CBOR Encoded X.509 Certificates

draft-ietf-cose-cbor-encoded-cert-04□05

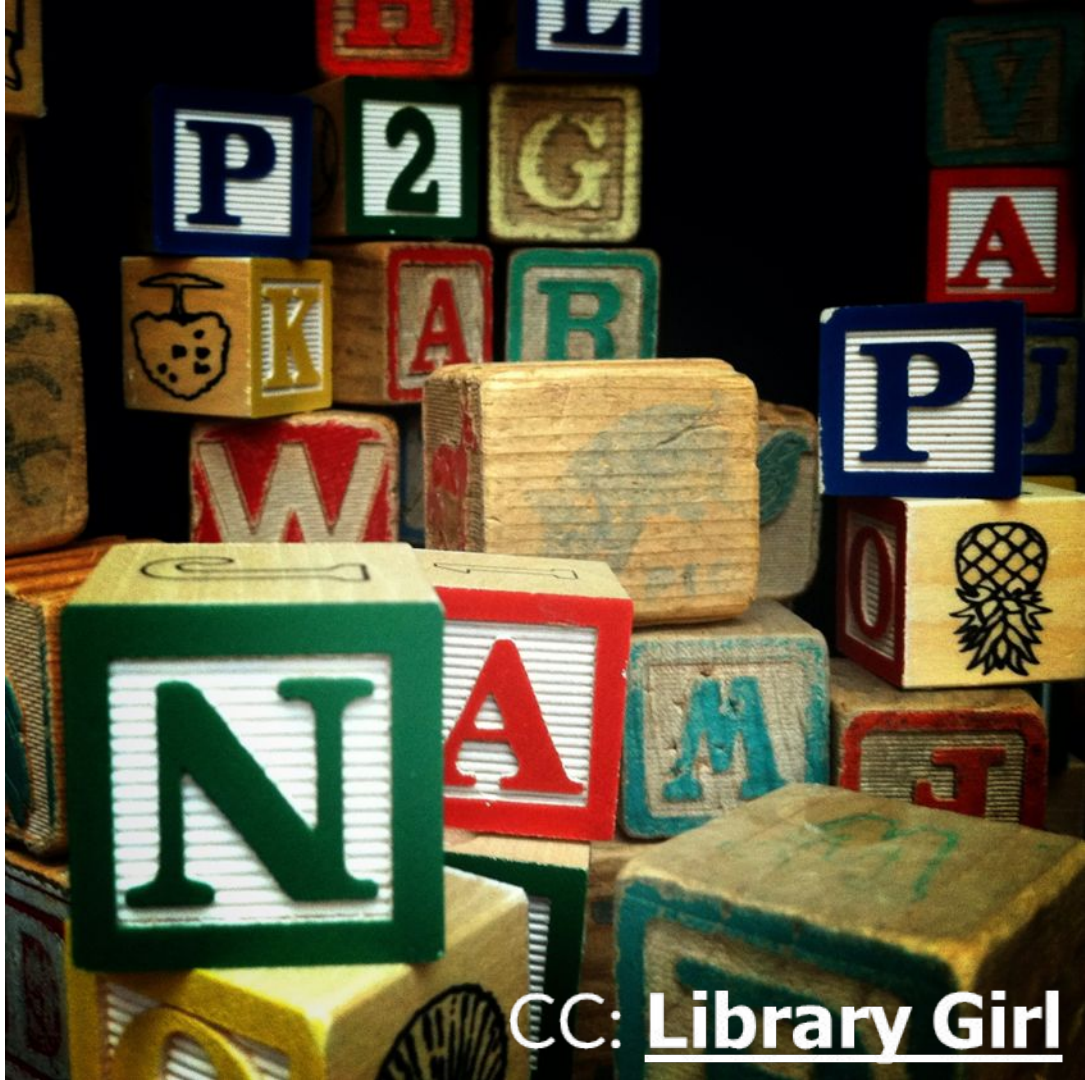
IETF 115, 2022-11-08

G. Selander, J. Mattsson (Ericsson AB),

Joel Höglund, S. Raza (RISE),

M. Furuhed (Nexus Group)

Status, ongoing work and issues for further discussions



Overall trade-offs and discussion themes

- Compactness / saving bytes
- Convenient to parse and process
- Generality, how to encode as many relevant X.509 certificates as possible

Discussions: Mixed optimizations (#56)

Ongoing discussions on if a number of minor optimizations are worth keeping.

