Internet Engineering Task Force (IETF)
Request for Comments: 9597
Category: Standards Track
ISSN: 2070-1721

T. Looker
Mattr
M.B. Jones
Self-Issued Consulting

June 2024

CBOR Web Token (CWT) Claims in COSE Headers

Abstract

This document describes how to include CBOR Web Token (CWT) claims in the header parameters of any CBOR Object Signing and Encryption (COSE) structure. This functionality helps to facilitate applications that wish to make use of 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. Another use case is using CWT claims with payloads that are not CWT Claims Sets, including payloads that are not CBOR at all.

Status of This Memo

This is an Internet Standards Track document.

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). Further information on Internet Standards is available in 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/rfc9597.

Table of Contents

Authors' Addresses

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. Another use case is using CWT claims with payloads that are not CWT Claims Sets, including payloads that are not CBOR at all. For instance, an application might want to include an "iss" (issuer) claim in a COSE_Sign1 structure when the payload being signed is a non-CBOR data structure, such as a bitmap image, and the issuer value is used for key discovery.

Section 5.3 of [RFC7519], "JSON Web Token (JWT)", defined a similar mechanism for expressing selected JWT-based claims as JSON Object Signing and Encryption (JOSE) header parameters. This JWT feature was motivated by the desire to have certain claims, such as the Issuer value, 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.

This specification does not define how to use CWT claims and their semantics for particular applications, whether they are in the COSE payload or the CWT Claims header parameter, or both. Therefore, understanding how to process the CWT Claims header parameter requires unambiguously knowing the intended interpretation. The necessary information about this MAY come from other header parameters. Unless there already is a natural way of providing this information at an appropriate level of integrity protection and authentication, a RECOMMENDED way to include this information in the COSE structure is use of the "typ" (type) Header Parameter [RFC9596]. Other methods for determining the intended interpretation MAY also be used. Recipients of the CWT Claims header parameter MUST NOT use the information in the CWT Claims header parameter beyond the integrity protection or authentication afforded to the CWT Claims header and the information used to derive its intended interpretation.

1.1. Requirements Terminology

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. Representation

This document defines the following COSE header parameter:

Name	Label	Value Type	Value Registry	Description	Reference
CWT Claims	15	map	map keys in [CWT.Claims]	Location for CWT Claims in COSE Header	Section 2 of RFC 9597

				Parameters	

Table 1

The following is a non-normative description for the value type of the CWT claim header parameter using CDDL [RFC8610].

```
CWT-Claims = {
 * Claim-Label => any
}

Claim-Label = int / text
```

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

It is RECOMMENDED that the CWT Claims header parameter only be used in a protected header to avoid the contents being malleable. The header parameter MUST only occur once in either the protected or unprotected header of a COSE structure.

The CWT Claims header parameter MAY be used in any COSE object using header parameters, such as COSE_Sign objects. Its use is not restricted to CWTs.

3. Privacy Considerations

Some of the registered CWT claims may contain privacy-sensitive information. Since CWT claims in COSE headers are not encrypted, when privacy-sensitive information is present in these claims, applications and protocols using them should ensure that these COSE objects are only made visible to parties for which it is appropriate for them to have access to this sensitive information.

4. Security Considerations

Implementers should also review the security considerations for CWT, which are documented in Section 8 of [RFC8392].

As described in [RFC9052], if the COSE payload is transported separately ("detached content"), then it is the responsibility of the application to ensure that it will be transported without changes.

The reason for applications to verify that CWT claims present in both the payload and the header of a CWT are identical, unless they define other specific processing rules for these claims, is to eliminate potential confusion that might arise by having different values for the same claim, which could result in inconsistent processing of such claims.

Processing information in claims prior to validating that their integrity is cryptographically secure can pose security risks. This is true whether the claims are in the payload or a header parameter. Implementers must ensure that any tentative decisions made based on previously unverified information are confirmed once the cryptographic processing has been completed. This includes any information that was used to derive the intended interpretation of the CWT claims parameter.

5. IANA Considerations

IANA has registered the new COSE header parameter "CWT Claims" defined in Table 1 in the "COSE Header Parameters" registry

[COSE.HeaderParameters].

6. References

6.1. Normative References

[COSE.HeaderParameters]
IANA, "COSE Header Parameters",
<https://www.iana.org/assignments/cose/>.

[CWT.Claims]
IANA, "CBOR Web Token (CWT) Claims",
<https://www.iana.org/assignments/cwt/>.

[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>.

[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>.

[RFC9596] Jones, M.B. and O. Steele, "CBOR Object Signing and Encryption (COSE) "typ" (type) Header Parameter", RFC 9596, DOI 10.17487/RFC9596, June 2024, <https://www.rfc-editor.org/info/rfc9596>.

6.2. Informative References

[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>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/info/rfc9052>.

Acknowledgements

We would like to thank Daisuke Ajitomi, Claudio Allocchio, Carsten Bormann, Laurence Lundblade, Ivaylo Petrov, Ines Robles, Orie Steele, Hannes Tschofenig, Paul Wouters, and Peter Yee for their valuable contributions to this specification.

Authors' Addresses

Tobias Looker
Mattr
Email: tobias.looker@mattr.global

Michael B. Jones
Self-Issued Consulting
Email: michael_b_jones@hotmail.com

URI: https://self-issued.info/