# CBOR Profile of X.509 Certificates

draft-raza-ace-cbor-certificates-00

T2TRG, IETF 103, Bangkok, November 2018

# PROBLEM

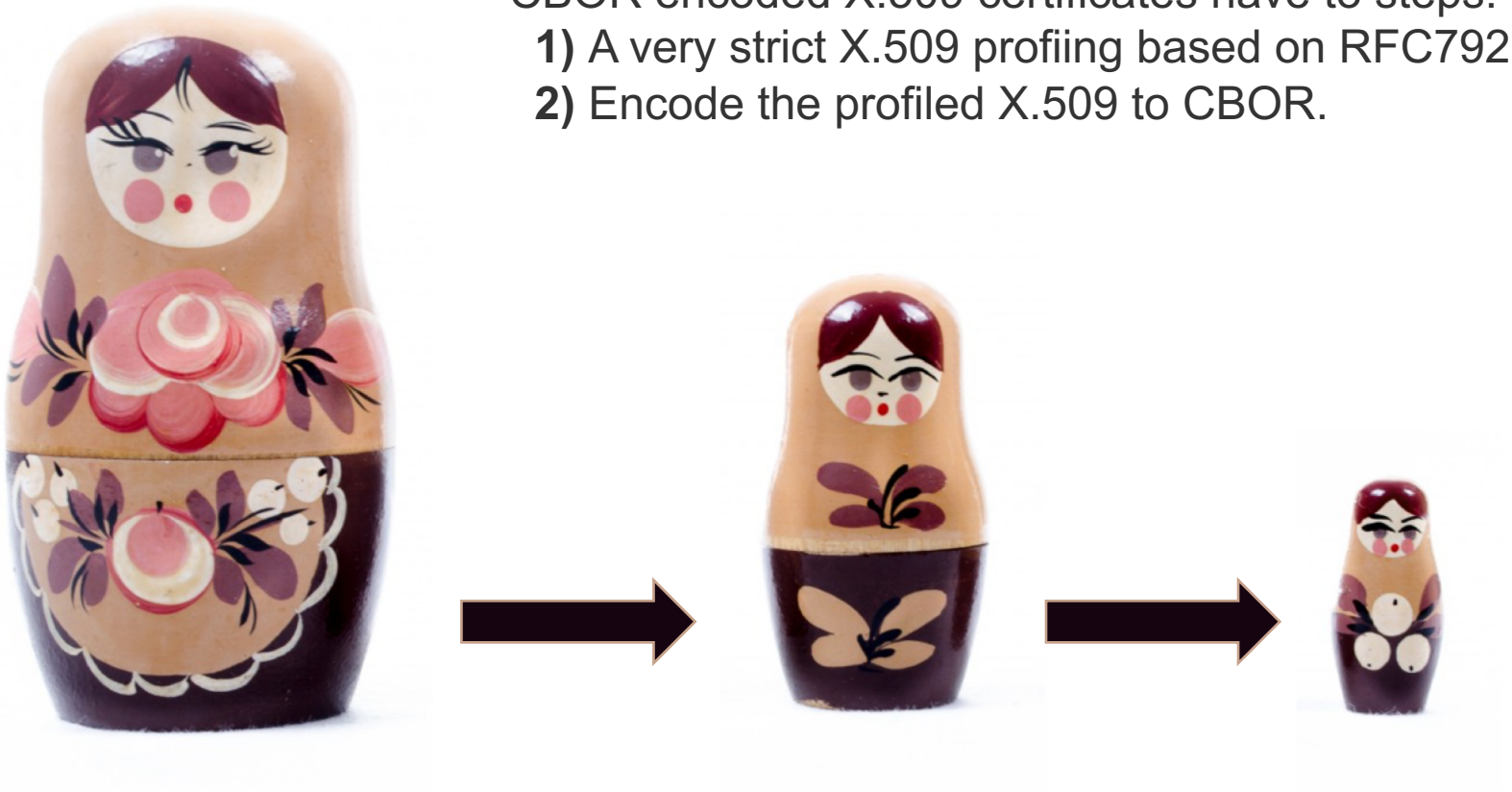
- Strong need for PKI, but PKI technologies are often too heavy for very resource-constrained devices.
- X.509 certificates are demanding in several ways (message, code size, memory, processing, etc. and are not designed for constrained IoT environments.
- X.509 certificates take up a large part of the total number of bytes when used in protocols. Expensive in terms of power consumption, and as the radio resources are often constrained, large messages lead to latency and long response times.
- New protocols (TLS 1.3, DTLS 1.3, EDHOC) encrypt the certificates. This means that than compression in intermediaries will not work in the future.
- (D)TLS 1.3 is currently specifying certificate compression, but the the use of general lossless compression algorithms are quite heavy and does not compress optimally.

