cbor

2019-01-16 virtual interim

Agenda

CBORbis

— Look through updates that led to –05
— (Let's do this first as Paul has to leave 1825Z)

CDDL, Tags

— Contemplate (lack of) progress

CBORbis status

Many issues and pull requests are handled now
(thanks to the contributors!)

— Remaining pull requests:
  — Well-formed, valid (#17)
  — Validity for tagged items (#18)
— Also, 9 open issues
  — Most point to potential editorial improvements
  — #51: Fix pseudo-code and language about non-well-formed Simple (MT7)

Do these next, ➔ –06 (4 weeks from nowish?)

CBORbis −05

−05 submitted 2019-01-15
−04 was 2018-10-23

Technical work (1)

Clarify that non-finite values for Tag 1 (UNIX time) are application-defined (as negative values already are).
(🎊🎉 we are at half time between Y2K and S31B!)

Describe preferred serialization of bignums (Tag 2/3):

— Leave out leading zeroes

— Explain that 2(h'') is not a preferred serialization of anything (but still means 0)

Technical work (2): base64(url) padding bikeshed

Background: In CBOR➔JSON converters, tags 22 and 23 generate base64(url) from byte strings:
This needs to be **deterministic** or the tags are useless.

— RFC 7049: No padding emitted for base64url, silence about base64 classic (just ➔ RFC4648)

— This should have been interpreted as defaulting to RFC 4648 defaults (do padding!), but wasn't

— Opportunity: Find out how RFCs **actually** use base64 classic in JSON, do the **right thing**

Technical work (3): base64 classic padding survey

Surprise: In RFCs, base64 classic data is represented in JSON **with padding** (and **no** exceptions were found).

— RFC 7265 (jCal), RFC 7515 (JWS: classic for x5c etc.), RFC 7711 (POSH), RFC 7951 (YANG-JSON).

Result (PR #48):
stick with the intention of RFC 7049 and just clarify it.

(Side effect: 4 Errata for other RFCs submitted/prepared.)

Editorial work

— Clean up text for "break" and indefinite (JY, PR #43)

— Terminology

   — parse ➜ decode (JY, PR #42)

— Remove some weird text about security miracles done by gatekeepers and strict decoders (LL, #44)

— Some more expressive section headings

— Reorder some earlier new text for clarity; typos

Not to forget: Work outside the draft

Work on test vectors (in particular: failing ones)

CDDL status (no change)

All COMMENTS should now be addressed in <u>editor's copy</u>.

One DISCUSS left (by Eric). Answered Eric's most recent mail in https://mailarchive.ietf.org/arch/msg/cbor/8nj4r-9YKKHeilGdlxxggajXwuo

One todo left from that mail:

— Paraphrase PEG so no normative reference is needed.

CDDL plan

— Write that PEG summary
(Find drafts in editor's copy, discuss 2019-01-30)

Then:

— Submit cddl-07

— Get confirmation from Eric that the other items are covered (non-blocking)

— Clear the DISCUSS