COSE Headers for Carrying CBOR Compressed Certificates

draft-mattsson-cose-cbor-cert-cert-compress-00

COSE, IETF 107, April 2020
New header attribute 'CBORchain' similar to 'x5chain' to convey a X.509 certificate chain compressed with CBOR.

- X.509 certificates take up a large part of the total number of bytes when used in COSE.

- Best practice is now to encrypt certificates, this means compression needs to be done in the protocol itself.

- Uses draft-raza-ace-cbor-certificates to compress certificates by encoding them from DER to CBOR.

- The aim is to be compatible with all RFC 7925 profiled certificates.

- General purpose compression algorithms (without dictionary) is not able to compress RFC 7925 X.509 certs much at all.
CBOR Compressed RFC 7925 X.509 certificates
draft-raza-ace-cbor-certificates-04

CBOR compression brings:

1) Compactness

2) Compatibility with and migration path from X.509

3) Smaller footprint than general compression algorithms.

4) Re-use of CBOR already used by COSE, but support for ASN.1 DER is still needed.

<table>
<thead>
<tr>
<th>Certificate Size</th>
<th>RFC 7925 X.509</th>
<th>zlib</th>
<th>CBOR Compression</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>314 bytes</td>
<td>295</td>
<td>136 bytes</td>
</tr>
</tbody>
</table>
Example CBOR Compression of RFC 7925 X.509

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 128269 (0x1f50d)
Signature Algorithm: ecdsa-with-SHA256
Issuer: CN=RFC test CA
Validity
Not Before: Jan 1 00:00:00 2020 GMT
Not After: Feb 2 00:00:00 2021 GMT
Subject: CN=01-23-45-FF-FF-67-89-AB
Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
  Public-Key: (256 bit)
pub:
  95:2b:76:10:n
ASN1 OID: prime256v1
NIST CURVE: P-256
X509v3 extensions:
  X509v3 Key Usage:
    Digital Signature
Signature Algorithm: ecdsa-with-SHA256

{,
1,
h'128269',
"RFC test CA",
1577836800,
161224000,
h'0123456789AB',
h'02ae4cdb01f614defc7121285fcd7f5c6d1d42c95647f061ba080df678867845e',
5,
h'373873EF8781B88297EF235C1FACCF62DA4E44740DC2A2E6A3C6C882A3238D9C3AD9353BA788683B06BB48FECAC16EA71171734C675C5332B2AF1CB733810A1FC'}
• Is certificate compression interesting for COSE?

• Is the RFC 7925 certificate profile useful for COSE or is something missing?

• Which kind of headers (x5chain, x5bag, x5t, x5u) should support compression?

• How should compression be indicated? New headers like 'CBORchain' or e.g. with an array?

[ COSE Header Attribute, Compression Alg ]