COSE WG
Internet-Draft
Intended status: Standards Track
Expires: 21 August 2026

C. Lemmons
Comcast

17 February 2026

Composite Token Claims
draft-lemmons-cose-composite-claims-02

Abstract

Composition claims are claims for CBOR Web Tokens (CWTs) and JSON Web Tokens (JWTs) 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 21 August 2026.

Table of Contents

1. Introduction

Composition claims are claims defined for CBOR Web Tokens (CWTs) [RFC8392] and JSON Web Tokens (JWTs) [RFC7519].

This document defines the CWT representations of the composition claims named "and", "or", "nor". It also defines a CWT definition for "crit".

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 [RFC8392], JWT [RFC7519], and COSE [RFC9052].

This term is defined by this specification:

Composition Claim A claim whose value contains one or more claim sets.
Claim Set A set of claims. For CWTs this is a CBOR map. For JWTs this is a JSON object.

3. Claims

Composition claims contain one or more claim sets.

In tokens without composition claims, there is exactly one set of claims, so the acceptability of the claim set decides the acceptability of the token. However, this document defines multiple claim sets, so it instead refers to accepting or rejecting claim sets. If the primary claim set is unacceptable, the token 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 may be nested arbitrarily. Implementations MAY reject tokens exceeding an implementation-defined nesting depth but MUST support at least four levels.

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.

In CWTs, the value is a CBOR array of CBOR maps. In JWTs, the value is a JSON array of JSON objects.

For the following CDDL, Claims-Set is a map of claims as defined in [RFC8392]. It is described informatively in [RFC9711], Appendix D.

3.1.1. or (Or) Claim

The "or" (Or) claim identifies one or more claim sets of which at least one is acceptable. If none of the claim sets in an "or" claim is acceptable, the claim set containing the "or" claim is also unacceptable.

Use of this claim is OPTIONAL.

In JWTs, the Claim Name is "or" and the Claim Value is a JSON array of JSON objects.

In CWTs, the Claim Key is TBD (to be registered in the "CBOR Web Token (CWT) Claims" registry).

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 claim sets of which none are acceptable. If any claim set in a "nor" claim is acceptable, the claim set containing the "nor" claim is also unacceptable.

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

Use of this claim is OPTIONAL.

In JWTs, the Claim Name is "nor" and the Claim Value is a JSON array of JSON objects.

In CWTs, the Claim Key is TBD (to be registered in the "CBOR Web Token (CWT) Claims" registry).

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 claim sets of which all are acceptable. If any claim set in an "and" claim is not acceptable, the claim set containing the "and" claim is also unacceptable.

The "and" claim is often unnecessary because a claim set is only accepted when all its claims are acceptable. However, CBOR maps cannot have duplicate keys, so claims cannot be repeated. The "and" claim is useful when a claim needs to appear multiple times, like when using the "or" and "nor" claims.

Use of this claim is OPTIONAL.

In JWTs, the Claim Name is "and" and the Claim Value is a JSON array of JSON objects.

In CWTs, the Claim Key is TBD (to be registered in the "CBOR Web Token (CWT) Claims" registry).

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 following JWT claim set example is equivalent:

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

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".

The following JWT claim set example is equivalent:

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

Complex relationships 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 indicates critical extensions to this kind of claim set.

The semantics of the JWT claim name "crit" are defined by OpenID Federation 1.0 [OpenID-Federation]. This specification defines only the CWT representation.

The value of this claim is an array. Each element identifies a claim within the same claim set.

In CWTs, elements are integers or text strings identifying claim keys. The "crit" array MUST NOT be empty. Each element of the "crit" array MUST identify a claim that is present in the same claim set. Elements in the "crit" array MUST be unique.

Elements in the "crit" array MUST NOT identify claims that are specified as MANDATORY to understand for the token. This will vary by application profile as described in [RFC7519], Section 4. As noted in [OpenID-Federation], Section 13.4, any profile that requires correct processing of the "crit" claim MUST of necessity specify that it is MANDATORY to understand.

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. (TODO: Square this with the OpenID definition. The OpenID definition does not explicitly require claim sets to be rejected if the claim name rules like including duplicates, empty arrays, or the presence of claims that are not present in the claim set.)

Use of this claim is OPTIONAL.

In CWTs, the Claim Key is TBD (to be registered in the "CBOR Web Token (CWT) Claims" registry).

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 existence 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 and JWTs in general will apply to tokens that use composition claims.

Additionally, processors of tokens 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.

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: or
Claim Key: TBD
Claim Value Type(s): array
Change Controller: IESG

Claim Name: nor
Claim Description: Logical NOR
JWT Claim Name: nor
Claim Key: TBD
Claim Value Type(s): array
Change Controller: IESG

Claim Name: and
Claim Description: Logical AND
JWT Claim Name: and
Claim Key: TBD
Claim Value Type(s): array
Change Controller: IESG

Claim Name: crit
Claim Description: Critical Claims
JWT Claim Name: crit
Claim Key: TBD
Claim Value Type(s): array
Change Controller: IESG

This specification requests that IANA register the following claim names in the "JSON Web Token Claims" registry established by [RFC7519]:

Claim Name: or
Claim Description: Logical OR
Change Controller: IESG
Specification Document(s): This document

Claim Name: nor
Claim Description: Logical NOR
Change Controller: IESG
Specification Document(s): This document

Claim Name: and
Claim Description: Logical AND
Change Controller: IESG
Specification Document(s): This document

The JWT Claim Name "crit" is already registered in the "JSON Web Token Claims" registry and is defined by OpenID Federation 1.0 [OpenID-Federation].

6. References

6.1. Normative References

[OpenID-Federation]
OpenID Foundation, "OpenID Federation 1.0", <https://openid.net/specs/openid-federation-1_0.html>.

[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>.

[RFC9711] Lundblade, L., Mandyam, G., O’Donoghue, J., and C. Wallace, "The Entity Attestation Token (EAT)", RFC 9711, DOI 10.17487/RFC9711, April 2025, <https://www.rfc-editor.org/info/rfc9711>.

Author’s Address

Chris Lemmons
Comcast
Email: chris_lemmons@comcast.com