OAuth Working Group
Internet-Draft
Intended status: Informational
Expires: May 15, 2016

E. Wahlstroem
Nexus Technology
M. Jones
Microsoft
H. Tschofenig
ARM Ltd.

November 12, 2015

CBOR Web Token (CWT)
draft-wahlstroem-oauth-cbor-web-token-00

Abstract

CBOR Web Token (CWT) is a compact means of representing claims to be transferred between two parties. CWT is a profile of the JSON Web Token (JWT) that is optimized for constrained devices. The claims in a CWT are encoded in the Concise Binary Object Representation (CBOR) and CBOR Object Signing and Encryption (COSE) is used for added application layer security protection. A claim is a piece of information asserted about a subject and is represented as a name/value pair consisting of a claim name and a claim value.

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 http://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 May 15, 2016.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. Claims 3
3.1. Claim Names 3
3.1.1. iss (Issuer) Claim 4
3.1.2. sub (Subject) Claim 4
3.1.3. aud (Audience) Claim 4
3.1.4. exp (Expiration Time) Claim 4
3.1.5. nbf (Not Before) Claim 4
3.1.6. iat (Issued At) Claim 5
3.1.7. cti (CWT ID) Claim 5
3.1.8. cks (COSE Key Structure) Claim 5
4. Summary of CBOR major types used by defined claims . . 5
5. CBOR Web Token Example 6
6. Security Considerations 6
7. IANA Considerations 6
8. Acknowledgements 6
9. References 7
9.1. Normative References 7
9.2. Informative References 7
Authors' Addresses 7

1. Introduction

With JSON Web Tokens (JWTs) a standardized format of security tokens has been defined and has found use in OAuth 2.0 and OpenID Connect deployments. With JSON Web Signatures (JWS) and JSON Web Encryption (JWE) security the content of the JWT, which comes in form of claims, is protected. The use of JSON for encoding information is popular for Web applications but it is still considered inefficient for use in many IoT systems that use low power radio technologies.

In this document an alternative encoding of claims is defined. Instead of using JSON, as provided by JWTs, this specification

suggests the use of CBOR and calls this new structure 'CBOR Web Token (CWT)', which is a compact means of representing claims to be transferred between two parties. To protect the claims inside the CWT the CBOR Object Signing and Encryption (COSE) specification is re-used.

The suggested pronunciation of CWT is the same as the English word "cot".

2. Terminology

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 "Key words for use in RFCs to Indicate Requirement Levels" [1].

This document reuses terminology and definitions from the CBOR [6] and COSE [4] specifications.

The following data types are used in this document:

StringOrURI:

A CBOR major type 3, string value, with the additional requirement that while arbitrary string values MAY be used, any value containing a ":" character MUST be a URI [3]. StringOrURI values are compared as case-sensitive strings with no transformations or canonicalizations applied.

DateTime:

The date/time strings are defined in Section 2.4.1 in RFC 7049 [2] as a CBOR major type 6, with tag value 0.

3. Claims

The set of claims that a CWT must contain to be considered valid is context dependent and is outside the scope of this specification. Specific applications of CWTs will require implementations to understand and process some claims in particular ways. However, in the absence of such requirements, all claims that are not understood by implementations MUST be ignored.

3.1. Claim Names

None of the claims defined below are intended to be mandatory to use or mandatory implement. They rather provide a starting point for a set of useful, interoperable claims. Applications using CWTs should define which specific claims they use and when they are required or optional.

3.1.1. iss (Issuer) Claim

The "iss" (issuer) claim identifies the principal that issued the CWT. The "iss" value is a case-sensitive string containing a StringOrURI value.

3.1.2. sub (Subject) Claim

The "sub" (subject) claim identifies the principal that is the subject of the CWT. The claims in a CWT are normally statements about the subject. The subject value MUST either be scoped to be locally unique in the context of the issuer or be globally unique. The processing of this claim is generally application specific. The "sub" value is a case-sensitive string containing a StringOrURI value.

3.1.3. aud (Audience) Claim

The "aud" (audience) claim identifies the recipients that the CWT is intended for. Each principal intended to process the CWT MUST identify itself with a value in the audience claim. If the principal processing the claim does not identify itself with a value in the "aud" claim when this claim is present, then the CWT MUST be rejected. In the general case, the "aud" value is an array of case-sensitive strings, each containing a StringOrURI value. In the special case when the CWT has one audience, the "aud" value MAY be a single case-sensitive string containing a StringOrURI value.