Our conclusion at the moment is that these are sufficiently useful to keep:

- subjectAltName 2 bytes
- keyUsage extension 2 bytes
- Issuer 3 bytes

RI. SE

Discussions: Big numbers for RSA+SHA-1 (#64)

Background: although SHA-1 usage is supposed to be phased out, it's still used for many X.509 root certificates, which do need to be handled.

Our proposal: use a 2 byte assignment to cover these cases

Proposed alternative: "punish" by a longer (5 byte) id.

RI. SE

Discussions: CRL and OCSP encodings (#68)

The C509 CBOR encoding could trivially be used for CRL and OCSP as well

RISE+Ericsson have a master thesis worker who has been looking into related issues, and the result will be incorporated into the C509 work

Discussions: Signature and Public Key Algorithms (#74)

There has been a request to add more info on the suitability of different algorithms for IoT:

We are working on adding more details on this.

Discussions: Certificate chain optimizations (#82)

CBOR certs could provide optimizations for self-issues certificates as well as for certs that are sent in cert chains.

Q: Should CBOR certs provide optimizations for self-issued certs or chains?

- Potentially large savings.
- Added complexity, Makes CBOR compression two pass
- Could be handled through COSE headers + Brotli

 Our suggestion is to keep the implementations simple, avoiding two-pass

RI. SE

Discussions: Further comments from Ilari (#102)

There has been a number of insightful observations on the mailing list by Ilari Liusvaara, which we are investigating and addressing.

Here I will briefly mention some of them.

Discussions: Further comments from Ilari (#102)

- Name Constraints extensions encoding
  - updated to handle absent fields as null.

- SubjectDirectoryAttributes extensions encoding
  - now wrapped as cbor array

- Several minor fixes

Discussions: Further comments from Ilari (#102)

IP address block extension:

- Encoded as difference between addresses
- When encoding IPv6 addresses the differences can theoretically overflow CBOR uint.

We propose leave this as is, but clarify in the limitation in text.

RI. SE

Discussions: Further comments from Ilari (#102)

About the Authority Key Identifier extension:

Ilari made the observation that “about 1/10 lack keyid in AKI”

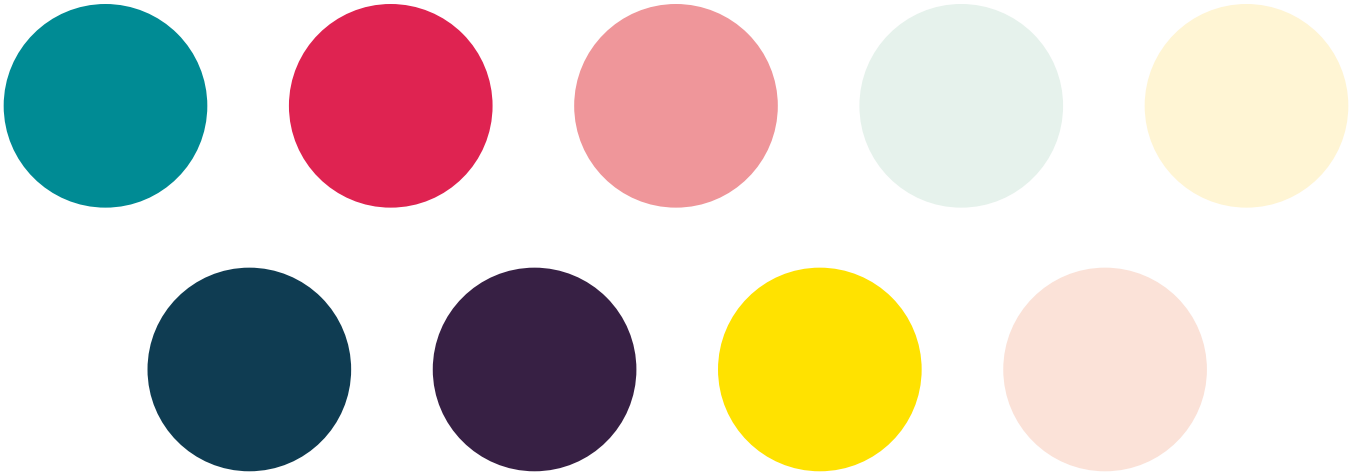
- We propose that absent keyid is encoded as null.

```
KeyIdentifierArray = [
    keyIdentifier: KeyIdentifier / null,
    authorityCertIssuer: GeneralNames,
    authorityCertSerialNumber: CertificateSerialNumber
]
```

What about the other fields:

- do they need null-encodings as well?

RI. SE



Joel Höglund

joel.hoglund@ri.se