COSE WG
Internet-Draft
Intended status: Standards Track
Expires: 24 January 2026

C. Lemmons
Comcast

23 July 2025

Composite Token Claims
draft-lemmons-cose-composite-claims-01

Abstract

Composition claims are CBOR Web Token claims that define logical relationships between sets of claims.

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 24 January 2026.

Table of Contents

1. Introduction

Composition claims are claims defined for CBOR Web Tokens (CWTs) [RFC7519]. These claims include logical operators "or", "nor", and "and" as well as a wrapper that encrypts the values, but not the keys, of some claims.

2. 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.

This document reuses terminology from CWT [RFC7519] and COSE [RFC9052].

This term is defined by this specification:

Composition Claim A composition claim is a CWT claim that contains, as part of its value, one or more CWT claim sets.

3. Claims

Composition claims contain one or more claim sets.

In CWTs without composition claims, there is exactly one set of claims, so the acceptability of the claim set decides the acceptability of the CWT. However, this document defines multiple sets of claim sets, so it instead refers to accepting or rejecting claim sets. If the primary claim set is unacceptable, the CWT is unacceptable and MUST be rejected.

Some applications use tokens to convey information. For example, a token might simply have a subject claim that identifies the bearer and the relying party simply uses that as information, not necessarily as a means by which to provide or deny access or make some other kind of decision. In this context, the token simply describes all situations in which the token would accurately describe that situation.

Composition claims can be nested to an arbitrary level of depth. Implementations MAY limit the depth of composition nesting by rejecting CWTs with too many levels but MUST support at least four levels of nesting.

3.1. Logical Claims

These claims identify one or more sets of claims in a logical relation. The type of these claims is array and the elements of the array are maps that are themselves sets of claims.

For the following CDDL, Claims-Set is a map of claims as defined in [RFC8392]. It is described informatively in [draft-ietf-rats-eat] Appendix D.

3.1.1. or (Or) Claim

The "or" (Or) claim identifies one or more sets of claims of which at least one is acceptable. If every set of claims in an "or" claim would, when considered with all the other relevant claims, result in the claim set being rejected, the claim set containing the "or" claim MUST be rejected.

Use of this claim is OPTIONAL. The Claim Key [add key number] is used to identify this claim.

The "or" (OR) claim is described by the following CDDL:

```
$$Claims-Set-Claims //= ( or-claim-label => or-claim-value )
or-claim-label = TBD
or-claim-value = [ + Claims-Set ]
```

3.1.2. nor (Not Or) Claim

The "nor" (Nor) claim identifies one or more sets of claims of which none are acceptable. If any set of claims in a "nor" claim would, when considered with all other relevant claims, result in the claim set being accepted, the claim set containing the "nor" MUST be rejected.

This is the logical negation of the "or" claim.

Use of this claim is OPTIONAL. The Claim Key [add key number] is used to identify this claim.

The "nor" (NOR) claim is described by the following CDDL:

```
$$Claims-Set-Claims //= ( nor-claim-label => nor-claim-value )
nor-claim-label = TBD
nor-claim-value = [ + Claims-Set ]
```

3.1.3. and (And) Claim

The "and" (And) claim identifies one or more sets of claims of which all are acceptable. If any claim in an "and" claim would, when considered with all other relevant claims, result in the claim set being rejected, the claim set containing the "and" claim MUST be rejected.

The "and" claim is often unnecessary because a given claim set is only accepted when all its claims are acceptable. However, CBOR maps cannot have duplicate keys, so claims cannot be repeated more than once. The "and" claim is useful for claims that may be claimed multiple times, including the "or" and "nor" claims.

Use of this claim is OPTIONAL. The Claim Key [add key number] is used to identify this claim.

The "and" (AND) claim is described by the following CDDL:

```
$$Claims-Set-Claims //= ( and-claim-label => and-claim-value )
and-claim-label = TBD
and-claim-value = [ + Claims-Set ]
```

3.1.4. Examples

These logical claims can be used to describe more complex relationships between claims. For example, the following claim set describes a token with multiple subject claims. This token describes a situation where either of the two subjects must be true, but the issuer is not disclosing which one must be true or even whether the two subjects are genuinely different.

```
{
  /or/ TBD: [
    { /sub/ 2: "george@example.net" },
    { /sub/ 2: "harriet@example.net" }
  ]
}
```

A relying party that receives this token knows that bearer claims to be both George and Harriet and if either subject is acceptable, the token is acceptable.

The "nor" claim is useful both as a logical negation, even when only one claim is present. For example, consider the following claim set:

```
{
  /nor/ TBD: [
    { /aud/ 3: "https://example.com" }
  ]
}
```

This token is intended for any audience except "example.com".

