Workgroup: None
Internet-Draft:
draft-prorock-jose-native-jwt-vcs-00
Published: 24 May 2023
Intended Status: Standards Track
Expires: 25 November 2023
Authors: M. Prorock  O. Steele
mesur.io  Transmute

# Native JWT Representation of Verifiable Credentials

## Abstract

This document describes how to construct and utilize a JWT as a Verifiable Credential utilizing only JSON and registered claims.

This document does not define any new cryptography, only seralizations of systems.

## 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 25 November 2023.

**Table of Contents**


1. Notational Conventions
2. Terminology
3. Native JWT Representation of Verifiable Credentials
   3.1. Overview
      3.1.1. Credential Header
      3.1.2. Credential
      3.1.3. Verifiable Credential
4. Security Considerations
5. IANA Considerations
   5.1. Media Type Registration
6. Normative References

Authors' Addresses


## 1. Notational Conventions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in [RFC2119].

## 2. Terminology

The following terminology is used throughout this document:

**signature** The digital signature output.

## 3. Native JWT Representation of Verifiable Credentials

### 3.1. Overview

This section provides guidance on how to use JSON [RFC8259] claimsets with JWT [RFC7519] registered claims to construct a JWT that can be mapped to a verifiable credential. This section also describes how to use content types and token types to distinguish different representations of verifiable credentials.

This representation relies on claims registered in the IANA JSON Web Token Claims Registry whenever possible.

Implementers using this representation SHOULD NOT use vc+ld+json as an input.

#### 3.1.1. Credential Header

typ MUST use the media type vc+jwt.

Example of credential metadata (decoded JWT header):

```
{
  "kid": "https://example.edu/issuers/14#key-0",
  "alg": "ES256",
  "typ": "vc+jwt"
}
```

#### 3.1.2. Credential

Example of a credential (decoded JWT payload):

```
{
  "iss": "https://example.edu/issuers/14",
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022,
  "urn:example:claim": true
}
```

NOTE: The vc and vp claims MUST NOT be present when the content type header parameter is set to credential-claims-set+json.

#### 3.1.3. Verifiable Credential

Example of an JWT encoded verifiable credential (using external proof):

```
=============== NOTE: '\' line wrapping per RFC 8792 ================
eyJraWQiOiJodHRwczovL2V4YW1wbGUuZWR1L2lzc3VlcnMvMTQja2V5LTAiLCJhbGci\
OiJFUzI1NiIsInR5cCI6InZjK2p3dCJ9.eyJpc3MiOiJodHRwczovL2V4YW1wbGUuZWR\
1L2lzc3VlcnMvMTQiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiw\
iaWF0IjoxNTE2MjM5MDIyLCJ1cm46ZXhhbXBsZTpjbGFpbSI6dHJ1ZX0.WLD4Qxh629T\
FkJHzmbkWEefYX-QPkdCmxbBMKNHErxND2QpjVBbatxHkxS9Y_SzBmwffuM2E9i5VvVg\
pZ6v4Tg
```

## 4. Security Considerations

All security considerations from JSON [RFC8259] and JWT [RFC7519] SHOULD be followed.

## 5. IANA Considerations

### 5.1. Media Type Registration

This section will register the "application/vc+jwt" media type [RFC2046] in the "Media Types" registry [IANA.MediaTypes] in the manner described in RFC 6838 [RFC6838], which can be used to indicate that the content is a JWT.

*Type name: application
*Subtype name: vc+jwt

*Required parameters: n/a
*Optional parameters: n/a
*Encoding considerations: 8bit; JWT values are encoded as a series of base64url-encoded values (some of which may be the empty string) separated by period ('.') characters.
*Security considerations: See the Security Considerations section of RFC 7519
*Interoperability considerations: n/a
*Published specification: n/a
*Applications that use this media type: OpenID Connect, Mozilla
*Persona, Salesforce, Google, Android, Windows Azure, Amazon Web
*Services, and numerous others
*Fragment identifier considerations: n/a
*Additional information: Magic number(s): n/a File extension(s): n/a Macintosh file type code(s): n/a
*Person & email address to contact for further information: Michael Prorock, mprorock@mesur.io
*Intended usage: COMMON
*Restrictions on usage: none
*Author: Michael Prorock, mprorock@mesur.io
*Change controller: IESG
*Provisional registration? Yes

## 6. Normative References


**[RFC2046]** Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

**[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>.

**[RFC6838]** Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/info/rfc6838>.

**[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>.

**[RFC8259]** Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

## Authors' Addresses

Michael Prorock
mesur.io

Email: mprorock@mesur.io

Orie Steele
Transmute

Email: orie@transmute.industries