# DISCUSSION

- We would like to start a discussion on how to minimize the overhead (message size, code size, memory, storage, processing, etc.) caused by certificates in IoT deployments.
  - Which aspects do the community prioritise the most? i.e. message size, code size, memory, processing, etc. And how should trade-offs between the aspects look like?
  - What are peoples opinions on general lossless compression algorithms in IoT?
  - How should new IoT CBOR certificates be introduced in protocols? New certificate type, new compression algorithms? Is compression/encoding done inside the protocol or outside of the protocol?
  - Which protocols/use cases/type of deployments to focus on?
  - For how long time is people planning to use older protocols that do not encrypt certificates? Is it worth looking at gateway type of compression for these protocols?

- https://tools.ietf.org/html/draft-birkholz-core-coid-00 have very similar problem statement!
  - What signed assertions do we need for constrained IoT, and which of these really "need" to be certificates?

# CBOR CERTIFICATES
# CBOR ENCODED X.509 CERTIFICATES



CBOR encoded X.509 certificates have to steps:

**1)** A very strict X.509 profiing based on RFC7925

**2)** Encode the profiled X.509 to CBOR.

Strict X.509 Profiling

CBOR Encoding

# CBOR CERTIFICATES
# NATIVE CBOR CERTIFICATES

Native CBOR certificates
could also be issued directly

# DRAFT-RAZA-ACE-CBOR-CERTIFICATES RESULTS

draft-raza-ace-cbor-certificates brings: **1)** compactness;
**2)** compability with X.509; **3)** potential migration path for CAs from X.509

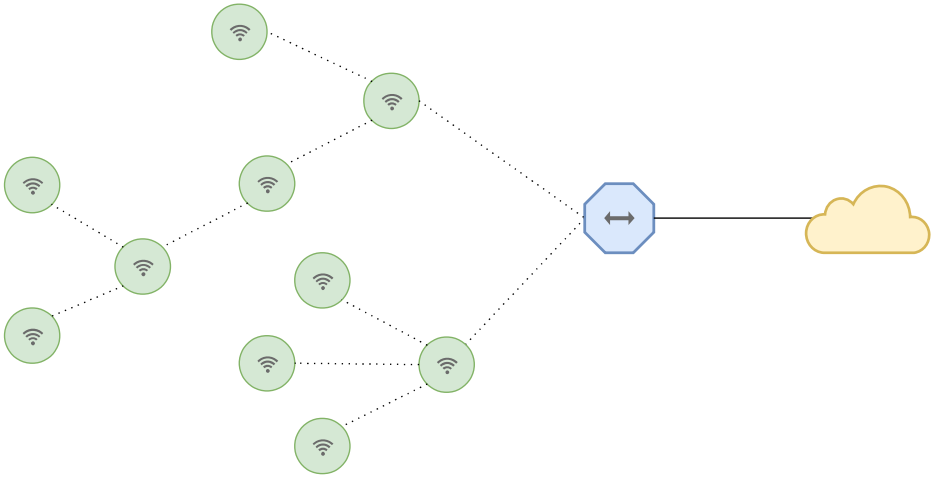

| | X.509 | X.509 Profiled | CBOR Encoded |
|---|---|---|---|
| Cert. Size | 450 | 392 | 238 |

