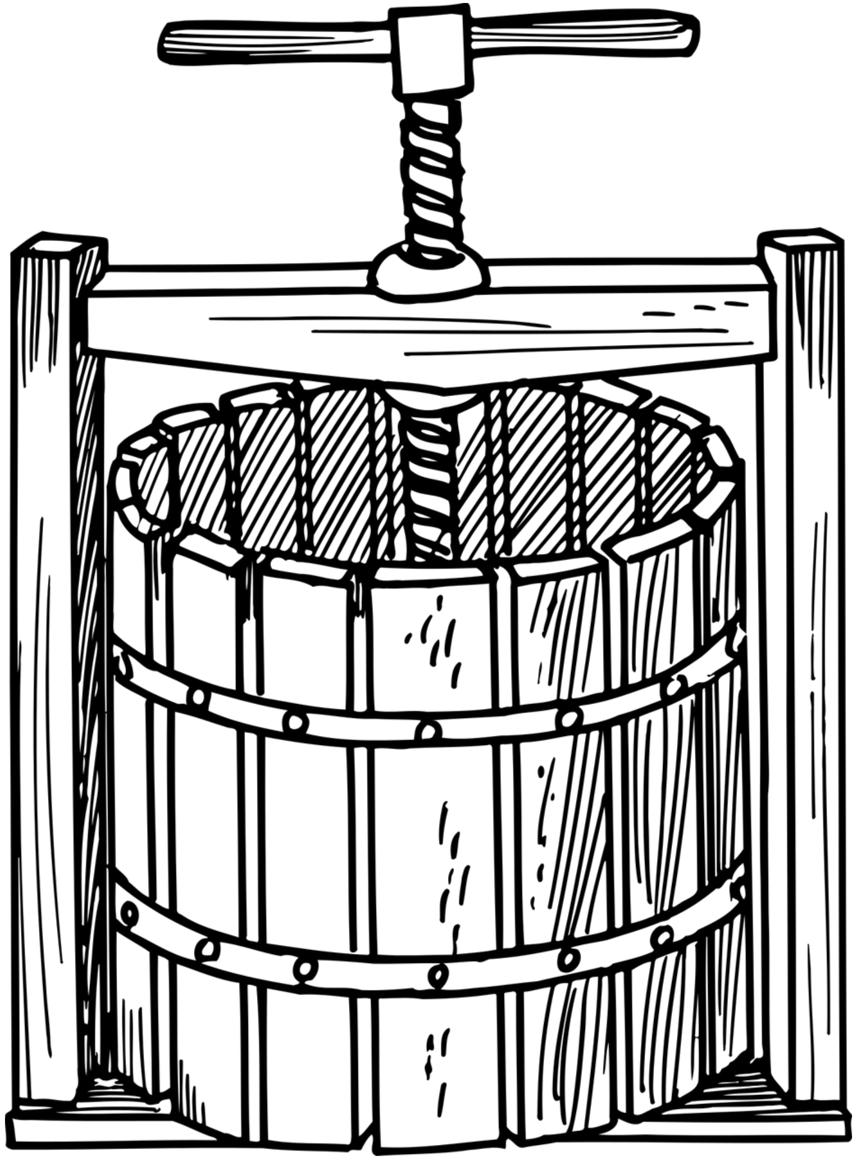
