RATS Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 3, 2020

H. Birkholz
Fraunhofer SIT
J. "O'Donoghue"
Qualcomm Technologies Inc.
N. Cam-Winget
Cisco Systems
C. Bormann
Universitaet Bremen TZI
June 01, 2020

A CBOR Tag for Unprotected CWT Claims Sets
draft-birkholz-rats-uccs-01

Abstract

CBOR Web Token (CWT, RFC 8392) Claims Sets sometimes do not need the protection afforded by wrapping them into COSE, as is required for a true CWT. This specification defines a CBOR tag for such unprotected CWT Claims Sets (UCCS) and discusses conditions for its proper use.

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 December 3, 2020.

Table of Contents

1. Introduction

A CBOR Web Token (CWT) as specified by [RFC8392] is always wrapped in a CBOR Object Signing and Encryption (COSE, [RFC8152]) envelope. COSE provides - amongst other things - the integrity protection mandated by RFC 8392 and optional encryption for CWTs. Under the right circumstances, though, a signature providing proof for authenticity and integrity can be provided through the transfer protocol and thus omitted from the information in a CWT without compromising the intended goal of authenticity and integrity. If a mutually Secured Channel is established between two remote peers, and if that Secure Channel provides the correct properties, it is possible to omit the protection provided by COSE, creating a use case for unprotected CWT Claims Sets. Similarly, if there is one-way authentication, the party that did not authenticate may be in a position to send authentication information through this channel that allows the already authenticated party to authenticate the other party.

This specification allocates a CBOR tag to mark Unprotected CWT Claims Sets (UCCS) as such and discusses conditions for its proper use in the scope of Remote ATtestation procedureS (RATS).

This specification does not change [RFC8392]: A true CWT does not make use of the tag allocated here; the UCCS tag is an alternative to using COSE protection and a CWT tag. Consequently, in a well-defined scope, it might be acceptable to strip a CWT of its COSE container an

replace the CWT Claims Set's CWT CBOR tag with a UCCS CBOR tag for further processing - or vice versa.

1.1. Terminology

The term Claim is used as in [RFC8725].

The terms Claim Key, Claim Value, and CWT Claims Set are used as in [RFC8392].

UCCS: Unprotected CWT Claims Set; a CBOR map of Claims as defined by the CWT Claims Registry that are composed of pairs of Claim Keys and Claim Values.

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. Motivation and Requirements

Use cases involving the conveyance of claims, in particular, remote attestations [I-D.ietf-rats-architecture] require a standardized data schema and format that can be trasferred and transported using different communication channels. As these are Claims, [RFC8392] are a suitable format but how these Claims are secured depends on the deployment, the security capabilities of the device, as well as their software stack. For example, a Claim may be securely stored and conveyed using the device's trusted execution environment or especially in some resource constrained environments the same process that provides the secure communication transport is also the delegate to compose the Claim to be conveyed. Whether it is a transfer or transport, a Secure Channel is presumed to be used for conveying such UCCS. The following section further describes the requirements and scenarios in which UCCS can be used.

3. Characteristics of a Secure Channel

A Secure Channel for the conveyance of UCCS needs to provide the security properties that would otherwise be provided by COSE for a CWT. In this regard, UCCS is similar in security considerations to JWTs [RFC8725] using the algorithm "none". RFC 8725 states: "if a JWT is cryptographically protected end-to-end by a transport layer, such as TLS using cryptographically current algorithms, there may be no need to apply another layer of cryptographic protections to the JWT. In such cases, the use of the "none" algorithm can be perfectly acceptable.". Analogously, the considerations discussed in Sections

2.1, 3.1, and 3.2 of RFC 8725 apply to the use of UCCS as elaborated on in this document.

Secure Channels are often set up in a handshake protocol that mutually derives a session key, where the handshake protocol establishes the authenticity of one of both ends of the communication. The session key can then be used to provide confidentiality and integrity of the transfer of information inside the Secure Channel. A well-known example of a such a Secure Channel setup protocol is the TLS [RFC8446] handshake; the TLS record protocol can then be used for secure conveyance.

As UCCS were initially created for use in Remote ATtestation procedureS (RATS) Secure Channels, the following subsection provides a discussion of their use in these channels. Where other environments are intended to be used to convey UCCS, similar considerations need to be documented before UCCS can be used.

3.1. UCCS and Remote ATtestation procedureS (RATS)

Secure Channels can be transient in nature. For the purposes of this specification, the mechanisms used to establish a Secure Channel are out of scope. As a minimum requirement in the scope of RATS Claims, however, the Verifier must authenticate the Attester as part of the Secure Channel establishment.

If only authenticity/integrity for a Claim is required, a Secure Channel MUST be established to, at minimum, provide integrity of the communication. Further, the provider of the UCCS SHOULD be authenticated by the reciever to ensure the channel is truly secured and the sender is validated. If confidentiality is also required, the receiving side SHOULD also be authenticated.

