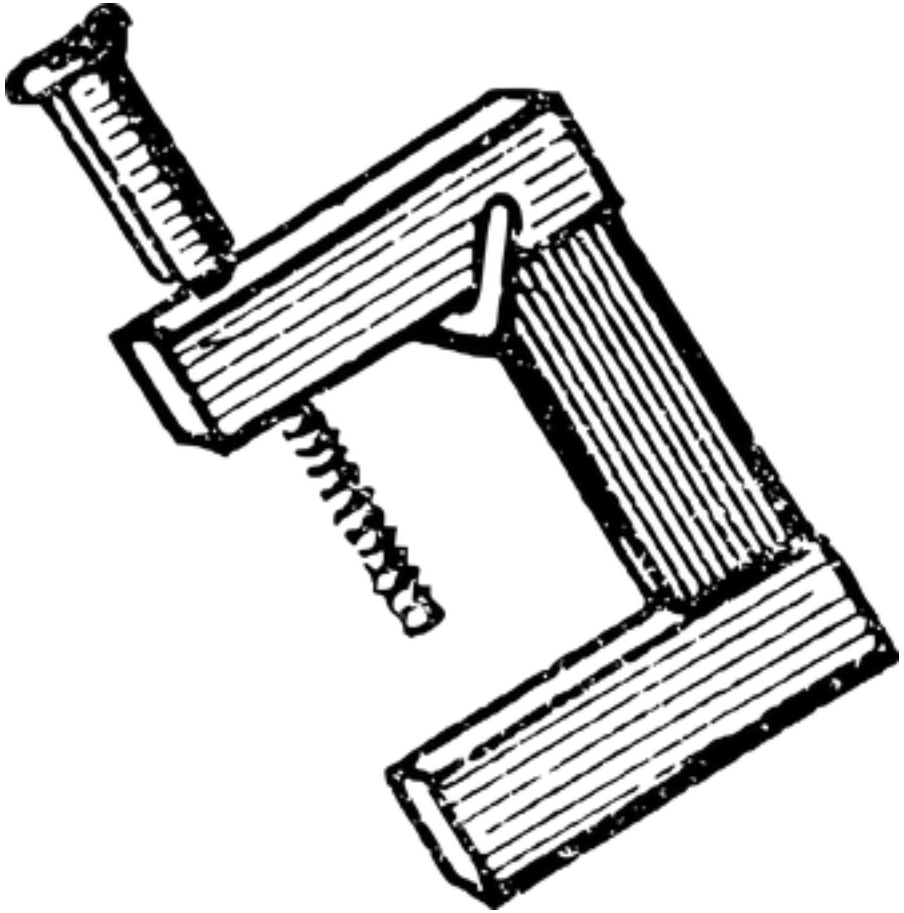


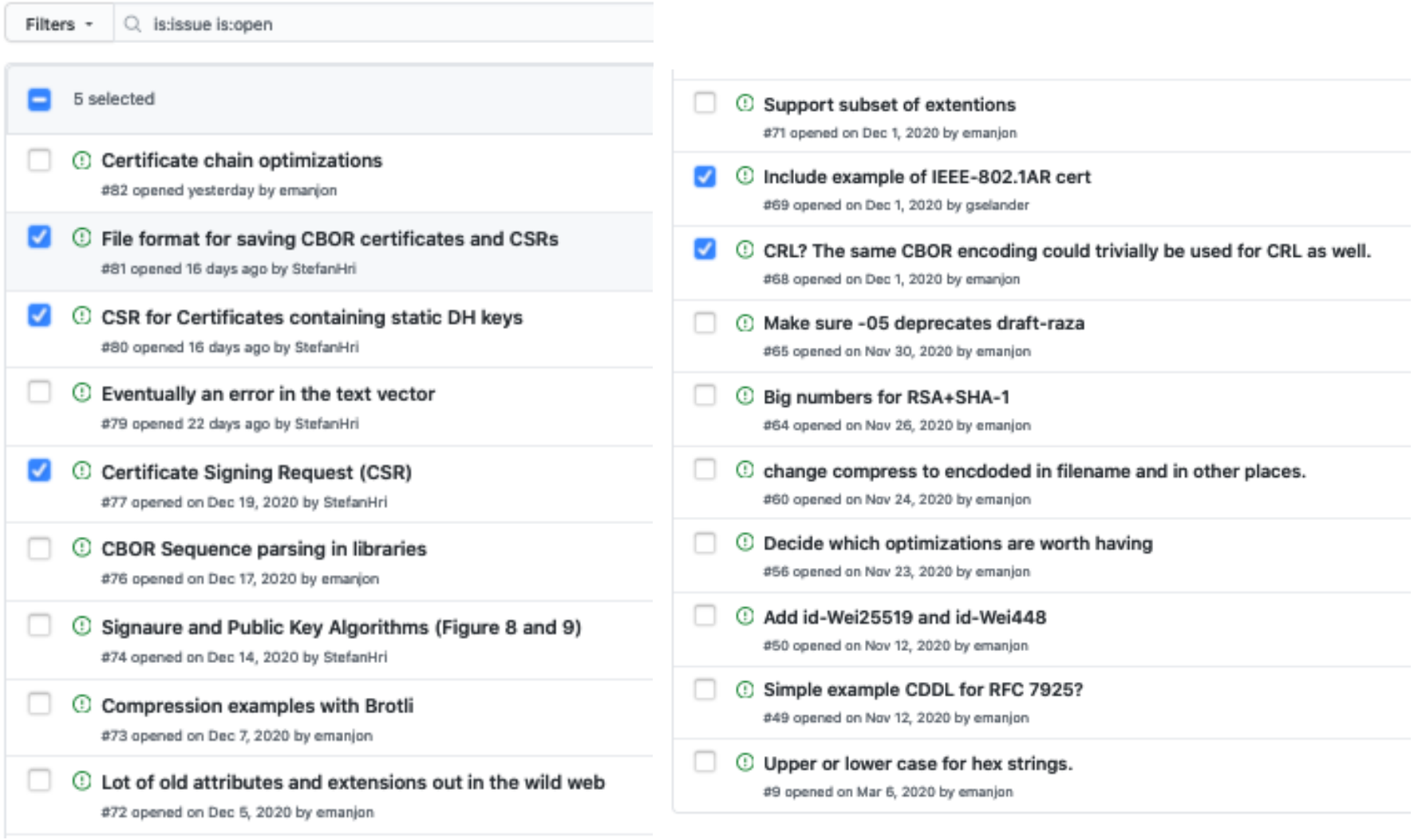
Selected Issues

draft-mattsson-cose-cbor-cert-compress-06

IETF COSE WG interim Jan 20, 2021

Open issues

https://github.com/EricssonResearch/CBOR-certificates



CBOR encoding of CSR (#77)

- Request to specify CBOR encoding of Certificate Signing Request (CSR, RFC 2986)

- A first sketch exists in another draft (draft-selander-ace-coap-est-oscore-04):

```
certificate request = (
   subject_common_name : bstr,
   public_key : bstr
   signature : bstr,
   ? ( signature_alg : int, public_key_info : int )
)
```

- This format needs further refinement. Can reuse encodings defined in CBOR certificates draft
  - subjectPublicKeyAlgorithm
  - Encoding of attributes specifying extension requests
- Beneficial for deployment if specification and time line of CBOR encoded CSR aligned with CBOR certificates
- The contributor of CBOR encoded CSR is an author of the CBOR certificates draft

- **Shall we move the specification of CBOR encoded CSR to this draft/separate COSE draft?**

CSR for static DH keys (#80)

- Request to specify encoding of CSR for static DH keys

- One solution is provided by RFC 6955 (Diffie-Hellman Proof-of-Possession Algorithms)
  - Proof of possession of static ECDH defined in section 6
  - Compute shared secret from DH keys of requesting endpoint and CA
  - Derive key for MAC
  - Substitute signature with MAC in CSR

- Replacing signature with MAC reduces overhead
  - One reason why static DH is relevant
  - Applies also to CSR
- Requires static DH key of CA
  - Trust anchor may be obtained from CA as part of enrolment functionality (see e.g. EST)

- **Same question: Shall we specify encoding in this draft/separate COSE draft?**

CBOR encoding of CRL (#68)

- Encoding of CRL is a straightforward addition to existing specification.
- OSCP response?

- **Include in the CBOR certificate draft or separate draft?**

File format of CBOR certificate (#81)

- **File extension for CBOR cert?**
- **Same question for CBOR encoded CSR, CRL, OSCP.**

Example IEEE-802.1AR (#69)

— @mcr kindly volunteered to provide an example IEEE-802.1AR certificate in January