CBOR Encoded X.509 Certificates (C509)

draft-ietf-cose-cbor-encoded-cert-00

COSE WG interim 2021-05-12

C509 update

- Submitted as WG document
  - draft-ietf-cose-cbor-encoded-cert-00
- Repo migrated to https://github.com/cose-wg/
- Latest changes to github:
  - Deterministic CBOR
  - Changed name of C509Certificate and c509CertificateType
    - (Let's decide on C509 so we don’t have to change again!)
  - COSE_C5 = [[+ C509Certificate]]
- Double signed certificates?
- We have requested time in TLS WG at IETF 111
  - Important to collaborate with TLS WG on the TLS certificate registration.
- Need to specify RPK by value
  - new type of C509 is one candidate (next slide)

RPK by value

- LAKE requirements include the case of RPK by value
  - i.e. transported in EDHOC
  - also requested by industrial partners interested in LAKE

- EDHOC relies on COSE header parameters to transport and identify credentials
  - 'kid', 'x5chain', 'x5bag', 'x5u', 'x5t’, 'c5c', 'c5b', 'c5u', 'c5t’.
  - RPK by value should also use a COSE header parameter

- Two main options. Roughly same size, but with different properties:
  1. COSE_Key
  2. C509 without issuer signature

COSE_Key vs C509

- COSE_Key
  - available in COSE implementations
  - not designed for transport on the wire
    (but this can be fixed)
  - no header parameter for use by value
  - only supports limited key_ops
  - does not offer any additional functionality like validity, subject name
  - Subject name is needed to align with SIGMA.
  - Validity and KeyUsage seems useful also for RPK

- C509
  - supported by EDHOC, so using both C509 and COSE_Key causes:
    - different key formats
    - additional code
    - key_ops / EKU needs to be registered twice

Examples of RPK with point compression 1(3)

COSE_Key

```
{
  1:  1,
-1:  4,
-2:  h'b1a3e89460e88d3a8d54211dc95f0b903ff205eb71912d6db8f4af980d2db83a',
-3:  true,
}
```

Examples of RPK with point compression 2(3)

C509 w/o Issuer and Issuer Signature (type 2)

```
TBSCertificate = (
  c509CertificateType: int,
  validityNotBefore: Time,
  validityNotAfter: Time,
  subject: Name,
  subjectPublicKeyAlgorithm: AlgorithmIdentifier,
  subjectPublicKey: any,
  extensions: Extensions,
)
```

C509 Type 2 Example

```
[
   2,
   h'01f50d',
   1577836800,
   1612224000,
   h'0123456789AB',
   1,
   h'02B1216AB96E5B3B3340F5BDF02E693F162
     13A04525ED44450B1019C2DFD3838AB',
   1
]
```

Examples of RPK with point compression 3(3)

C509 Type 2 Example 2

```
[
    2,
    h’’,
    [],
    null,
    null,
    [],
    1,
    h'02B1216AB96E5B3B3340F5BDF02E693F162
      13A04525ED44450B1019C2DFD3838AB’,
    1
]
```

C509 Type 2
slimmed down variant

```
[
    2,
    1,
    h'02B1216AB96E5B3B3340F5BDF02E693F162
      13A04525ED44450B1019C2DFD3838AB’
]
```