# Introduction

- 6LoWPAN
- X.509 Certificates

# 6LoWPAN

- IEEE 802.15.4
- CoAP
- Zolertia Firefly:
  - 32 MHz CPU
  - 32 kB RAM
  - 512 kB Flash



# X.509 Certificates

- Subject Identity
  - Public key
- Basic information
- CA Signature
- (Extensions)
- ASN.1

# Problem?

```
-----BEGIN CERTIFICATE-----
MIIF8jCCBNqgAwIBAgIQDmTF+8I2reFLFyrrQceMsDANBgkqhkiG9w0BAQsFADBw
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMS8wLQYDVQQDEyZEaWdpQ2VydCBTSEEyIEhpZ2ggQXNz
dXJhbmNlIFNlcnZlciBDQTAeFw0xNTExMDMwMDAwMDBaFw0xODExMjgxMjAwMDBa
MIGlMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEUMBIGA1UEBxML
TG9zIEFuZ2VsZXMxPDA6BgNVBAoTM0ludGVybmV0IENvcnBvcmF0aW9uIGZvciBB
c3NpZ25lZCBOYW1lcyBhbmQgTnVtYmVyczETMBEGA1UECxMKVGVjaG5vbG9neTEY
MBYGA1UEAxMPd3d3LmV4YW1wbGUub3JnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAs0CWL2FjPiXBl61lRfvvE0KzLJmG9LWAC3bcBjgsH6NiVVo2dt6u
Xfzi5bTm7F3K7srfUBYkLO78mraM9qizrHoIeyofrV/n+pZZJauQsPjCPxMEJnRo
D8Z4KpWKX0LyDu1SputoI4nlQ/htEhtiQnuoBfNZxF7WxcxGwEsZuS1KcXIkHl5V
RJOreKFHTaXcB1qcZ/QRaBIv0yhxvK1yBTwWddT4cli6GfHcCe3xGMaSL328Fgs3
jYrvG29PueB6VJi/tbbPu6qTfwp/H1brqdjh29U52Bhb0fJkM9DWxCP/Cattcc7a
z8EXnCO+LK8vkhw/kAiJWPKx4RBvgy73nwIDAQABo4ICUDCCAkwwHwYDVR0jBBgw
FoAUUWj/kK8CB3U8zNllZGKiErhZcjswHQYDVR0OBBYEFKZPYB4fLdHn8SOgKpUW
5Oia6m5IMIGBBgNVHREEejB4gg93d3cuZXhhbXBsZS5vcmeCC2V4YW1wbGUuY29t
ggtleGFtcGxlLmVkdYILZXhhbXBsZS5uZXSCC2V4YW1wbGUub3Jngg93d3cuZXhh
bXBsZS5jb22CD3d3dy5leGFtcGxlLmVkdYIPd3d3LmV4YW1wbGUubmV0MA4GA1Ud
DwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdQYDVR0f
BG4wbDA0oDKgMIYuaHR0cDovL2NybDMuZGlnaWNlcnQuY29tL3NoYTItaGEtc2Vy
dmVyLWc0LmNybDA0oDKgMIYuaHR0cDovL2NybDQuZGlnaWNlcnQuY29tL3NoYTIt
aGEtc2VydmVyLWc0LmNybDBMBgNVHSAERTBDMDcGCWCGSAGG/WwBATAqMCgGCCsG
AQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5jb20vQ1BTMAgGBmeBDAECAjCB
gwYIKwYBBQUHAQEEdzB1MCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2Vy
dC5jb20wTQYIKwYBBQUHMAKGQWh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9E
aWdpQ2VydFNIQTJIaWdoQXNzdXJhbmNlU2VydmVyQ0EuY3J0MAwGA1UdEwEB/wQC
MAAwDQYJKoZIhvcNAQELBQADggEBAISomhGn2L0LJn5SJHuyVZ3qMIlRCIdvqe0Q
6ls+C8ctRwRO3UU3x8q8OH+2ahxlQmpzdC5al4XQzJLiLjiJ2Q1p+hub8MFiMmVP
PZjb2tZm2ipWVuMRM+zgpRVM6nVJ9F3vFfUSHOb4/JsEIUvPY+d8/Krc+kPQwLvy
ieqRbcuFjmqfyPmUv1U9QoI4TQikpw7TZU0zYZANP4C/gj4Ry48/znmUaRvy2kvI
l7gRQ21qJTK5suoiYoYNo3J9T+pXPGU7Lydz/HwW+w0DpArtAaukI8aNX4ohFUKS
wDSiIIWIWJiJGbEeIO0TIFwEVWTOnbNl/faPXpk5IRXicapqiII=
-----END CERTIFICATE-----
```

