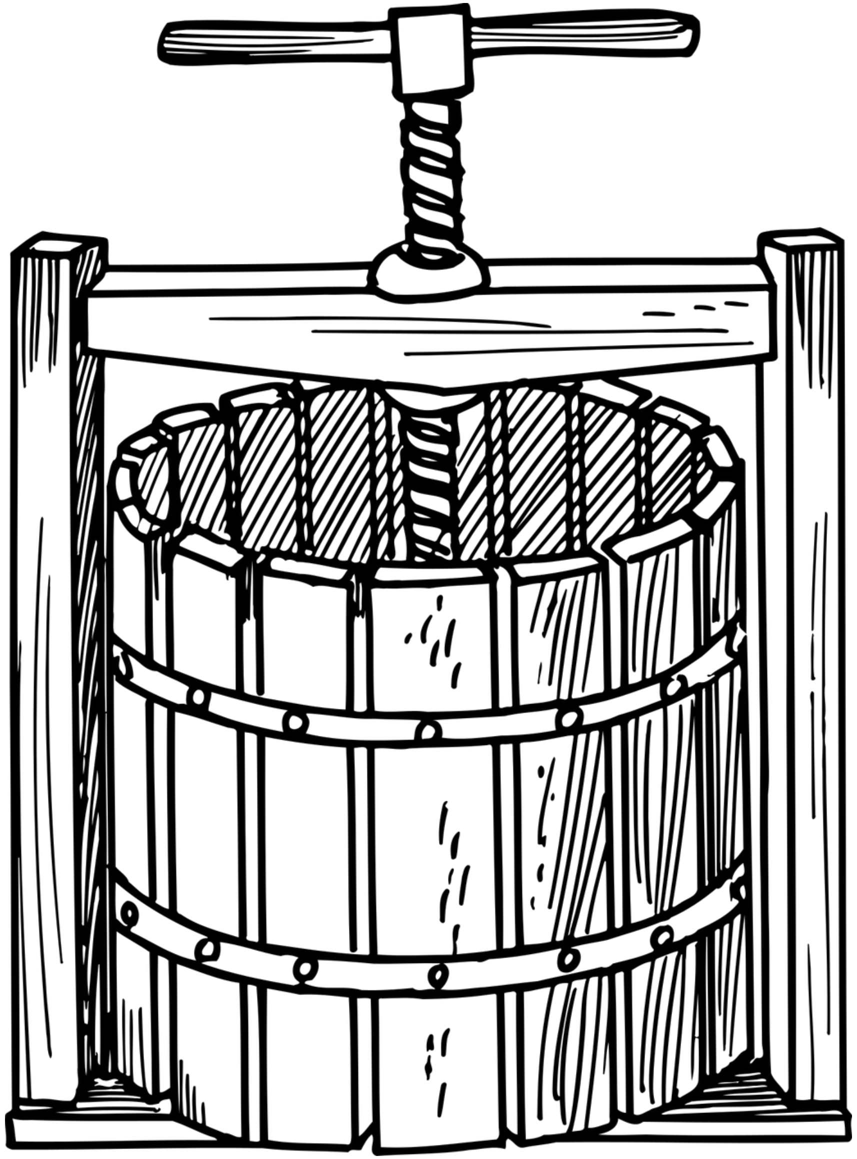


CBOR Encoding of X.509 Certificates (C509 Certificates)

