.org/assignments/cwt/cwt.xhtml>>.

## 8. Informative References

Looker & Jones

Expires 2 September 2022

[Page 3]

---

Internet-Draft    CBOR Web Token (CWT) Claims in COSE Head

March 2022

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", [RFC 7519](#), DOI 10.17487/RFC7519, May 2015, <<https://www.rfc-editor.org/info/rfc7519>>.

[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>>.

## Appendix A. Document History

-00

\* Initial version

### Authors' Addresses

Tobias Looker  
Mattr  
Email: [tobias.looker@mattr.global](mailto:tobias.looker@mattr.global)

Michael B. Jones  
Microsoft  
Email: [mbj@microsoft.com](mailto:mbj@microsoft.com)  
URI: <https://self-issued.info/>

