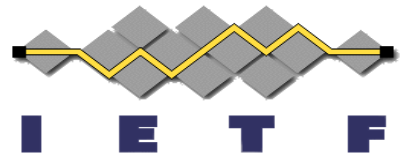
COSE "typ" (type) Header Parameter

draft-ietf-cose-typ-header-parameter

Mike Jones and Orie Steele

IETF 118, Prague

November 7, 2023



What Does It Do?

- Adds the “typ” (type) COSE Protected Header
  - Enables typing the entire COSE object using registered
    - CoAP Content-Format numbers or
    - Media Types and Media Type Parameters

- Background: While COSE included “content type” paralleling the JOSE “cty”, it failed to include the equivalent of “typ”

Why Do It?

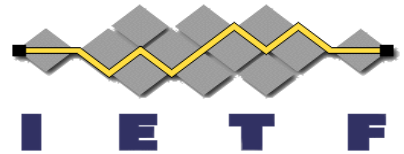
- Enable explicit typing, in parallel with the JWT BCP [RFC 8725]
- Distinguishing between “whole COSE object” and “payload” content types

Status

- Review feedback incorporated after IETF 117 in San Francisco
- Then adopted by the working group
- Now being recommended by draft-ietf-cose-cwt-claims-in-headers
  - Based on feedback from Carsten Bormann
- Added language describing use of Entity Type parameters
  - Also based on feedback from Carsten Bormann
- -01 just published incorporating this feedback
  - No breaking changes
- No other feedback received since WG adoption

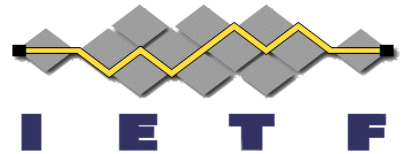
Next Steps

- Time for Working Group Last Call?



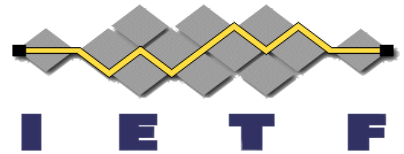
Backup Slides

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)




```
# COSE_Sign1
18([

  # Protected Header
  h'a2012…43833633531',
  # {
  #   "alg" : "ES256",
  #   1 : -7,
  #   "typ" : “application/receipt+cose",
  #   TBD (requested 15) : h'a2012…43833633531',
  #   … additional application specific headers …
  # }

  # Unprotected Header
  {
     ….
  },

  # Protected Payload
  …

  # Signature
  h'486…7f77ea'
])
```

```
# COSE_Sign1
18([

  # Protected Header
  h'a2012…43833633531',
  # {
  #   "alg" : "ES384",
  #   1 : -35,
  #   "typ" : "application/cwt",
  #   TBD (requested 15) : 61,
  #   … additional application specific headers …
  # }

  # Unprotected Header
  {
     ….
  },

  # Protected Payload
  …

  # Signature
  h'486…7f77ea'
])
```