# Already existing solutions

- Compressed IPsec
- Lightweight CoAPs
- Compressed X.509 Format (CXF)
- DTLS Profiles for IoT

# Achievements

- Reduced certificate size
- Reduced energy consumption
  - Extended battery life
- X.509 compatible

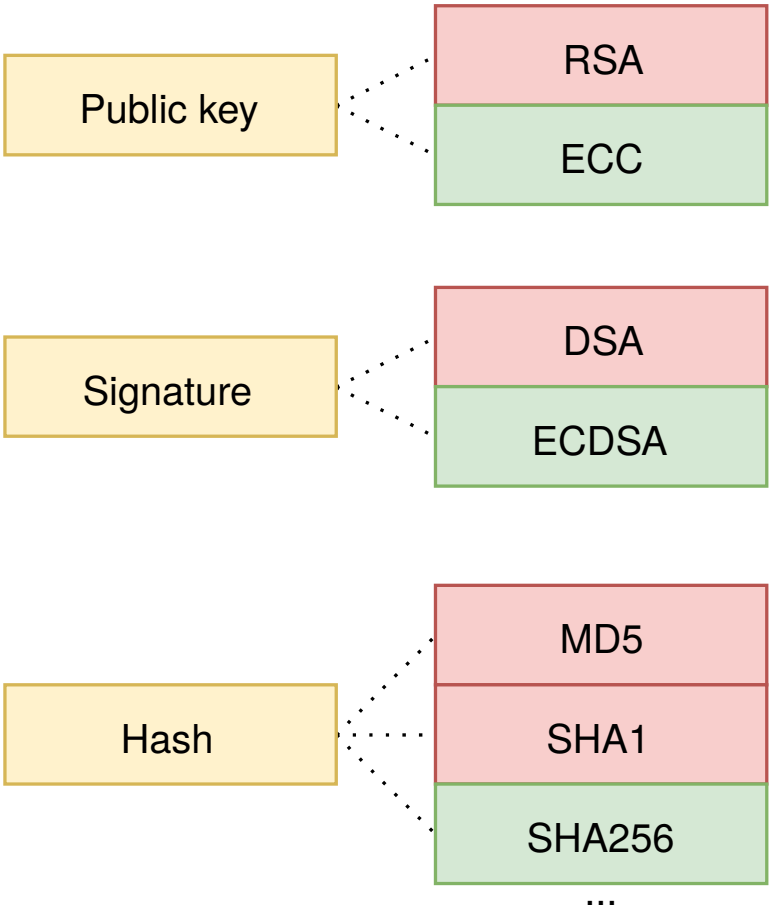
# How does it work?