draft-mattsson-cose-cbor-cert-compress-08

COSE, IETF 110, John Preuß Mattsson

C509 Certificate Scope

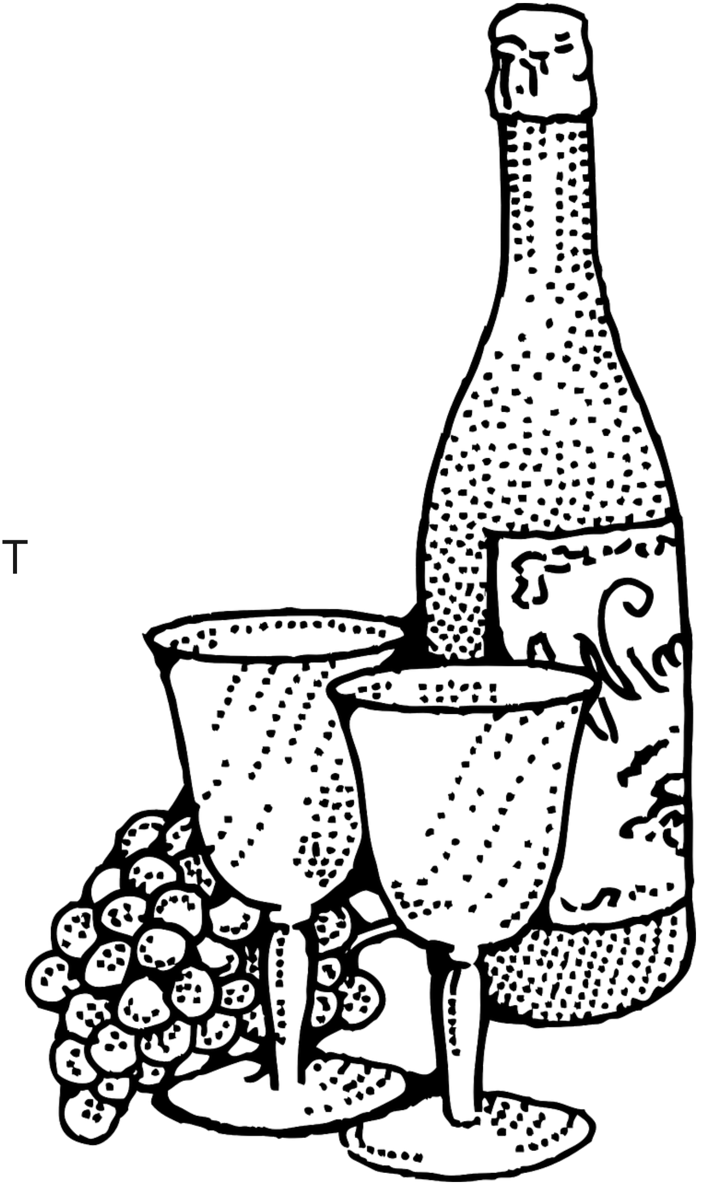
- High level goal: *"Make sweet CBOR wine from sour ASN.1 grapes"*

- Began as optimal CBOR encoding of a subset of RFC 7925.
- Shifted to cover much of RFC 5280.

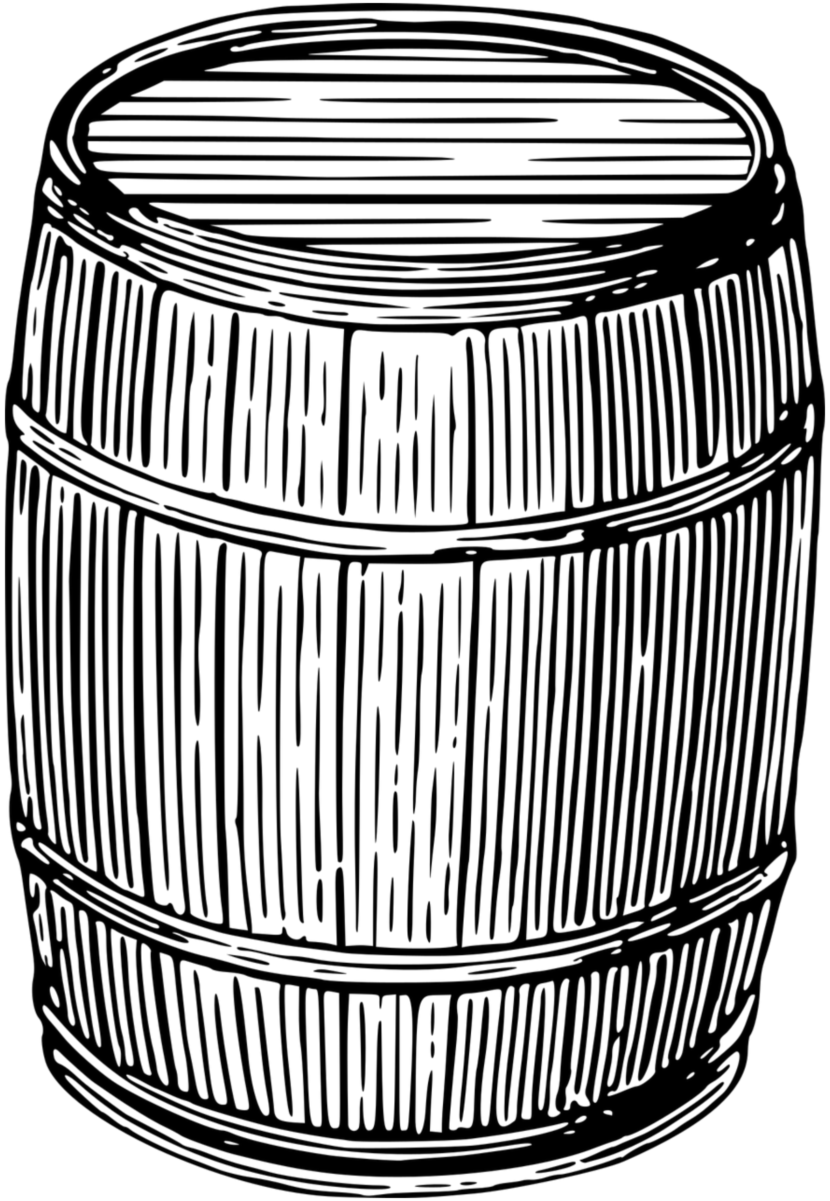
Scope:

- Define CBOR encoding for a large subset of RFC 5280
- Close to optimally compact encoding of certificates profiled for constrained IoT
  - RFC 7925
  - draft-ietf-uta-tls13-iot-profile
  - IEEE 802.1AR
- The CBOR encoded X.509 certificates are called "C509 Certificates"
- Make registrations so that C509 certificates can be used in COSE and TLS.

("C509" is a working title – to be confirmed by the COSE WG. Later.)



List of Changes



Changes from -03 to -08

Since IETF 109

From -03 to -05:
https://datatracker.ietf.org/meeting/interim-2020-cose-06/materials/slides-interim-2020-cose-06-sessa-cbor-certificates-00.pdf

From -05 to -06:
https://datatracker.ietf.org/meeting/interim-2021-cose-01/materials/slides-interim-2021-cose-01-sessa-cbor-certificates-00.pdf

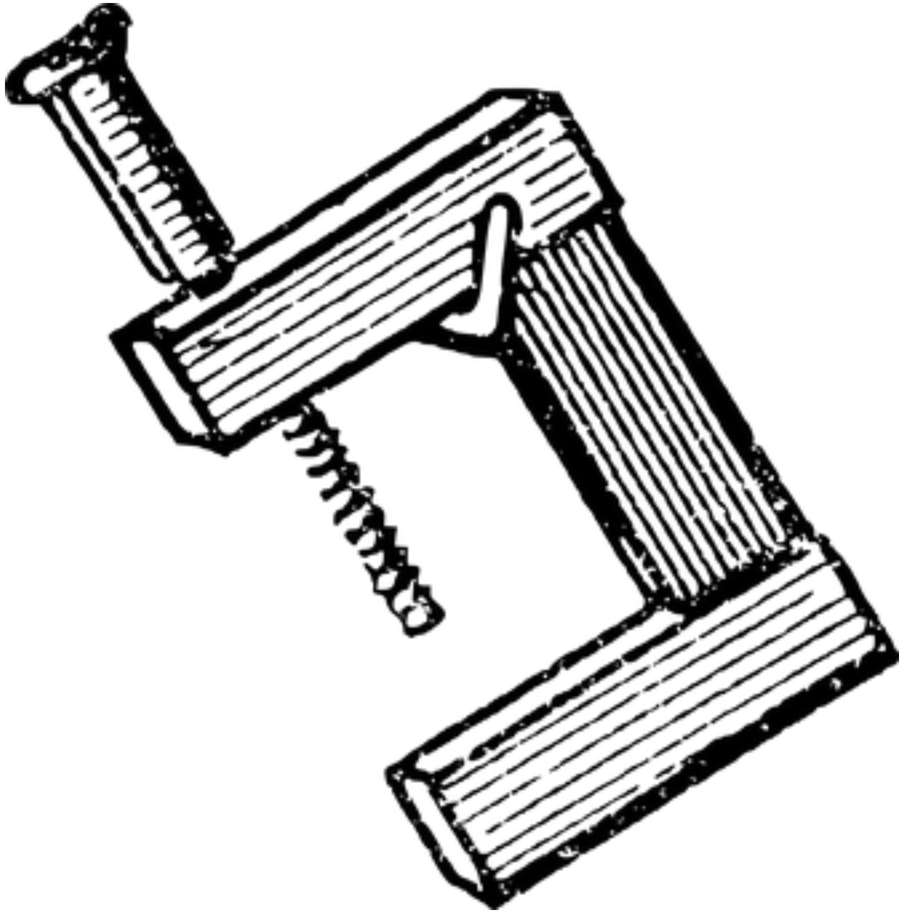
Changes from -06 to -07 to -08

Changes from -06 to -07

- Section 7 “Natively Signed CBOR Certificates“ removed
  - Request by Michael
  - Content essentially already integrated in the draft
  - Only missing info put into two paragraphs in the introduction
- Changed name of “CBOR Certificates”
  - Request by Michael & Carsten
  - Working title: “C509 Certificates” (data structure still called “CBORCertificate”)
- IANA registration of COSE header parameters
  - Changes to c5b, c5c, c5t, and c5u header parameters based on x509 discussion.
  - New structure COSE_C5 = [+ CBORCertificate]
    - Further changes waiting for conclusion on X.509 issues
- IANA registration of CBOR tag
  - Tagged COSE_C5
  - Ordered chain of C509 certificates

