

draft-ietf-rats-uccs-10

A CBOR Tag for Unprotected CWT Claims Sets (UCCS)

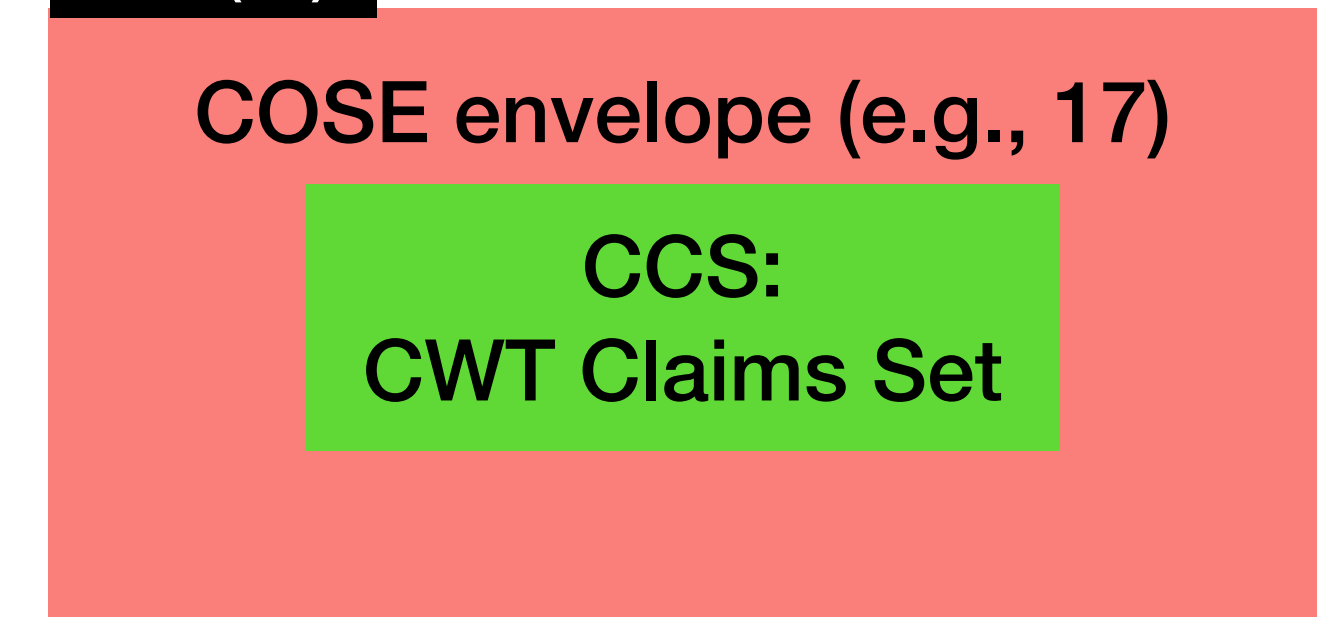
Carsten Bormann, 2024-07-23 · IETF 120

CWT, CCS, and UCCS

- RFC 8392 defines CWT:
 - CWT = COSE armor around CCS (tag 61)
 - CCS (CWT Claims Set) is similar to a JWT claims set (RFC 7519, RFC 8725):
 - key/value set (map) of “claims”
 - **together** form an assertion
- UCCS = Unprotected CCS (tag 601*)

CWT:

CWT (61):



UCCS:

UCCS (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 can provide CDDL spec for CCS.
 - (Note that CDDL for COSE was in RFC 8152 [yes, that predates RFC 8610, too] and is in RFC 9052.)
- Grander plans for unification between JWT (JCS) and CWT (CCS):
Probably not.
And if yes anyway, not here.

Next Steps

- This a -10, based on a lot of editorial feedback that has been acted upon
- Next step: WGLC