The extent to which a Secure Channel can provide assurances that UCCS originate from a trustworthy attesting environment depends on the characteristics of both the cryptographic mechanisms used to establish the channel and the characteristics of the attesting environment itself. A Secure Channel established or maintained using weak cryptography may not provide the assurance required by a relying party of the authenticity and integrity of the UCCS.

Where the security assurance required of an attesting environment by a relying party requires it, the attesting environment may be implemented using techniques designed to provide enhanced protection from an attacker wishing to tamper with or forge UCCS. A possible approach might be to implement the attesting environment in a hardened environment such as a TEE [I-D.ietf-teep-architecture] or a TPM [TPM2].

As with EATs nested in other EATs (Section 3.12.1.2 of [I-D.ietf-rats-eat]), the Secure Channel does not endorse fully formed CWTs transferred through it. Effectively, the COSE envelope of a CWT shields the CWT Claims Set from the endorsement of the Secure Channel. (Note that EAT might add a nested UCCS Claim, and this statement does not apply to UCCS nested into UCCS, only to fully formed CWTs)

3.2. Privacy Preserving Channels

A Secure Channel which preserves the privacy of the Attester may provide security properties equivalent to COSE, but only inside the life-span of the session established. In general, a Verifier cannot correlate UCCS received in different sessions from the same attesting environment based on the cryptographic mechanisms used when a privacy preserving Secure Channel is employed.

In the case of a Remote Attestation, the attester must consider whether any UCCS it returns over a privacy preserving Secure Channel compromises the privacy in unacceptable ways. As an example, the use of the EAT UEID [I-D.ietf-rats-eat] Claim in UCCS over a privacy preserving Secure Channel allows a verifier to correlate UCCS from a single attesting environment across many Secure Channel sessions. This may be acceptable in some use-cases (e.g. if the attesting environment is a physical sensor in a factory) and unacceptable in others (e.g. if the attesting environment is a device belonging to a child).

4. IANA Considerations

In the registry [IANA.cbor-tags], IANA is requested to allocate the tag in Table 1 from the FCFS space, with the present document as the specification reference.

Tag	Data Item	Semantics
TBD601	map	Unprotected CWT Claims Set [RFCthis]

Table 1: Values for Tags

5. Security Considerations

The security considerations of [RFC7049] and [RFC8392] apply.

{#secchan} discusses security considerations for Secure Channels, in which UCCS might be used. This documents provides the CBOR tag

definition for UCCS and a discussion on security consideration for the use of UCCS in Remote ATtestation procedureS (RATS). Uses of UCCS outside the scope of RATS are not covered by this document. The UCCS specification - and the use of the UCCS CBOR tag, correspondingly - is not intended for use in a scope where a scope-specific security consideration discussion has not been conducted, vetted and approved for that use.

6. References

6.1. Normative References

[IANA.cbor-tags]
IANA, "Concise Binary Object Representation (CBOR) Tags", <http://www.iana.org/assignments/cbor-tags>.

[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>.

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

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8725] Sheffer, Y., Hardt, D., and M. Jones, "JSON Web Token Best Current Practices", BCP 225, RFC 8725, DOI 10.17487/RFC8725, February 2020, <https://www.rfc-editor.org/info/rfc8725>.

[TPM2] "Trusted Platform Module Library Specification, Family "2.0", Level 00, Revision 01.59 ed., Trusted Computing Group", 2019.

6.2. Informative References

[I-D.ietf-rats-architecture]
Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", draft-ietf-rats-architecture-04 (work in progress), May 2020.

[I-D.ietf-rats-eat]
Mandyam, G., Lundblade, L., Ballesteros, M., and J. O'Donoghue, "The Entity Attestation Token (EAT)", draft-ietf-rats-eat-03 (work in progress), February 2020.

[I-D.ietf-teep-architecture]
Pei, M., Tschofenig, H., Thaler, D., and D. Wheeler, "Trusted Execution Environment Provisioning (TEEP) Architecture", draft-ietf-teep-architecture-08 (work in progress), April 2020.

Appendix A. Example

The example CWT Claims Set from Appendix A.1 of [RFC8392] can be turned into an UCCS by enclosing it with a tag number TBD601:

```
 <TBD601>(
   {
     / iss / 1: "coap://as.example.com",
     / sub / 2: "erikw",
     / aud / 3: "coap://light.example.com",
     / exp / 4: 1444064944,
     / nbf / 5: 1443944944,
     / iat / 6: 1443944944,
     / cti / 7: h'0b71'
   }
 )
```

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295
Germany

Email: henk.birkholz@sit.fraunhofer.de

Jeremy O'Donoghue
Qualcomm Technologies Inc.
279 Farnborough Road
Farnborough GU14 7LS
United Kingdom

Email: jodonogh@qti.qualcomm.com

Nancy Cam-Winget
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
USA

Email: ncamwing@cisco.com

Carsten Bormann
Universitaet Bremen TZI
Bibliothekstrasse 1
Bremen 28369
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.de