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

Expressing CWT claims in COSE headers
Rationale

JSON Web Tokens, a related predecessor to CBOR Web Tokens included normative text that permitted JWT claims appearing in the protected header, however CWT when standardized did not define the equivalent behaviour, this draft rectifies this.

Being able to place CWT claims in the header of a COSE structure has multiple possible applications.
Use Case - Encrypted CWT's

In some scenarios when an encrypted CWT is being created, there is the desire to have some of the claims present in the encrypted payload, replicated into the unencrypted header, examples include:

- The issuer claim (iss)
- Token validity information (exp iat)

Having these claims available in the header can both help in the decryption process (e.g. selecting which key to use for decryption) and also validate basic aspects of the token prior to decrypting it.
Use Case - Detached Payload

In scenarios where a COSE sign structure featuring a detached payload (not present) is being used, being able to define CWT claims in the COSE header of the structure can be useful, examples include:

- The issuer claim (iss)
- Token validity information (exp iat)

The claims can be used to validate the structure such as selecting the appropriate public key for signature verification.
Key Design Consideration

The IANA registry for the CWT claims and COSE header parameters are distinct meaning they cannot simply be merged as is the case in JWT, instead we propose to register a single new header parameter whose value is a map, where any CWT claims can then be located.