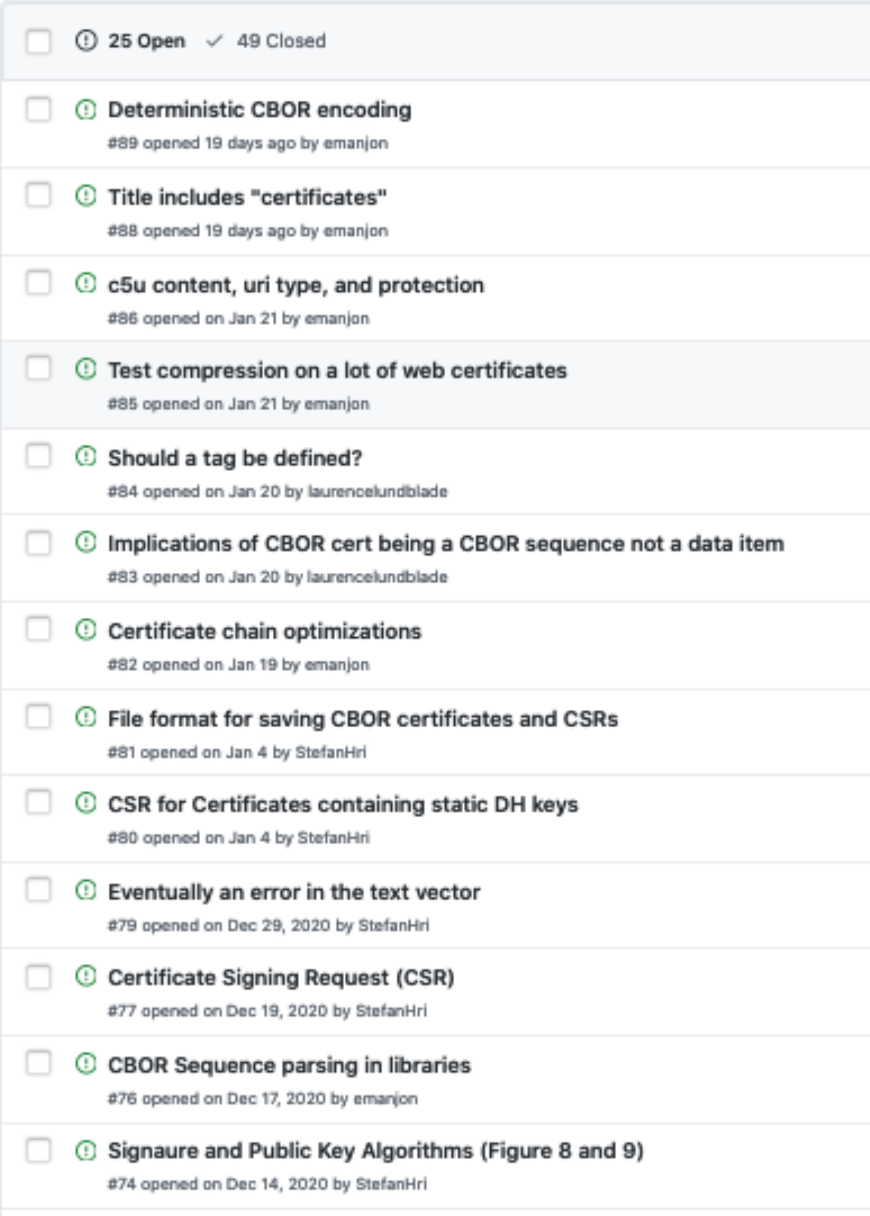
Changes from -07 to -08

- Layout. PR by Carsten, thanks!



