COSE "typ" (type) Header Parameter

draft-jones-cose-typ-header-parameter

M.B. Jones, O. Steele
IETF 117, San Francisco
July 24, 2023
What Does It Do?

- Adds the `typ` to COSE Protected Header
  - Enables typing the entire COSE structure using registered media types
  - While COSE included “content type” paralleling the JOSE “cty”, it failed to include the equivalent of “typ”.
Why Do It?

- Enable explicit typing, in parallel with the JWT BCP
- Consistently distinguishing “envelope” and “payload” media types, as discussed on the list:
  - typ: application/foo+yaml+jose
  - cty: application/yaml
  - typ: application/foo+json+cose
  - content_type: application/json
Why not just use CBOR tags?

- CBOR tags prefix the COSE structure and are not part of it
  - Therefore, they’re not integrity-protected and might be omitted
- “typ” (typ) parallels COSE “content type” and JOSE “typ”
  - Uses CoAP Content-Formats numbers and Media Type strings
Application Examples (SCITT Receipt & W3C Verifiable Credentials)

```plaintext
# COSE_Sign1
18([
  # Protected Header
  h'a2012...43833633531,'
  # {
  #   "alg" : "ES256",
  #   1 : -7,
  #   "typ" : "receipt+cose",
  #   "TBD (requested 14)" : h'a2012...43833633531',
  #   ... additional application specific headers ... 
  # }
  # Unprotected Header
  { 
    .... 
  },
  # Protected Payload
  ...
  # Signature
  h'486...7f77ea'
])
```

```plaintext
# COSE_Sign1
18([
  # Protected Header
  h'a2012...43833633531,'
  # {
  #   "alg" : "ES384",
  #   1 : -35,
  #   "typ" : "application/cwt",
  #   "TBD (requested 14)" : 61,
  #   ... additional application specific headers ... 
  # }
  # Unprotected Header
  { 
    .... 
  },
  # Protected Payload
  ...
  # Signature
  h'486...7f77ea'
])
```
Status

- Recently published -00
- Need to add CDDL examples
Next Steps

- Review by working group members
- Then consider for working group adoption?