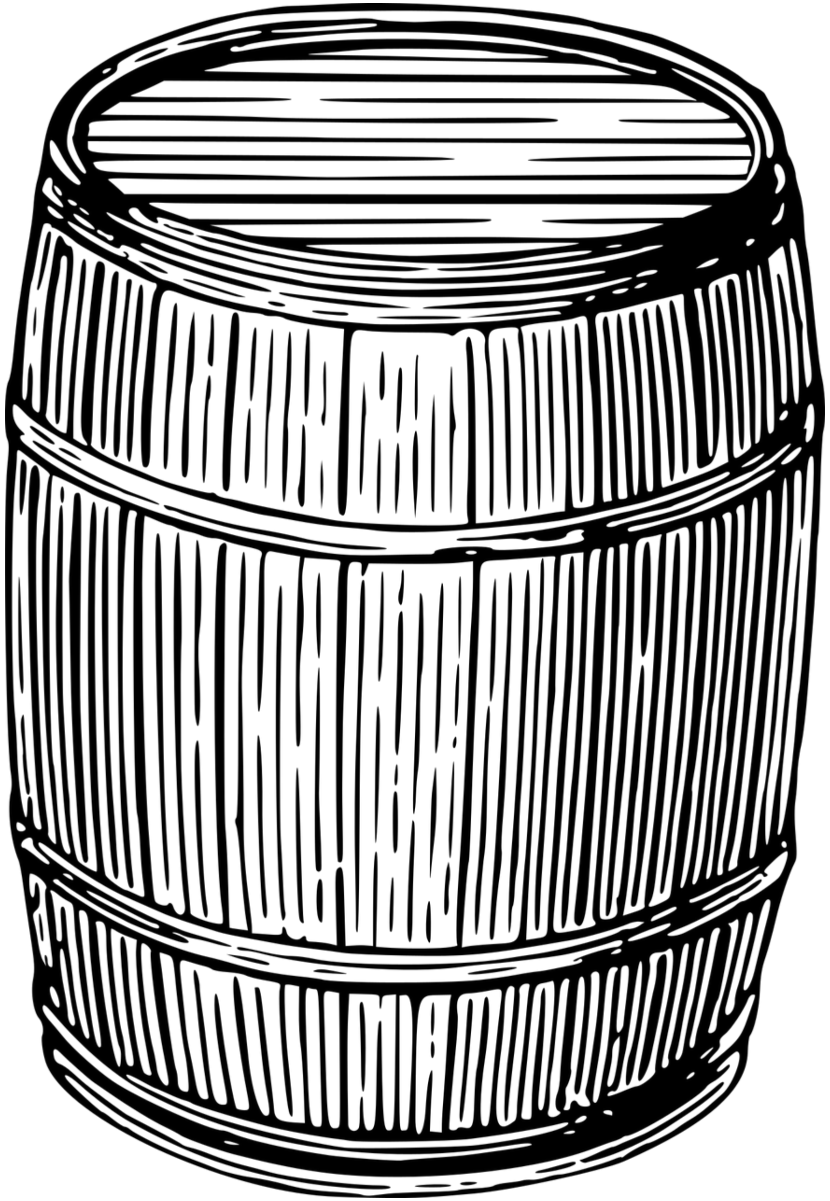