Open Issues

Open Issues



□ 25 Open ✓ 49 Closed

□ Deterministic CBOR encoding
#89 opened 19 days ago by emanjon

□ Title includes "certificates"
#88 opened 19 days ago by emanjon

□ c5u content, uri type, and protection
#86 opened on Jan 21 by emanjon

□ Test compression on a lot of web certificates
#85 opened on Jan 21 by emanjon

□ Should a tag be defined?
#84 opened on Jan 20 by laurencelundblade

□ Implications of CBOR cert being a CBOR sequence not a data item
#83 opened on Jan 20 by laurencelundblade

□ Certificate chain optimizations
#82 opened on Jan 19 by emanjon

□ File format for saving CBOR certificates and CSRs
#81 opened on Jan 4 by StefanHri

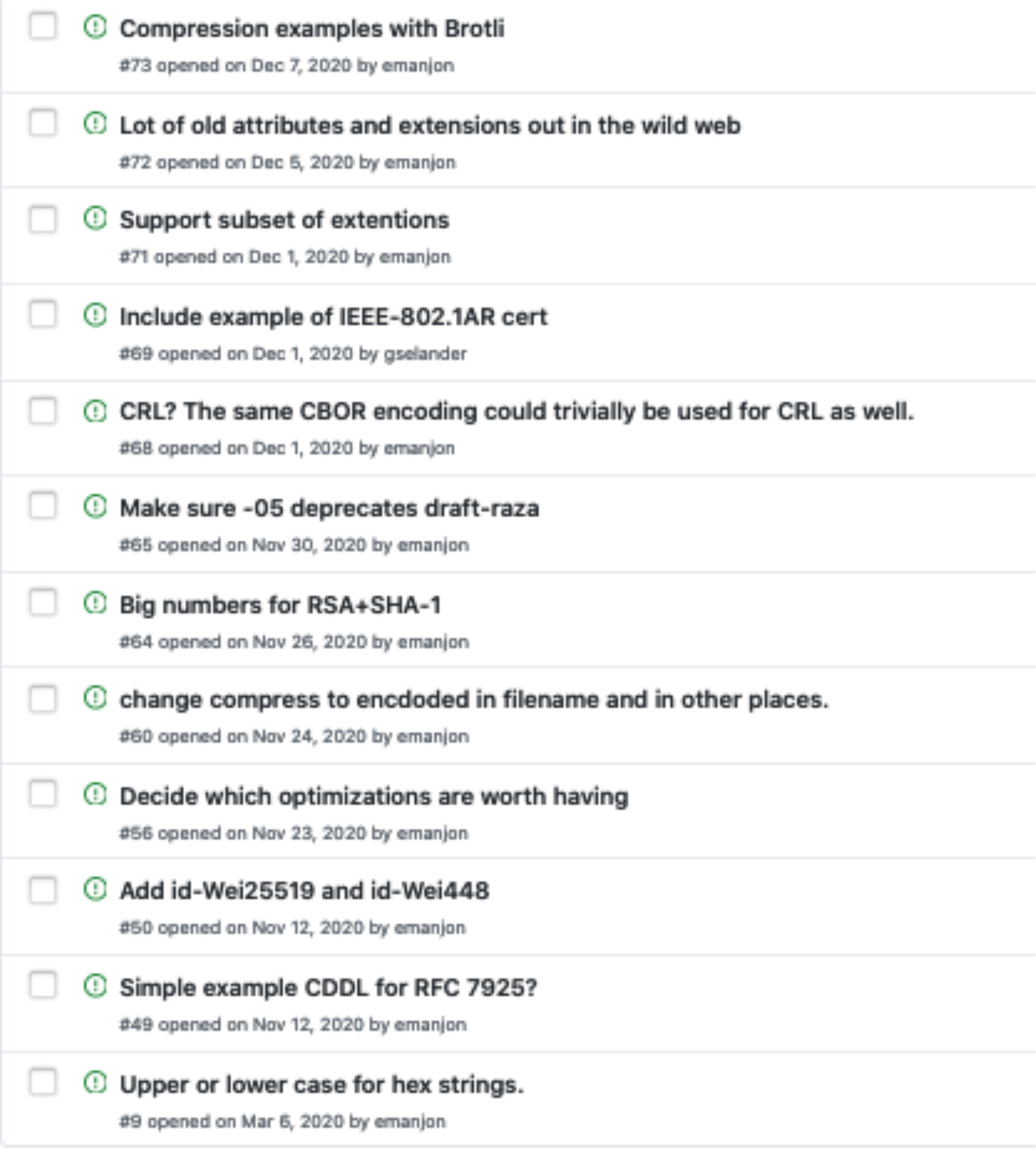
□ CSR for Certificates containing static DH keys
#80 opened on Jan 4 by StefanHri

