CBOR Web Token (CWT) Claims in COSE Headers

draft-ietf-cose-cwt-claims-in-headers

Tobias Looker & Mike Jones
IETF 116, Yokohama
March 27, 2022
What Does It Do?

- Enables including CBOR Web Token (CWT) claims in a COSE header parameter
- CWT claims are contained within a new COSE header parameter because there are conflicts between the numeric header parameter assignments and the numeric CWT claim assignments
Why Do It?

- In some cases, it is useful to express CWT claims in a header parameter of a COSE structure instead of just in the payload.

- Examples:
  - Including unencrypted claims, such as Issuer, in an encrypted CWT.
  - Including CWT claims when the payload isn’t a CWT.
Status

• Very simple draft that does one thing
• Adopted by working group in July 2022
• Just published -03 with a couple of minor changes:
  • Added a CDDL description for the value type of this header
  • Clarified treatment of the claim in protected vs unprotected usages
Next Steps

• Time for Working Group Last Call?