- X.509 Profile for IoT
- Certificate compression

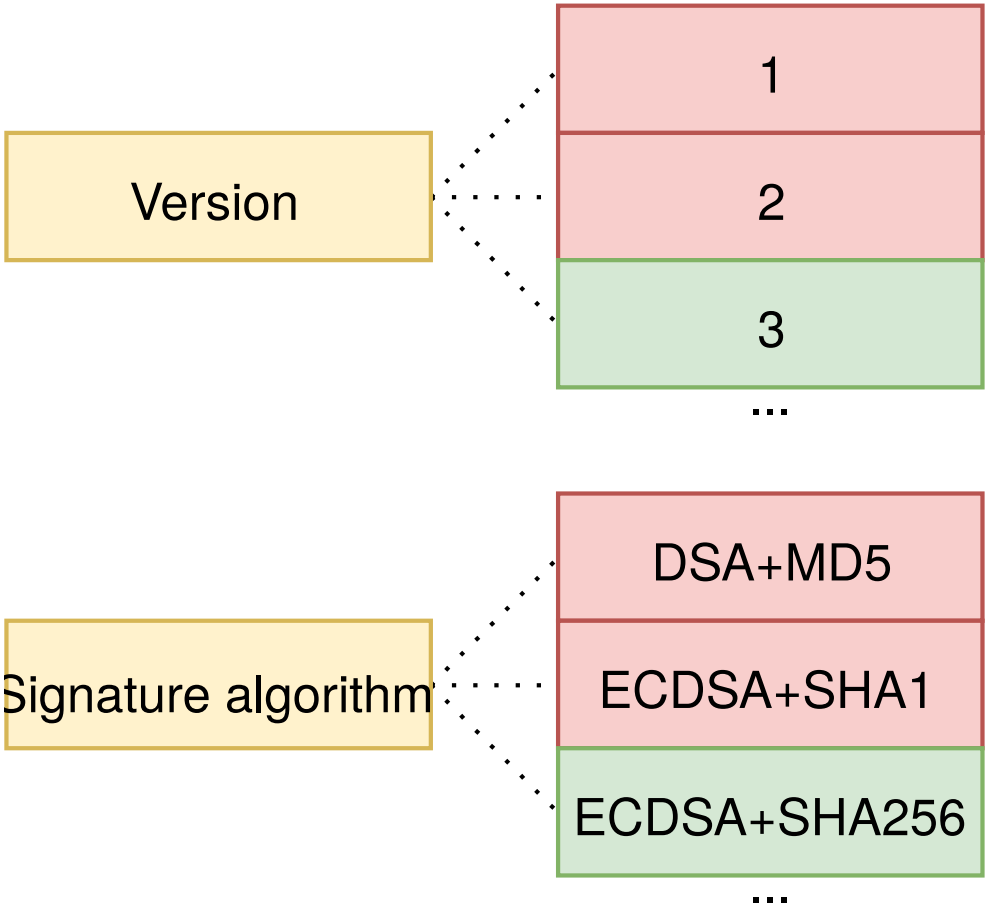
# X.509 Profile for IoT

- Specific cryptographic algorithms
- Mandatory field values
- Restricted field structure