CBOR Encoding of X.509 Certificates (CBOR Certificates)

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

COSE, John Preuß Mattsson



Changes from -05 to -06

Changes from -05 to -06

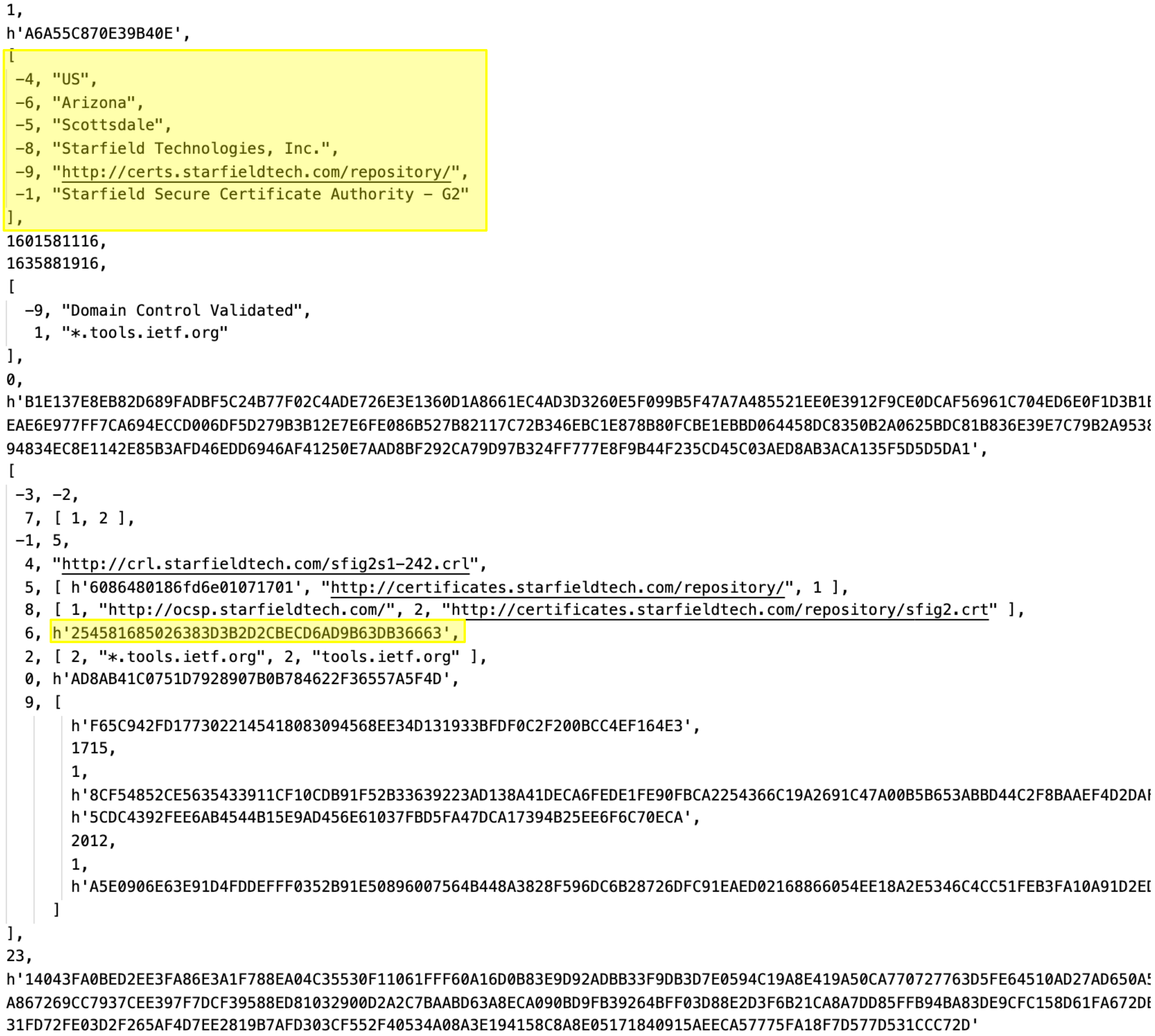
- Added references to the certificate profiles CAB baseline and RFC 8603.
- Added text in introduction that certificate chain sizes are major problems also in EAP and QUIC.
- Based on the certificates found on the web, attributes, extensions, and algorithms can now all be expressed with OID and raw DER byte strings.
- Optimized for a single attribute per RDN as all the certificates on the web seem to be following this practice.
- Added registration for StreetAdress and PostalCode (included in CAB baseline)
- Algorithms registries so that the int encodes the whole AlgorithmIdentifier including parameters.
- Changed ECDSA signatureValue encoding as the old one depended on the issuer public key algorithm. Optimize RSA public key encoding.
- Changed from zlib to brotli
- Significantly restructured IANA tables to make them better
- Subject private key for the example certificates.
- ASN.1 appendix removed
- Editorial changes

Plans and discussions for -07

Plans and discussions for -07 (or later)

