Secure Patterns for Internet CrEdentials
Internet-Draft
Intended status: Informational
Expires: 4 June 2026

B. Maldant
SimpleLogin
M. B. Jones
Self-Issued Consulting

1 December 2025

OpenID Connect Standard Claims Registration for CBOR Web Tokens
draft-ietf-spice-oidc-cwt-04

Abstract

This document registers OpenID Connect standard claims already used in JSON Web Tokens for use in CBOR Web Tokens.

About This Document

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

The latest revision of this draft can be found at https://ietf-wg-spice.github.io/draft-ietf-spice-oidc-cwt/#go.draft-ietf-spice-oidc-cwt.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-spice-oidc-cwt/.

Discussion of this document takes place on the Secure Patterns for Internet CrEdentials Working Group mailing list (mailto:spice@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/spice/. Subscribe at https://www.ietf.org/mailman/listinfo/spice/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-wg-spice/draft-ietf-spice-oidc-cwt.

Status of This Memo

This Internet-Draft will expire on 4 June 2026.

Table of Contents

1. Introduction

OpenID Connect [OpenID.Core] is an authentication standard including standard claims already in use for JSON Web Tokens (JWT) [RFC7519]. CBOR Web Tokens (CWT) [RFC8392] have a claims registry, but do not include most of these claims. This draft aims at unifying use of OpenID Connect claims in JWTs and CWTs.

2. Conventions and Definitions

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.

3. OpenID Connect Claims

This section enumerates the OpenID Connect claims that are registered, including the fields necessary for registration with IANA; see Section 5. The definitions of each field are taken from [OpenID.Core] verbatim.

3.1. name

Claim Name: name
Claim Description: End-User's full name in displayable form
   including all name parts, possibly including titles and suffixes,
   ordered according to the End-User's locale and preferences.
JWT Claim Name: name
Claim Key: TBD1 (170 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.2. given_name

Claim Name: given_name
Claim Description: Given name(s) or first name(s) of the End-User.
JWT Claim Name: given_name
Claim Key: TBD2 (171 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.3. family_name

Claim Name: family_name
Claim Description: Surname(s) or last name(s) of the End-User.
JWT Claim Name: family_name
Claim Key: TBD3 (172 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.4. middle_name

Claim Name: middle_name
Claim Description: Middle name(s) of the End-User.
JWT Claim Name: middle_name
Claim Key: TBD4 (173 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.5. nickname

Claim Name: nickname
Claim Description: Casual name of the End-User that may or may not be the same as the given_name.
JWT Claim Name: nickname
Claim Key: TBD5 (174 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.6. preferred_username

Claim Name: preferred_username
Claim Description: Shorthand name by which the End-User wishes to be referred to at the Resource Server.
JWT Claim Name: preferred_username
Claim Key: TBD6 (175 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.7. profile

Claim Name: profile
Claim Description: URL of the End-User’s profile page.
JWT Claim Name: profile
Claim Key: TBD7 (176 suggested)

Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.8. picture

Claim Name: picture
Claim Description: URL of the End-User's profile picture. This URL MUST refer to an image file, rather than to a Web page containing an image.
JWT Claim Name: picture
Claim Key: TBD8 (177 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.9. website

Claim Name: website
Claim Description: URL of the End-User's Web page or blog.
JWT Claim Name: website
Claim Key: TBD9 (178 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.10. email

Claim Name: email
Claim Description: End-User's preferred e-mail address.
JWT Claim Name: email
Claim Key: TBD10 (179 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.11. email_verified

Claim Name: email_verified
Claim Description: True if the End-User's e-mail address has been verified; otherwise false. When this Claim Value is true, this means that the OP took affirmative steps to ensure that this e-mail address was controlled by the End-User at the time the verification was performed. The means by which an e-mail address is verified is context specific, and dependent upon the trust framework or contractual agreements within which the parties are operating.
JWT Claim Name: email_verified

Claim Key: TBD11 (180 suggested)
Claim Value Type(s): bool
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.12. gender