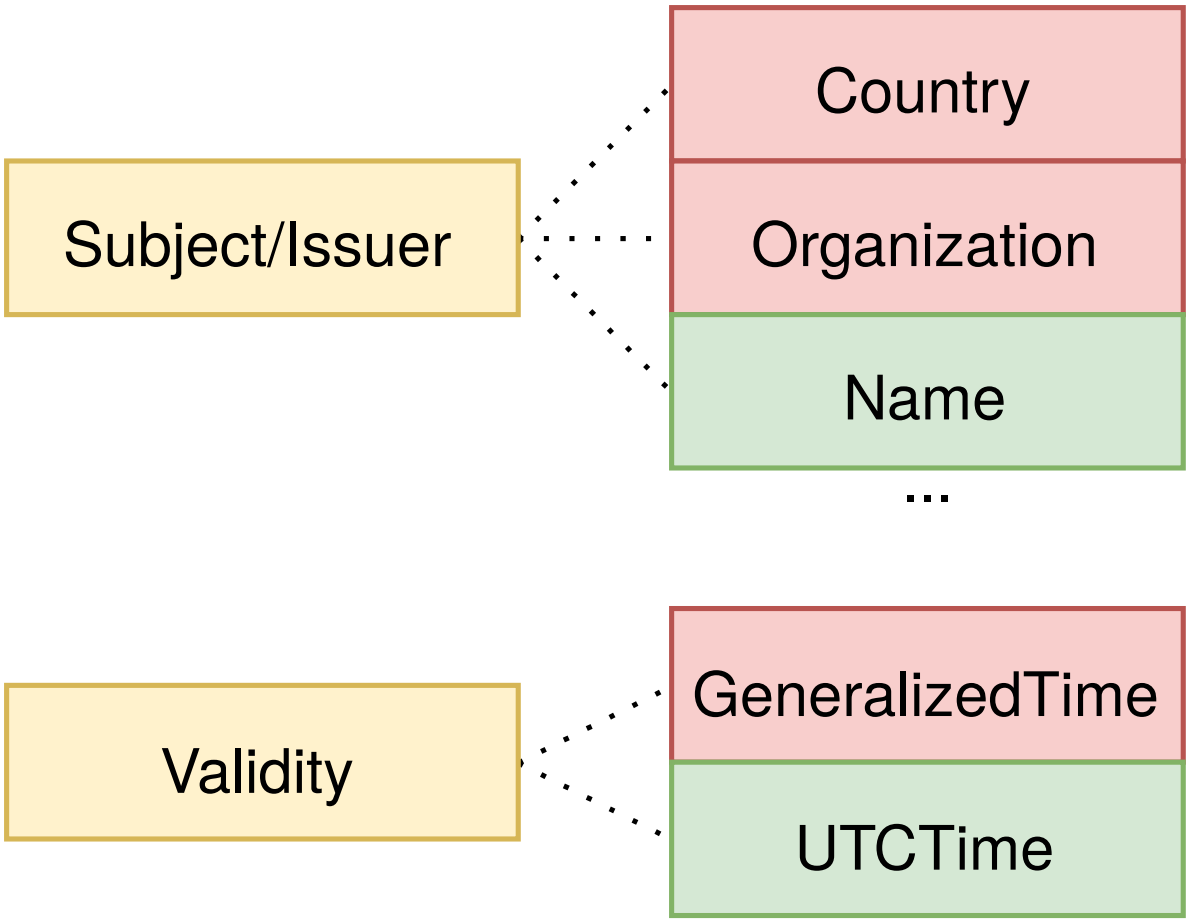
# Cryptographic algorithms



# Field values



# Restricted structure



# Compression

- CBOR
- ECC point compression
- Omitting implied fields
- Time to integer
- Subject to byte array
- Extensions