- Example encoding of IEEE 802.1AR DevID.
- More deployment guidance for IoT, comment that it would be good to discuss how different algorithms affect size.
- Test the encoding on a large amount of certificates, hopefully millions.
    - **Summary of 1M lists:** https://hackertarget.com/top-million-site-list-download/
    - **Cisco Umbrella 1M**: http://s3-us-west-1.amazonaws.com/umbrella-static/index.html
    - **The Majestic Million**: http://s3-us-west-1.amazonaws.com/umbrella-static/index.html
    - **Tanco List:** https://tranco-list.eu/
- Finalize CBOR encoding specification for all extensions that are very common for HTTPS. Plan is to base support will be based on what is used on the web.
- Certificate chain encoding (TLS certificate message) showing sizes for DER, DER+Brotli, CBOR, CBOR+Brotli.

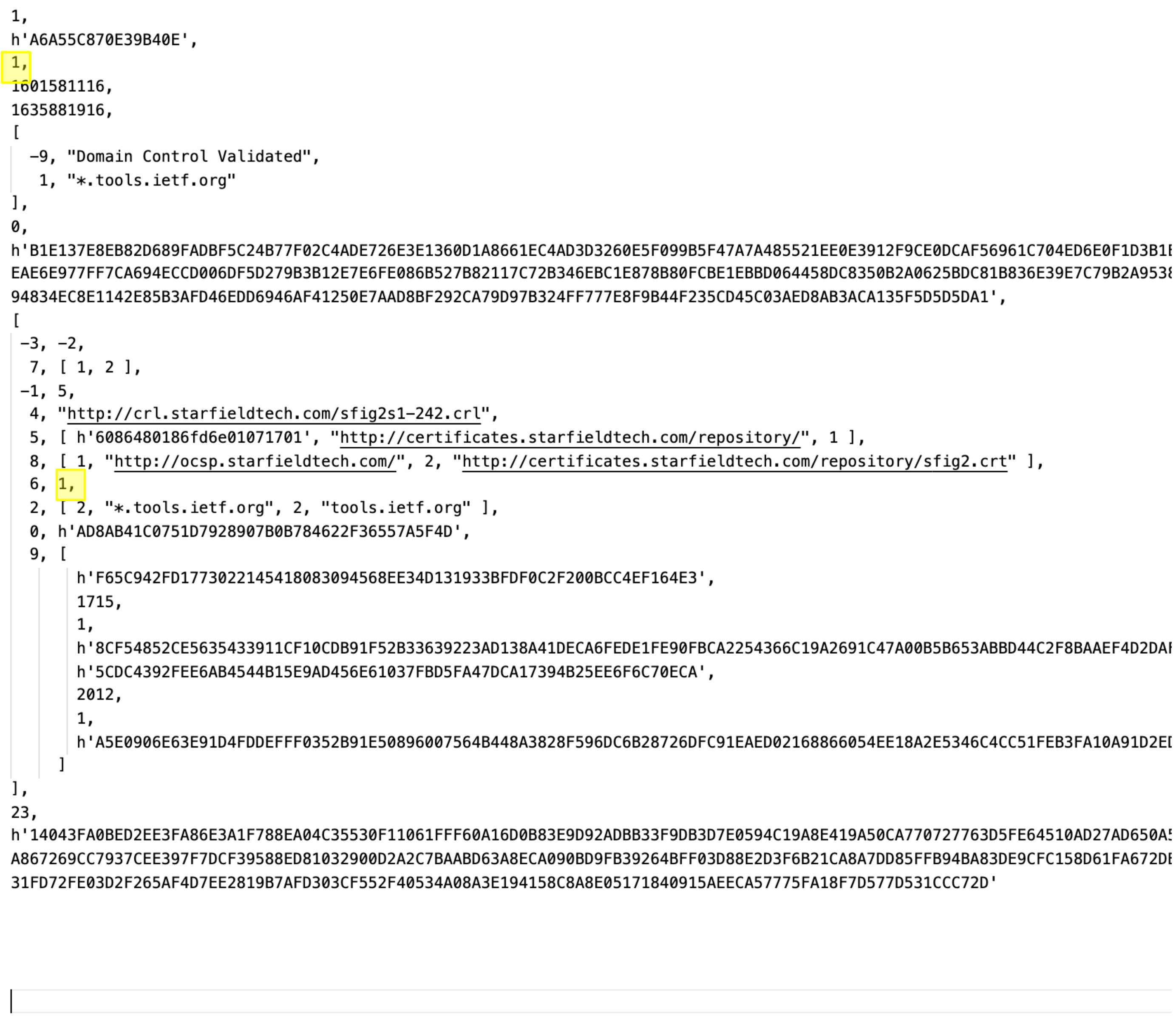
Certificate chain optimizations?



```
1,
h'A6A55C870E39B40E',
[
 -4, "US",
 -6, "Arizona",
 -5, "Scottsdale",
 -8, "Starfield Technologies, Inc.",
 -9, "http://certs.starfieldtech.com/repository/",
 -1, "Starfield Secure Certificate Authority - G2"
],
1601581116,
1635881916,
[
  -9, "Domain Control Validated",
   1, "*.tools.ietf.org"
],
0,
h'B1E137E8EB82D689FADBF5C24B77F02C4ADE726E3E1360D1A8661EC4AD3D3260E5F099B5F47A7A485521EE0E3912F9CE0DCAF56961C704ED6E0F1D3B1
EAE6E977FF7CA694ECCD006DF5D279B3B12E7E6FE086B527B82117C72B346EBC1E878B80FCBE1EBBD064458DC8350B2A0625BDC81B836E39E7C79B2A953
94834EC8E1142E85B3AFD46EDD6946AF41250E7AAD8BF292CA79D97B324FF777E8F9B44F235CD45C03AED8AB3ACA135F5D5D5DA1',
[
 -3, -2,
  7, [ 1, 2 ],
 -1, 5,
  4, "http://crl.starfieldtech.com/sfig2s1-242.crl",
  5, [ h'6086480186fd6e01071701', "http://certificates.starfieldtech.com/repository/", 1 ],