Claim Name: gender
Claim Description: End-User's defined gender. Values defined by this specification are female and male. Other values MAY be used when neither of the defined values are applicable.
JWT Claim Name: gender
Claim Key: TBD12 (181 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.13. birthdate

Claim Name: birthdate
Claim Description: End-User's birthday, represented as an [ISO8601_1] YYYY-MM-DD format. The year MAY be 0000, indicating that it is omitted. To represent only the year, YYYY format is allowed. Note that depending on the underlying platform's date related function, providing just year can result in varying month and day, so the implementers need to take this factor into account to correctly process the dates.
JWT Claim Name: birthdate
Claim Key: TBD13 (182 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.14. zoneinfo

Claim Name: zoneinfo
Claim Description: String from IANA Time Zone Database [IANAtimezones] representing the End-User's time zone.
JWT Claim Name: zoneinfo
Claim Key: TBD14 (183 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.15. locale

Claim Name: locale
Claim Description: End-User's locale, represented as a BCP47

[RFC5646] language tag.
JWT Claim Name: locale
Claim Key: TBD15 (184 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.16. phone_number

Claim Name: phone_number
Claim Description: End-User's preferred telephone number.
JWT Claim Name: phone_number
Claim Key: TBD16 (185 suggested)
Claim Value Type(s): text string
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.17. phone_number_verified

Claim Name: phone_number_verified
Claim Description: True if the End-User's phone number has been verified; otherwise false. When this Claim Value is true, this means that the OP took affirmative steps to ensure that this phone number was controlled by the End-User at the time the verification was performed. The means by which a phone number is verified is context specific, and dependent upon the trust framework or contractual agreements within which the parties are operating. When true, the phone_number Claim MUST be in E.164 format and any extensions MUST be represented in [RFC3966] format.
JWT Claim Name: phone_number_verified
Claim Key: TBD17 (186 suggested)
Claim Value Type(s): bool
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.18. address

Claim Name: address
Claim Description: End-User's preferred postal address.
JWT Claim Name: address
Claim Key: TBD18 (187 suggested)
Claim Value Type(s): map
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

3.18.1. Address Claim

To further reduce the size of this prevalent and large claim, these unsigned integer labels for its members are defined:

Name	Label	Type	Description
formatted	1	text string	Full mailing address, formatted for display or use on a mailing label. This field MAY contain multiple lines, separated by newlines. Newlines can be represented either as a carriage return/line feed pair ("\r\n") or as a single line feed character ("\n").
street_address	2	text string	Full street address component, which MAY include house number, street name, Post Office Box, and multi-line extended street address information. This field MAY contain multiple lines, separated by newlines. Newlines can be represented either as a carriage return/line feed pair ("\r\n") or as a single line feed character ("\n").
locality	3	text string	City or locality component.
region	4	text string	State, province, prefecture, or region component.
postal_code	5	text string	Zip code or postal code component.
country	6	text string	Country name component.

Table 1: Address labels

We strictly map the definition of claims in Section 5.1.1 of [OpenID.Core]: all the claims are optional and "formatted" can either be used instead or in addition of all the other fields.

3.19. updated_at

Claim Name: updated_at
Claim Description: Time the End-User’s information was last updated. Its value is a NumericDate as defined in Section 2 of [RFC8392].
JWT Claim Name: updated_at
Claim Key: TBD19 (188 suggested)
Claim Value Type(s): integer or floating-point number
Change Controller: IETF
Specification Document(s): Section 5.1 of [OpenID.Core]

4. Security Considerations

This document registers existing OpenID Connect standard claims already used in JSON Web Tokens [RFC7519] for use in CBOR Web Tokens [RFC8392] without changing their semantics. The Security and Privacy Considerations respectively of Sections 16 and 17 of [OpenID.Core] also apply.

5. IANA Considerations

All claims defined in Section 3 are registered in the (CBOR Web Token (CWT) Claims) [IANA.CWT.Claims] Registry (part of the eponymous registry group). No new IANA registry is created.

In case any of the suggested code points would have been claimed by the time the IESG approves the document for publication as an RFC, IANA is asked to assign Claim Key values from the 170-256 range.