3.1.4. exp (Expiration Time) Claim

The "exp" (expiration time) claim identifies the expiration time on or after which the CWT MUST NOT be accepted for processing. The processing of the "exp" claim requires that the current date/time MUST be before the expiration date/time listed in the "exp" claim. Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew. Its value MUST be a number containing a DateTime value.

3.1.5. nbf (Not Before) Claim

The "nbf" (not before) claim identifies the time before which the CWT MUST NOT be accepted for processing. The processing of the "nbf" claim requires that the current date/time MUST be after or equal to the not-before date/time listed in the "nbf" claim. Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew. Its value MUST be a number containing a DateTime value.

3.1.6. iat (Issued At) Claim

The "iat" (issued at) claim identifies the time at which the CWT was issued. This claim can be used to determine the age of the CWT. Its value MUST be a number containing a DateTime value.

3.1.7. cti (CWT ID) Claim

The "cti" (CWT ID) claim provides a unique identifier for the CWT. The identifier value MUST be assigned in a manner that ensures that there is a negligible probability that the same value will be accidentally assigned to a different data object; if the application uses multiple issuers, collisions MUST be prevented among values produced by different issuers as well. The "cti" claim can be used to prevent the CWT from being replayed. The "cti" value is a case-sensitive string of CBOR major type 3.

3.1.8. cks (COSE Key Structure) Claim

The "cks" (COSE Key Structure) claim holds members representing a COSE Key Structure. The members of the structure can be found in Section 7.1 of [4]. The "cti" value is a case-sensitive string of

CBOR major type 2, byte string.

4. Summary of CBOR major types used by defined claims

Value	Major Type	Key
1	3	iss
2	3	sub
3	3	aud
4	6 tag value 0	exp
5	6 tag value 0	nbf
6	6 tag value 0	iat
7	3	cti
8	2	cks

Figure 1: Summary of CBOR major types used by defined Claims.

Note: Claims defined by the OpenID Foundation have not yet been included in the table above.

5. CBOR Web Token Example

This section illustrates a CWT in the CBOR diagnostic notation. This example CWT was issued by the AS identified as "coap://as.example.com" in the "iss" (issuer) claim. The CWT is only valid at a resource server at "coap://light.example.com". Its validity is 2 minutes.

```
{
  "iss": "coap://as.example.com",
  "aud": "coap://light.example.com",
  "exp": 1444064944,
  "iat": 1443944944
}
```

Figure 2: CWT Example in the CBOR Diagnostic Notation.

6. Security Considerations

The security of the CWT is dependent on the protection offered by COSE. Without protecting the claims contained in a CWT an adversary is able to modify, add or remove claims. Since the claims conveyed in a CWT are used to make authorization decisions it is not only important to protect the CWT in transit but also to ensure that the recipient is able to authenticate the party that collected the claims and created the CWT. Without trust of the recipient in the party that created the CWT no sensible authorization decision can be made. Furthermore, the creator of the CWT needs to carefully evaluate each claim value prior to including it in the CWT so that the recipient can be assured about the correctness of the provided information.

7. IANA Considerations

This section will create a registry for CWT claims, possibly relating them to the JWT Claims Registry.

8. Acknowledgements

Add your name here.

A straw man proposal of CWT was written in the draft "Authorization for the Internet of Things using OAuth 2.0" [5] with the help of Ludwig Seitz, Goeran Selander, and Samuel Erdtman.

9. References

9.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[2] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <http://www.rfc-editor.org/info/rfc7049>.

[3] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[4] Schaad, J., "CBOR Encoded Message Syntax", draft-ietf-cose-msg-07 (work in progress), November 2015.

9.2. Informative References

[5] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authorization for the Internet of Things using OAuth 2.0", draft-seitz-ace-oauth-authz-00 (work in progress), October 2015.

[6] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <http://www.rfc-editor.org/info/rfc7519>.

Authors' Addresses

Erik Wahlstroem
Nexus Technology
Sweden

Email: erik.wahlstrom@nexusgroup.com
URI: https://www.nexusgroup.com

Michael B. Jones
Microsoft

Email: mbj@microsoft.com
URI: http://self-issued.info/

Hannes Tschofenig

ARM Ltd.
Hall in Tirol 6060
Austria

Email: Hannes.Tschofenig@arm.com