Network Working Group
Internet-Draft
Intended status: Experimental
Expires: April 25, 2019

J. Schaad
August Cellars

October 22, 2018

# Use of a CWT identifier as a Confirmation Method
# draft-schaad-cnf-cwt-id-00

Abstract

TBD

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 April 25, 2019.

Table of Contents



## 1. Introduction

In many cases an authorization in the form of a COSE Web Token (CWT) [RFC8392] will be issued in the ACE OAuth [I-D.ietf-ace-oauth-authz] framework with a minimal set of privileges and a Proof-of-Possession claim [I-D.ietf-ace-cwt-proof-of-possession]. It may then become necessary to issue a new token for a shorter period with more capabilities, but use the same information for validation. In these cases it makes sense to issue a new authorization token which refers the the first token to provide the additional capabilities. This document defines a new confirmation type that allows this type of referencing to be done.

This differs from the refresh token in that the new token will be limited to the duration of the existing CWT, while a new POP CWT would be issued when using a refresh token.

## 1.1. Conventions Used in This Document

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.

## 2. Terminology

- "Relying Party" is used in this document to refer to the party which is relying on the contents of a CWT in order to make a security decision. In other OAuth documents, this is normally referred to as the XXXXXX.

- "Referenced CWT" is used to denote the CWT which is referred to or referenced by a referencing CWT. The referenced CWT has a confirmation type with the POP keying information in it.

- "Referencing CWT" is used to denote the CWT which is making a reference to a second CWT. The referencing CWT contains the confirmation type defined in this document.

## 3. CWT Id Confirmation Method

The CWT Id confirmation method is identified by TBD1 in the 'cnf' element (defined in [I-D.ietf-ace-cwt-proof-of-possession]. For use in documentation the string value of 'cwtid' is to be used to refer to this confirmation type.

The CWT Id confirmation method uses the type of CBOR map and has the following fields:

- Issuer is an optional field in the map. If present the issuer field contains the 'iss' field of CWT which is being referenced. If absent, the issuer is the same entity which issued the referencing CWT. When encoded, this field uses TBD2 as the map key.

- CWT Id is a required field in the map. The field contains the 'cwtid' field of the referenced CWT. When encoded, this field uses TBD3 as the map key.

An example of what this would look like is:

```
/ cnf /: {
    / cwtid /: 'CWTID 1234',
    / iss /: "Entry-Level AS"
}
```

## 4. CWT Id in AS Response

Since the CWT Id is currently only provided to the RS as part of the token, for an AS which supports this option the CWT Id additionally needs to be provided to the Client. This document therefore defines two new fields to go into C-AS response messages:

"iss" provides the issuer name of the CWT. This field is only present for an AS which would allow a second AS to refer to the CWT.

"cwtid" contains the CWT Id for the issued token.

## 5. Processing Rules for the Issuer of a CWT Id Confirmation Method

When an AS is going to issue a CWT it MUST perform the following steps or their equivalent:

1. If the issued CWT will refer to a CWT issued by a different AS, the issuing AS MUST be configured to permit this.

2. The AS MUST validate that the entity for which this CWT is being issued for is the same entity that is the subject of the referenced CWT. This can be done by causing the client to perform a POP operation with the referenced CWTs POP key information or by querying the AS which issued the referenced CWT. If the same AS is being used for both CWTs, then the AS can consult a database of clients and CWTs to check for identity matching.

3. The issued CWT should refer to the original POP CWT. The chain of trust SHOULD NOT be transitive through another CWT.

## 6. Processing Rules for the CWT Id Confirmation Method

When a relying party receives a referencing CWT it MUST perform the following steps or their equivalent as part of making a security decision:

1. The referencing CWT MUST have the authentication checked on it. If the authentication fails, the CWT MUST be rejected.

2. If the CWT Id confirmation type contains an issuer field, configuration information MUST be checked that the referencing CWT issuer is permitted to use the referenced CWT issuer. If the reference is not permitted, then the CWT MUST be rejected.

3. If the referenced CWT is expired, the referencing CWT MUST be rejected.

4. The claims in the referenced CWT are copied from the referenced CWT to the referencing CWT if the claim does not exist in the referencing CWT.

5. The modified CWT is then processed in a normal manner.

## 7. Security Considerations

As the security of the set of CWTs is going rest on the underlying POP CWT, loss of the key will allow any CWT which references the

orignal CWT to be used by a third party. All entities which have the secret portion of the key need to protect that portion of the key.

The use of this feature assumes a specific model of evaluating the rules for access control. Specifically, it assumes that if there are multiple access tokens, satisfying the conditions for any of the tokens means that access is going to be granted. This model is in contrast to one where if any of the access tokens was a deny, then access to to the resource would be denied.

## 8. IANA Considerations

There are some items that need to be registered. Figure out what they are and put them here.

## 9. Normative References

[I-D.ietf-ace-cwt-proof-of-possession]
Jones, M., Seitz, L., Selander, G., Erdtman, S., and H. Tschofenig, "Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)", draft-ietf-ace-cwt-proof-of-possession-03 (work in progress), June 2018.

[I-D.ietf-ace-oauth-authz]
Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", draft-ietf-ace-oauth-authz-16 (work in progress), October 2018.

[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>.

[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>.

Author's Address

Jim Schaad
August Cellars

Email: ietf@augustcellars.com