Complex relationshops can also be described using the claims in combination. The "geohash" claim [CTA5009A] describes a geographical region. For example:

```
{
  { /aud/ 3: "https://example.com" },
  { /geohash/ 282: "9q8yy" },
  { /nor/ TBD: [
      { /geohash/ 282: ["9q8yy9", "9q8yyd"] }
    ]
  }
}
```

This token describes an audience of "https://example.com" (https://example.com") and a region described by the geohash of "9q8yy" that does not include the region described by "9q8yy9" or "9q8yyd".

And if a very complex relationship is required, the "and" claim can be used to combine multiple claims. For example, consider the following claim set:

```
{
  /and/ TBD: [
    {
      /or/ TBD: [
        { /sub/ 2: "george@example.net" },
        { /sub/ 2: "harriet@example.net" }
      ]
    },
    {
      /or/ TBD: [
        { /aud/ 3: "https://example.com" },
        { /aud/ 3: "https://example.net" }
      ]
    }
  ]
}
```

This admittedly contrived example describes a token that is valid for both George and Harriet and is intended for both https://example.com (https://example.com) and https://example.net (https://example.net). It is a bit contrived because the "aud" claim already describes a list of acceptable audiences. The use of the "and" claim is required in order to effectively repeat the "or" claim, because a single claim set cannot contain the same claim twice.

3.2. crit (Critical) Claim

The "crit" (Critical) claim lists the claims required to process this claim set.

The type of this claim is array and the elements of the array are strings, negative integers, or unsigned integers. The elements of the array correspond to claims that MUST be present in the token.

If a claim listed in the "crit" claim is present in a claim set and the processor cannot process the claim for any reason, the claim set MUST be rejected.

If a claim listed in the "crit" claim is not present in a claim set, the claim set MUST be rejected.

If a "crit" claim is present in a claim set, a processor SHOULD consider claims it does not understand to be acceptable if they are not present in the "crit" claim, unless application-specific

processing defines otherwise. That is, when a "crit" claim is present, any claims not listed may by default be assumed to be non-critical.

Use of this claim is OPTIONAL. The Claim Key [add key number] is used to identify this claim.

3.2.1. Example

A "crit" claim can be used in conjunction with logical claims to condition a portion of the token on the ability to process a claim:

```
{
  /or/ TBD: [
    { /geohash/ 282: "9q8y", /crit/ TBD: [ 282 ] },
    { /private/ -524289: "sf", /crit/ TBD: [ -524289 ] }
  ]
}
```

This example assumes the existance of some kind of claim in the private space that a relying party may or may not be able to process. This token claims that the subject is in the described region and also that a private claim is present and that the relying party must be able to verify at least one of those claims, but it does not need to be able to process both.

4. Security Considerations

All security considerations relevant to CWTs in general will apply to CWTs that use composition claims.

Additionally, processors of CWTs with composition claims will need to be aware of the possibility of receiving highly nested tokens. Excessive nesting can lead to overflows or other processing errors.

Additionally, there is a chicken-and-egg problem with the "crit" claim. A relying party that does not support the "crit" claim cannot be expected to enforce it to make other claims mandatory. As a result, an application that includes the "crit" claim in its CWT profile MUST make the correct processing of the claim REQUIRED for relying parties. It MAY be OPTIONAL for issuers. This allows the "crit" claim to be used to facilitate extensions and interoperability.

5. IANA Considerations

This specification requests that IANA register the following claim keys in the "CBOR Web Token (CWT) Claims" registry established by [RFC8392]:

Claim Name: or
Claim Description: Logical OR
JWT Claim Name: N/A
Claim Key: TBD (greater than 285)
Claim Value Type(s): array
Change Controller: IETF

Claim Name: nor
Claim Description: Logical NOR
JWT Claim Name: N/A
Claim Key: TBD (greater than 285)
Claim Value Type(s): array
Change Controller: IETF

Claim Name: and
Claim Description: Logical AND
JWT Claim Name: N/A
Claim Key: TBD (greater than 285)
Claim Value Type(s): array
Change Controller: IETF

Claim Name: crit
Claim Description: Critical Claims
JWT Claim Name: N/A
Claim Key: TBD (greater than 285)
Claim Value Type(s): array
Change Controller: IETF

6. References

6.1. Normative References

[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>.

[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>.

[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>.

[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>.

6.2. Informative References

[CTA5009A] Consumer Technology Association, "CTA 5009-A: Fast and Readable Geographical Hashing", 2024, <https://shop.cta.tech/products/fast-and-readable-geographical-hashing-cta-5009>.

Author’s Address

Chris Lemmons
Comcast
Email: chris_lemmons@comcast.com