

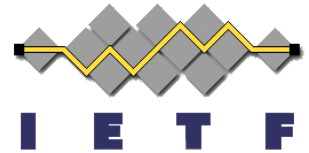
CBOR Web Token (CWT) Claims in COSE Headers

draft-looker-cose-cwt- claims-in-headers

Tobias Looker & Mike Jones
IETF 113, Vienna
March 21, 2022

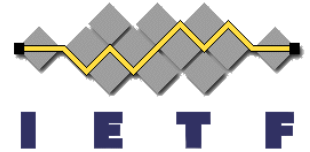


Context



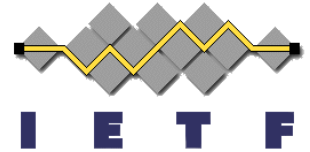
- The CBOR Web Token [RFC 8392] establishes a registry of useful claims for developing interoperable security tokens.
- In some cases, it is useful to be able to express some of these claims in the headers of a COSE structure instead of just in the payload. Examples include:
 - Encrypted CWTs
 - COSE structures using detached signatures
- Section 5.3 of JWT [RFC 7519] defined a mechanism for expressing JWT claims in JOSE headers.
 - That the equivalent capability was not included in CWT is an oversight this draft intends to rectify.

How



- The draft requests the registration of one new COSE header parameter (of type map) that defines a location and mechanism for expressing CWT claims in a COSE header.
- The CWT claims must be namespaced within a new COSE header parameter because there are conflicts between the numeric header parameter assignments and the numeric CWT claim assignments.

Next Steps



- The authors request working group review of the document.
- Following addressing working group review comments, we plan to request working group adoption.