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

Carsten Bormann, 2021-11-08 · IETF 112
CWT, CCS, and UCCS

- RFC 8392 defines CWT:
  - CWT = COSE armor around CCS (tag 61)
  - CCS is similar to a JWT claims set (RFC 7519, RFC 8726):
    - key/value set (map) of “claims”
    - **together** form an assertion
  - UCCS = Unprotected CCS (tag 601*)

*) Tag 601 proposed, but not yet assigned.
Why does UCCS need a specification?

- Actually: no. Could just register the tag and refer to RFC 8392.
- Better: yes.
  - Write up the area of application: UCCS is not a replacement for CWT.
    - Security considerations.
  - Relationship to RATS concepts, likely usage in RATS.
    What are the RATS requirements on a secure channel carrying a UCCS?
While we are at it...

- RFC 8392 (CWT) predates completion of RFC 8610 (CDDL). Now could provide CDDL spec for CCS. (Proposal is in a UCCS repo branch.)

  - (Note that CDDL for COSE is in RFC 8152 and RFC 9052-to-be.)

- Grander plans for unification between JWT (JCS) and CWT (CCS): Probably not. And if yes anyway, not here.
Next Steps

- Accept or reject the idea to add CDDL for CCS
- One more round of editing to address more of Thomas Fossati’s review
- WGLC then