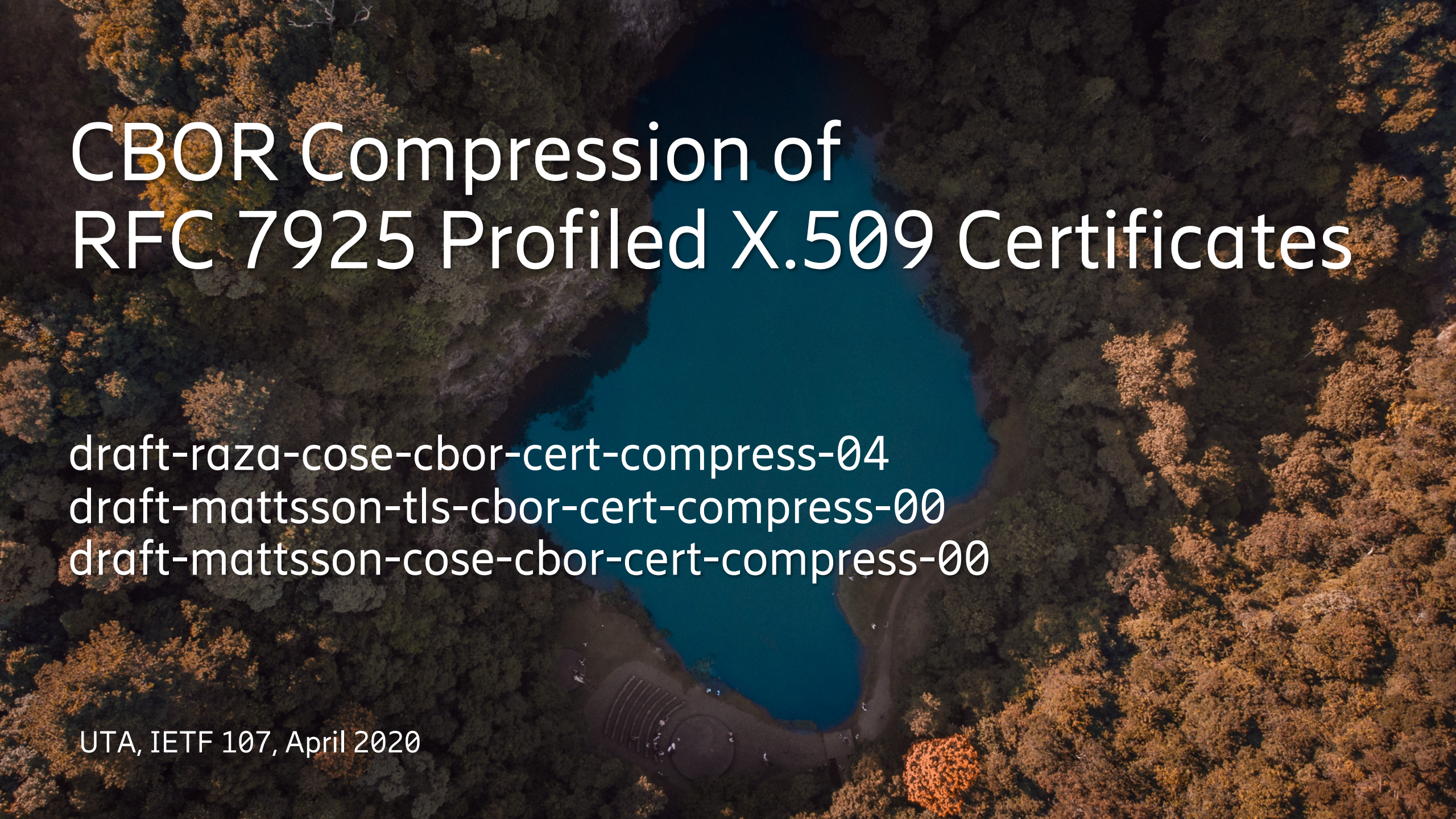

CBOR Compression of RFC 7925 Profiled X.509 Certificates

draft-raza-cose-cbor-cert-compress-04
draft-mattsson-tls-cbor-cert-compress-00
draft-mattsson-cose-cbor-cert-compress-00

UTA, IETF 107, April 2020

CBOR Certificate Algorithm for TLS Certificate Compression

draft-mattsson-tls-cbor-cert-compress-00

- X.509 certificates take up a large part of the total number of bytes in TLS 1.3 handshakes. Especially in cTLS.
- Draft registers a code point to use the algorithm 'CBOR Compression' in draft-ietf-tls-certificate-compression.
- 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.
- COSE WG is re-chartering, current plan is to work on CBOR compression of RFC 7925 (and maybe IEEE 802.11AR)

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.

	RFC 7925 X.509	zlib	CBOR Compression
Certificate Size	314 bytes	295 bytes	136 bytes

```
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-FE-67-89-AB
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:ae:4c:db:01:f6:14:de:fc:71:21:28:5f:dc:7f:
                    5c:6d:1d:42:c9:56:47:f0:61:ba:00:80:df:67:88:
                    67:84:5e:e9:a6:9f:d4:89:31:49:da:e3:d3:b1:54:
                    16:d7:53:2c:38:71:52:b8:0b:0d:f3:e1:af:40:8a:
                    95:d3:07:1e:58
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature
    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:37:38:73:ef:87:81:b8:82:97:ef:23:5c:1f:ac:
         cf:62:da:4e:44:74:0d:c2:a2:e6:a3:c6:c8:82:a3:23:8d:9c:
         02:20:3a:d9:35:3b:a7:88:68:3b:06:bb:48:fe:ca:16:ea:71:
         17:17:34:c6:75:c5:33:2b:2a:f1:cb:73:38:10:a1:fc
```

```
(
  1,
  h'128269',
  "RFC test CA",
  1577836800,
  1612224000,
  h'0123456789AB',
  h'02ae4cdb01f614defc7121285fdc7f5c6d1d42c95647f061ba
    0080df678867845e',
  5,
  h'373873EF8781B88297EF235C1FACCF62DA4E44740DC2A2E6A3
    C6C882A3238D9C3AD9353BA788683B06BB48FECA16EA711717
    34C675C5332B2AF1CB733810A1FC'
)
```

Example CBOR Compression of RFC 7925 X.509

Discussion

- Is CBOR compression interesting for TLS 1.3 / cTLS?
- OK to make TLS IANA registration in COSE WG?
- Should draft-tschofenig-uta-tls13-profile mandate a X.509 profile?
- Should the RFC 7925 certificate profile be updated in any way and in that case where? E.g.
  - An ASN.1 schema would be extremely beneficial.
  - Is the encoding of EUI-64 as a X.509 text string specified somewhere?
  - Is ‘pathLenConstraint’ mandatory to support? In that case, are there any minimum length that is mandatory to support?
  - For ‘BasicConstraints’, the only valid options are "Present and true", and "Absent and therefore false". For the bool ‘critical’ in ‘expansions’, both "Present and false" and "Absent and therefore false" seems to be valid. Is this intentional?