# Compression Example

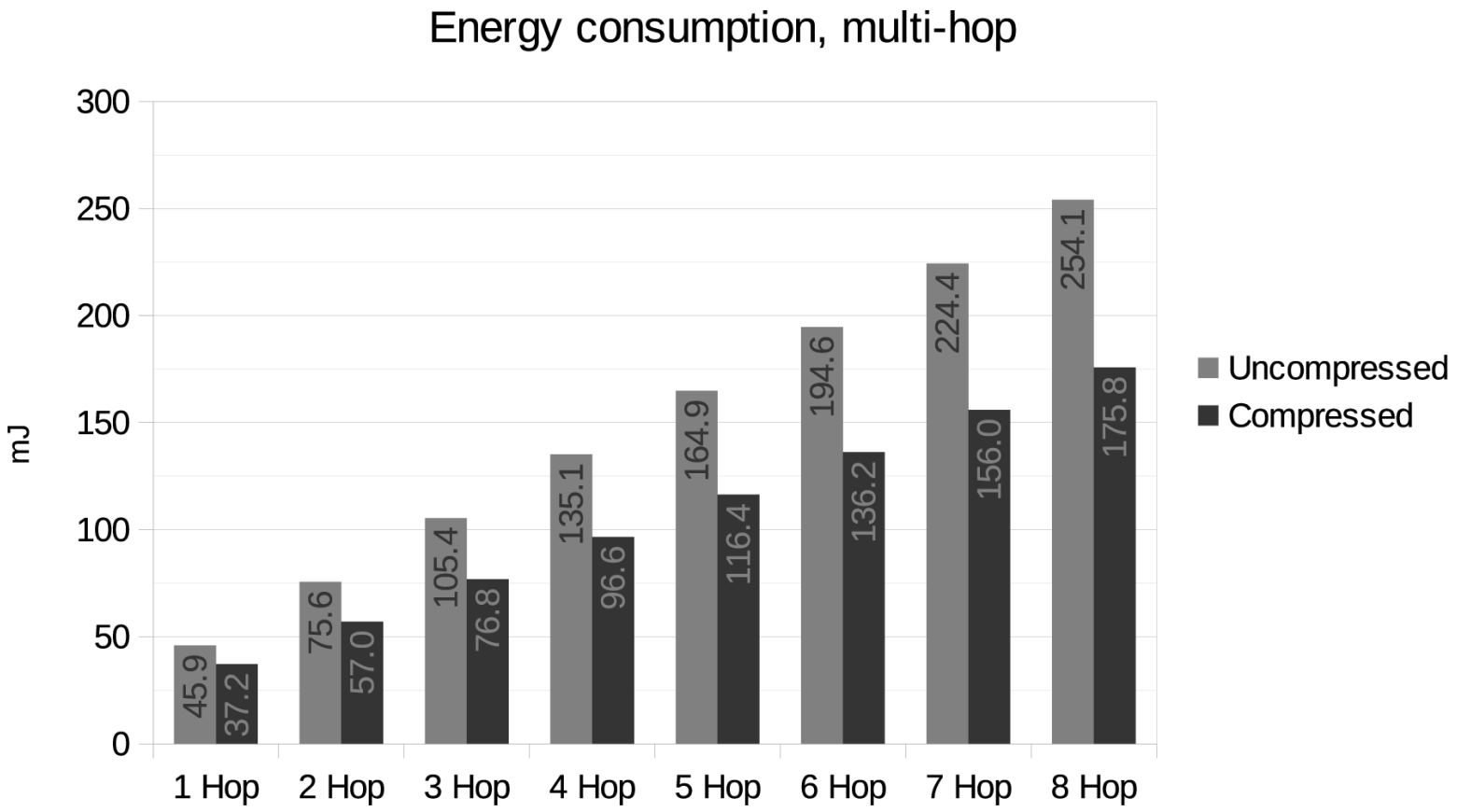
```
-- Uncompressed ASN.1 --
0x30    // Sequence
0x22    // Size 34
0x31    // Set
0x20    // Size 32
0x30    // Sequence
0x1E    // Size 30
0x06    // OID
0x03    // Size 3
0x55 0x04 0x03
        // 2.5.4.3
            (commonName)
0x0C    // UTF8 string
0x17    // Size 23
0x30 0x31 0x2D 0x32 0x33 0x2D 0x34
    0x35 0x2D 0x36 0x37 0x2D 0x38
    0x39 0x2D 0x41 0x42 0x2D 0x43
    0x44 0x2D 0x45 0x46
        // Value
        "01-23-45-67-89-AB-CD-EF"

    (36 bytes)
```

```
-- Compressed CBOR --
0x48    // Byte array of size 8
0x01 0x23 0x45 0x67 0x89
    0xAB 0xCD 0xEF
        // Value
        0x0123456789ABCDEF

    (9 bytes)
```

# Results


Energy consumption, multi-hop
mJ
300
250
200
150
100
50
0
45.9
37.2
75.6
57.0
105.4
76.8
135.1
96.6
164.9
116.4
194.6
136.2
224.4
156.0
254.1
175.8
1 Hop
2 Hop
3 Hop
4 Hop
5 Hop
6 Hop
7 Hop
8 Hop
Uncompressed
Compressed


THE
END