6. References

6.1. Normative References

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

[IANAtimezones]
"IANA time zones", n.d., <https://www.iana.org/time-zones>.

[ISO8601_1]
"ISO8601-1", n.d., <https://www.iso.org/standard/81801.html>.

[OpenID.Core]
Sakimura, N., Bradley, J., Jones, M. B., Medeiros, B. de., and C. Mortimore, "OpenID Connect Core 1.0 incorporating errata set 2", 15 December 2023, <https://openid.net/specs/openid-connect-core-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/rfc/rfc2119>.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, DOI 10.17487/RFC3966, December 2004, <https://www.rfc-editor.org/rfc/rfc3966>.

[RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <https://www.rfc-editor.org/rfc/rfc5646>.

[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/rfc/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/rfc/rfc8392>.

6.2. Informative References

[CDDL] 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/rfc/rfc8610>.

[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/rfc/rfc7519>.

Appendix A. CDDL Schema

The following CDDL Schema [CDDL] includes example values for each item.

```
   name = (TBD1 => tstr) ; "Jane Doe"
   given_name = (TBD2 => tstr) ; "Jane"
   family_name = (TBD3 => tstr) ; "Doe"
   middle_name = (TBD4 => tstr) ; "Ellen"
   nickname = (TBD5 => tstr) ; "Jane D."
   preferred_username = (TBD6 => tstr) ; "j.doe"
   profile = (TBD7 => tstr) ; "https://example.org/about.html"
   picture = (TBD8 => tstr) ; "https://example.org/avatar.png"
   website = (TBD9 => tstr) ; "https://example.org"
   email = (TBD10 => tstr) ; "janedoe@example.com"
   email_verified = (TBD11 => bool) ; true
   gender = (TBD12 => tstr) ; "female"
   birthdate = (TBD13 => tstr) ; "1970-03-22"
   zoneinfo = (TBD14 => tstr) ; "America/Los_Angeles"
   locale = (TBD15 => tstr) ; "en_US"
   phone_number = (TBD16 => tstr) ; "+1 (425) 555-1212"
   phone_number_verified = (TBD17 => bool) ; true
   address = {
       &(formatted: 1) ^ => tstr,
       ; "1234 Hollywood Blvd. Los Angeles CA,"
       ; " 90210 United States of America"
       &(street_address: 2) ^ => tstr, ; "1234 Hollywood Blvd."
       &(locality: 3) ^ => tstr, ; "Los Angeles"
       &(region: 4) ^ => tstr, ; "CA"
       &(postal_code: 5) ^ => tstr, ; "90210"
       &(country: 6) ^ => tstr, ; "United States of America"
   }
   updated_at = (TBD19 => int / float) ; 1730123071

   TBD1 = 170
   TBD2 = 171
   TBD3 = 172
   TBD4 = 173
   TBD5 = 174
   TBD6 = 175
   TBD7 = 176
   TBD8 = 177
   TBD9 = 178
   TBD10 = 179
   TBD11 = 180
   TBD12 = 181
   TBD13 = 182
   TBD14 = 183
   TBD15 = 184
   TBD16 = 185
   TBD17 = 186
   TBD18 = 187
   TBD19 = 188
```

Figure 1: A CDDL description of each claim

Acknowledgments

The authors would like to thank the following individuals for their contributions to this specification: Martin Thompson and David Waite.

Document History

-04

* Moved claim definitions into the body of the specification.

-03

* Defined numeric labels for address claim items.

* Copied text describing gender claim values from [OpenID.Core].

-02

* Update descriptions of email_verified, phone_number_verified, and birthdate claims using text from [OpenID.Core].

* Use TBDn names for CWT requested claim numbers.

-01

* Aligned terminology with OpenID Connect specification.

* Added Michael B. Jones as an editor.

-00

* Initial working group draft, based on draft-maldant-spice-oidc-cwt-02.

Authors' Addresses

Beltram Maldant
SimpleLogin
Email: beltram.ietf@pm.me

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

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