



Selected Issues

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

IETF COSE WG interim Jan 20, 2021

Open issues

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

Filters -

5 selected

- Certificate chain optimizations**
#82 opened yesterday by emanjon
- File format for saving CBOR certificates and CSRs**
#81 opened 16 days ago by StefaniHri
- CSR for Certificates containing static DH keys**
#80 opened 16 days ago by StefaniHri
- Eventually an error in the text vector**
#79 opened 22 days ago by StefaniHri
- Certificate Signing Request (CSR)**
#77 opened on Dec 19, 2020 by StefaniHri
- CBOR Sequence parsing in libraries**
#76 opened on Dec 17, 2020 by emanjon
- Signature and Public Key Algorithms (Figure 8 and 9)**
#74 opened on Dec 14, 2020 by StefaniHri
- 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 encoded 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

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