□ Eventually an error in the text vector
#79 opened on Dec 29, 2020 by StefanHri

□ Certificate Signing Request (CSR)
#77 opened on Dec 19, 2020 by StefanHri

□ CBOR Sequence parsing in libraries
#76 opened on Dec 17, 2020 by emanjon

□ Signaure and Public Key Algorithms (Figure 8 and 9)
#74 opened on Dec 14, 2020 by StefanHri



□ Compression examples with Brotli
#73 opened on Dec 7, 2020 by emanjon

□ Lot of old attributes and extensions out in the wild web
#72 opened on Dec 5, 2020 by emanjon

□ Support subset of extentions
#71 opened on Dec 1, 2020 by emanjon

□ Include example of IEEE-802.1AR cert
#69 opened on Dec 1, 2020 by gselander

□ CRL? The same CBOR encoding could trivially be used for CRL as well.
#68 opened on Dec 1, 2020 by emanjon

□ Make sure -05 deprecates draft-raza
#65 opened on Nov 30, 2020 by emanjon

□ Big numbers for RSA+SHA-1
#64 opened on Nov 26, 2020 by emanjon

□ change compress to encdoded in filename and in other places.
#60 opened on Nov 24, 2020 by emanjon

□ Decide which optimizations are worth having
#56 opened on Nov 23, 2020 by emanjon

□ Add id-Wei25519 and id-Wei448
#50 opened on Nov 12, 2020 by emanjon

□ Simple example CDDL for RFC 7925?
#49 opened on Nov 12, 2020 by emanjon

□ Upper or lower case for hex strings.
#9 opened on Mar 6, 2020 by emanjon

Selected Issues

Selected Issues

- <new issue> what to write in common name / subject alt name
- Deterministic CBOR encoding (#89)
- Should a tag be defined? (#84)
- Implications of CBOR cert being a CBOR sequence not a data item (#83)
- File format for saving CBOR certificates and CSRs (#81)
- CRL? The same CBOR encoding could trivially be used for CRL as well. (#68)

<new issue> what to write in common name / subject alt name

- **draft-ietf-uta-tls13-iot-profile-01**
- "If the EUI-64 format is used to identify the subject of a client certificate, it MUST be encoded in a subjectAltName"

- **draft-rsalz-use-san-00**
  - "updates RFC 6125 to remove commonName as a way to identify the server; just use subjectAltName."
  - "The CN-ID MUST NOT be used."
  - "The appropriate value in the subjectAltName extension MUST be used to get the presented identity of the server."

Deterministic CBOR encoding (#89)

- The draft should refer to deterministic CBOR encoding for integers
  - Section 4.2 in RFC 8949

- This was always the intention but is not mentioned in the draft.

Implications of CBOR cert being a CBOR sequence not a data item (#83)

- Note that cbor.me and certain CDDL tools now supports CBOR sequences

File format for saving CBOR certificates and CSRs (#81)

- How to apply CBOR file magic to C509?
  - https://datatracker.ietf.org/doc/draft-ietf-cbor-file-magic/

- What to save? A chain? A bag? A single cert? A tagged chain?

Should a tag be defined? (#84)

- COSE_C5 = [+ CBORCertificate]
  - Chain
  - Bag
  - Save to file
  - Media type
- CBOR array at least needed for tag