  8, [ 1, "http://ocsp.starfieldtech.com/", 2, "http://certificates.starfieldtech.com/repository/sfig2.crt" ],
  6, h'254581685026383D3B2D2CBECD6AD9B63DB36663',
  2, [ 2, "*.tools.ietf.org", 2, "tools.ietf.org" ],
  0, h'AD8AB41C0751D7928907B0B784622F36557A5F4D',
  9, [
       h'F65C942FD1773022145418083094568EE34D131933BFDF0C2F200BCC4EF164E3',
       1715,
       1,
       h'8CF54852CE5635433911CF10CDB91F52B33639223AD138A41DECA6FEDE1FE90FBCA2254366C19A2691C47A00B5B653ABBD44C2F8BAAEF4D2DA
       h'5CDC4392FEE6AB4544B15E9AD456E61037FBD5FA47DCA17394B25EE6F6C70ECA',
       2012,
       1,
       h'A5E0906E63E91D4FDDEFFF0352B91E50896007564B448A3828F596DC6B28726DFC91EAED02168866054EE18A2E5346C4CC51FEB3FA10A91D2E
     ]
],
23,
h'14043FA0BED2EE3FA86E3A1F788EA04C35530F11061FFF60A16D0B83E9D92ADBB33F9DB3D7E0594C19A8E419A50CA770727763D5FE64510AD27AD650A
A867269CC7937CEE397F7DCF39588ED81032900D2A2C7BAABD63A8ECA090BD9FB39264BFF03D88E2D3F6B21CA8A7DD85FFB94BA83DE9CFC158D61FA672D
31FD72FE03D2F265AF4D7EE2819B7AFD303CF552F40534A08A3E194158C8A8E05171840915AEECA57775FA18F7D577D531CCC72D'
```

- A lot of duplicated information in certificate chain/bags like TLS certxample encoding of IEEE 802.1AR DevID.
- The issuer field is is often duplicate of a subject field from a certificate in the chain.
- The authority key identifier key identifier is is often a duplicate of a subject key identifier from a certificate in the chain.
- The authority key identifier authority Cert Issuer is often a duplicate of a subject field from a certificate in the chain.
- The issuer and key identifier in these cases could just be a relative pointer to the certificate with the information.
  - I.e. typically `0` or 1.

