CBOR Encoded X.509 Certificates (C509)

COSE WG interim 2021-06-23
C509 Updates

— Still version -01
— Updates to github:
  — CBOR encoding of all remaining RFC 5280 extensions
  — Support for RPKI
    — Thanks Russ for providing samples!
  — Support for GSMA eUICC PKI profile
  — Not yet added support for IEEE 802.1AR
    — Thanks Michael for providing samples!
  — New section on CRL (later slide)
  — New section on CSR (later slide)
  — New section on certificate issuance
  — Removed section stub on profiling
  — Several updates of extensions and tables
  — Code for generating C509
    — https://github.com/cose-wg/CBOR-certificates/tree/master/c509
C509 CRL

— based on and compatible with RFC5280
— reusing the formatting for C509

```
C509CertificateRevocationList = [
    TBSCertificateRevocationListType: int,
    issuer: Name,
    thisUpdate: Time,
    nextUpdate: Time,
    revokedCertificates: RevokedCertificates,
    crlExtensions: Extensions,
    issuerSignatureAlgorithm: AlgorithmIdentifier
]

RevokedCertificates = [
    userCertificate: CertificateSerialNumber,
    revocationDate: Time,
    crlEntryExtensions: Extensions,
]
```

```
TBSCertificateRevocationList = (  
    C509CertificateRevocationListType: int,
    issuer: Name,
    thisUpdate: Time,
    nextUpdate: Time,
    revokedCertificates: RevokedCertificates,
    crlExtensions: Extensions,
    issuerSignatureAlgorithm: AlgorithmIdentifier,
)
```
C509 CSR

— based on and compatible with RFC 2986
— reusing the formatting for C509

```
C509CertificateSigningRequest = [ 
  TBSCertificateSigningRequest, 
  subjectProofOfPossessionValue: any, 
]
```

Two `c509CertificateSigningRequestType` values defined:

— 0 requests a `c509CertificateType = 0`
— 1 requests a `c509CertificateType = 1`

```
TBSCertificateSigningRequest = ( 
  c509CertificateSigningRequestType: int, 
  subject: Name, 
  subjectPublicKeyAlgorithm: AlgorithmIdentifier, 
  subjectPublicKey: any, 
  extensionsRequest : Extensions, 
  subjectProofOfPossessionAlgorithm: AlgorithmIdentifier, 
)
```
#98 Compression of chains

— Proposal:

— comp = 0 → no compression
— other values of comp are use for a compressed chain conveyed in a bstr

— Would allow significant compression, compare values from TLS:

```
<table>
<thead>
<tr>
<th></th>
<th>C509</th>
<th>C509 + Brotli</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDSA HTTPS Chain</td>
<td>1409</td>
<td>1058</td>
</tr>
<tr>
<td>RSA HTTPS Chain</td>
<td>3957</td>
<td>2841</td>
</tr>
</tbody>
</table>
```
#81 File format for saving C509 certificates and CSRs

— Michael provided pointer to draft-ietf-cbor-file-magic
  — CBOR Tag Wrapped or CBOR Tag Sequence?