- Tagged COSE_C5
  - Ordered chain of C509 certificates

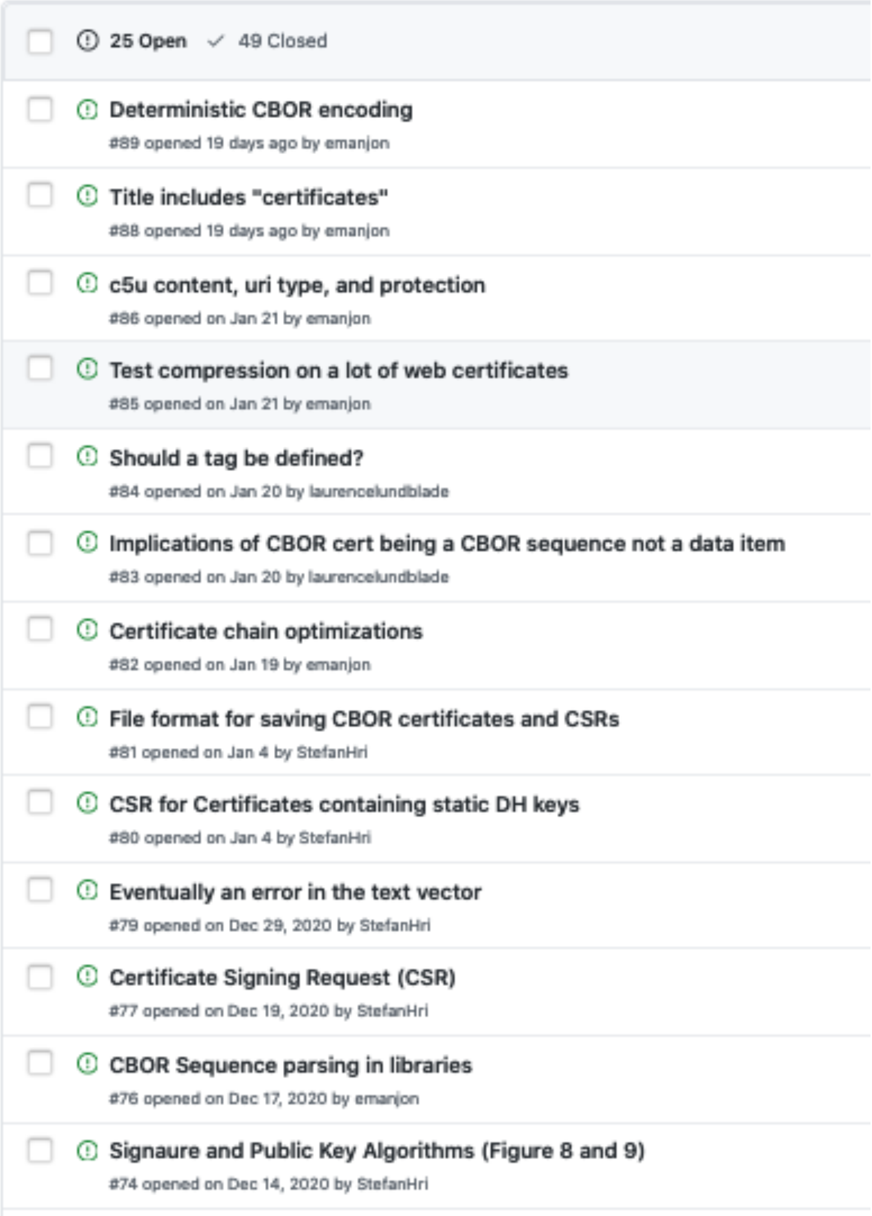
CRL? The same CBOR encoding could trivially be used for CRL as well. (#68)

- Comment that OCSP stapling would probably be more relevant

- Needed for cose-x509 in general?

- Probably also needed in e.g. draft-ingles-eap-edhoc
  - EAP-TLS 1.3 has recently mandated revocation checking.

Questions / comments?



□ 25 Open ✓ 49 Closed

□ Deterministic CBOR encoding
#89 opened 19 days ago by emanjon

□ Title includes "certificates"
#88 opened 19 days ago by emanjon

□ c5u content, uri type, and protection
#86 opened on Jan 21 by emanjon

□ Test compression on a lot of web certificates
#85 opened on Jan 21 by emanjon

□ Should a tag be defined?
#84 opened on Jan 20 by laurencelundblade

□ Implications of CBOR cert being a CBOR sequence not a data item
#83 opened on Jan 20 by laurencelundblade

□ Certificate chain optimizations
#82 opened on Jan 19 by emanjon

□ File format for saving CBOR certificates and CSRs
#81 opened on Jan 4 by StefanHri