Certificate chain optimizations?



```
1,
h'A6A55C870E39B40E',
1,
1601581116,
1635881916,
[
  -9, "Domain Control Validated",
   1, "*.tools.ietf.org"
],
0,
h'B1E137E8EB82D689FADBF5C24B77F02C4ADE726E3E1360D1A8661EC4AD3D3260E5F099B5F47A7A485521EE0E3912F9CE0DCAF56961C704ED6E0F1D3B1
EAE6E977FF7CA694ECCD006DF5D279B3B12E7E6FE086B527B82117C72B346EBC1E878B80FCBE1EBBD064458DC8350B2A0625BDC81B836E39E7C79B2A953
94834EC8E1142E85B3AFD46EDD6946AF41250E7AAD8BF292CA79D97B324FF777E8F9B44F235CD45C03AED8AB3ACA135F5D5D5DA1',
[
 -3, -2,
  7, [ 1, 2 ],
 -1, 5,
  4, "http://crl.starfieldtech.com/sfig2s1-242.crl",
  5, [ h'6086480186fd6e01071701', "http://certificates.starfieldtech.com/repository/", 1 ],
  8, [ 1, "http://ocsp.starfieldtech.com/", 2, "http://certificates.starfieldtech.com/repository/sfig2.crt" ],
  6, 1,
  2, [ 2, "*.tools.ietf.org", 2, "tools.ietf.org" ],
  0, h'AD8AB41C0751D7928907B0B784622F36557A5F4D',
  9, [
       h'F65C942FD1773022145418083094568EE34D131933BFDF0C2F200BCC4EF164E3',
       1715,
       1,
       h'8CF54852CE5635433911CF10CDB91F52B33639223AD138A41DECA6FEDE1FE90FBCA2254366C19A2691C47A00B5B653ABBD44C2F8BAAEF4D2DA
       h'5CDC4392FEE6AB4544B15E9AD456E61037FBD5FA47DCA17394B25EE6F6C70ECA',
       2012,
       1,
       h'A5E0906E63E91D4FDDEFFF0352B91E50896007564B448A3828F596DC6B28726DFC91EAED02168866054EE18A2E5346C4CC51FEB3FA10A91D2E
     ]
],
23,
h'14043FA0BED2EE3FA86E3A1F788EA04C35530F11061FFF60A16D0B83E9D92ADBB33F9DB3D7E0594C19A8E419A50CA770727763D5FE64510AD27AD650A
A867269CC7937CEE397F7DCF39588ED81032900D2A2C7BAABD63A8ECA090BD9FB39264BFF03D88E2D3F6B21CA8A7DD85FFB94BA83DE9CFC158D61FA672D
31FD72FE03D2F265AF4D7EE2819B7AFD303CF552F40534A08A3E194158C8A8E05171840915AEECA57775FA18F7D577D531CCC72D'
```

- For the example tools.ietf.org certificate the saving are quite large
  - 1075 bytes instead of 1242 bytes

- Even bigger savings for self-issued certs that often have a authority key identifier authority Cert Issuer field (common in HTTPS).

- Should CBOR certificates provide optizations for self-issued certificates. I.e. issuer and auth key id is replaced with 0?
- Should CBOR certificates provide optizations for certs in chains . I.e. issuer and auth key id is replaced with 1?

- Provides large savings.
- Adds complexity, Makes CBOR compression two pass
- May not be needed for TLS with Brotli as Brotli hopefully compresses these things anyway (should be tested)

How to progress until next meeting

- Reviews
- Implementations
- Discussion on the list