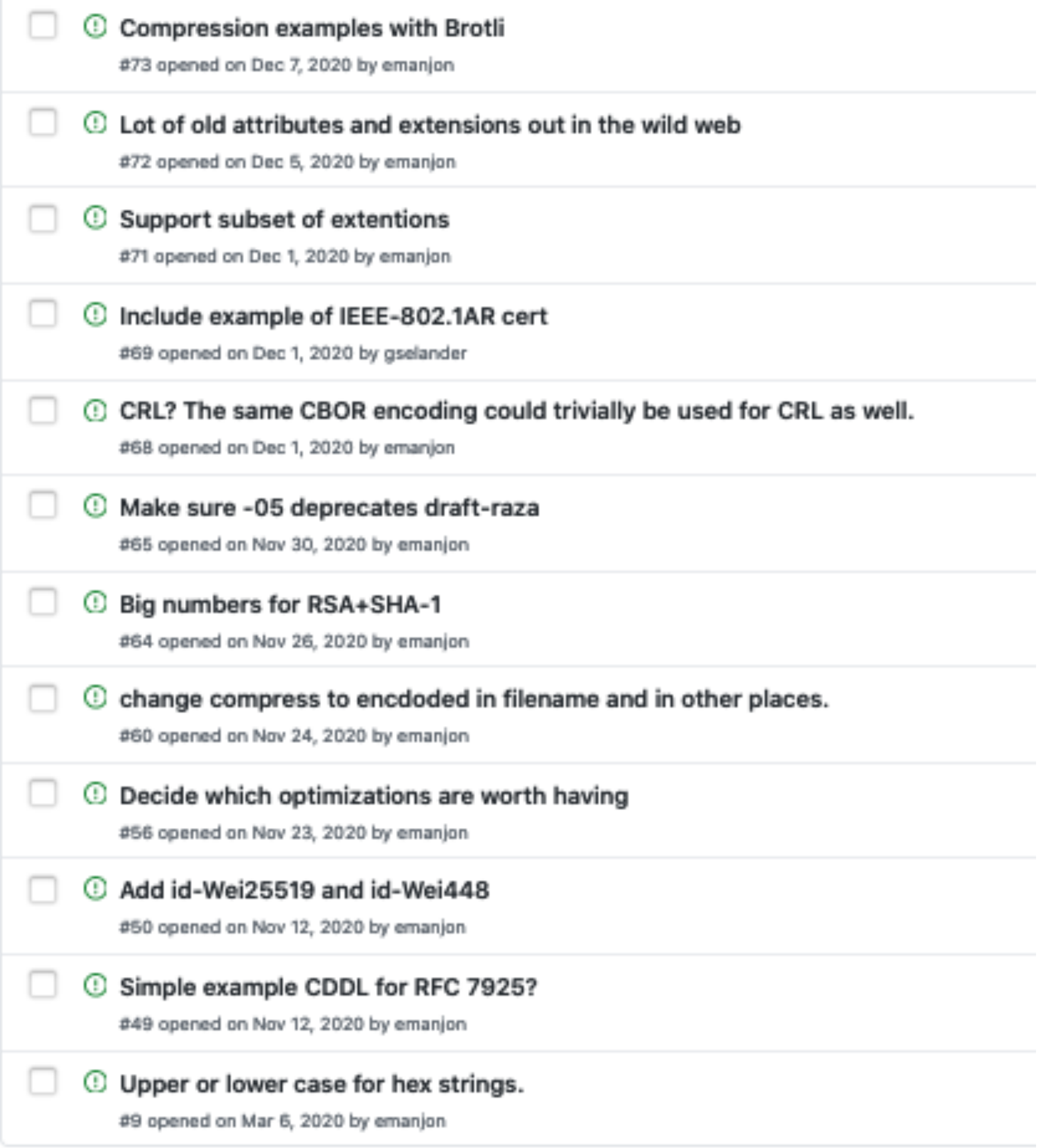
□ CSR for Certificates containing static DH keys
#80 opened on Jan 4 by StefanHri

□ Eventually an error in the text vector
#79 opened on Dec 29, 2020 by StefanHri

□ Certificate Signing Request (CSR)
#77 opened on Dec 19, 2020 by StefanHri

□ CBOR Sequence parsing in libraries
#76 opened on Dec 17, 2020 by emanjon

□ Signaure and Public Key Algorithms (Figure 8 and 9)
#74 opened on Dec 14, 2020 by StefanHri



□ Compression examples with Brotli
#73 opened on Dec 7, 2020 by emanjon

□ Lot of old attributes and extensions out in the wild web
#72 opened on Dec 5, 2020 by emanjon

□ Support subset of extentions
#71 opened on Dec 1, 2020 by emanjon

□ Include example of IEEE-802.1AR cert
#69 opened on Dec 1, 2020 by gselander

□ CRL? The same CBOR encoding could trivially be used for CRL as well.
#68 opened on Dec 1, 2020 by emanjon

□ Make sure -05 deprecates draft-raza
#65 opened on Nov 30, 2020 by emanjon

□ Big numbers for RSA+SHA-1
#64 opened on Nov 26, 2020 by emanjon

□ change compress to encdoded in filename and in other places.
#60 opened on Nov 24, 2020 by emanjon

□ Decide which optimizations are worth having
#56 opened on Nov 23, 2020 by emanjon

□ Add id-Wei25519 and id-Wei448
#50 opened on Nov 12, 2020 by emanjon

□ Simple example CDDL for RFC 7925?
#49 opened on Nov 12, 2020 by emanjon

□ Upper or lower case for hex strings.
#9 opened on Mar 6, 2020 by emanjon

How to progress until next meeting

- Reviews
- Implementations
- Github issues/ Discussion on the list