CBOR Profile of X.509 Certificates

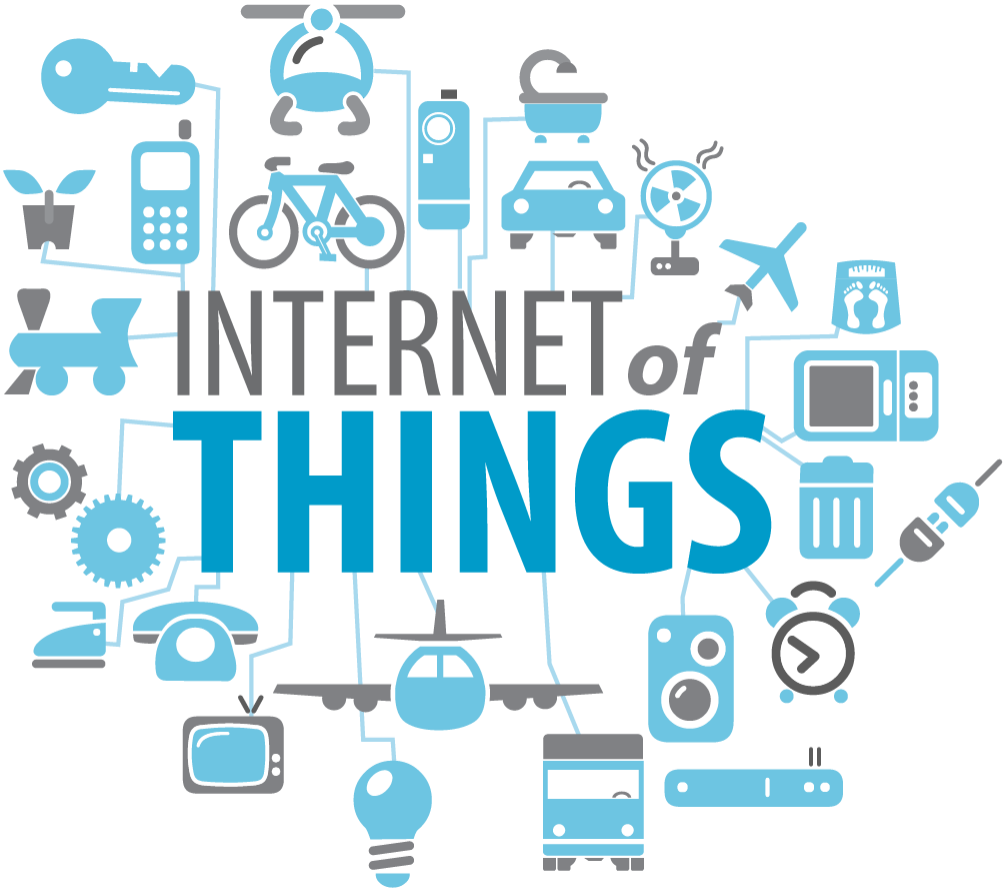
draft-mattsson-cose-cbor-cert-compress-01

IETF 108, 2020-07-29

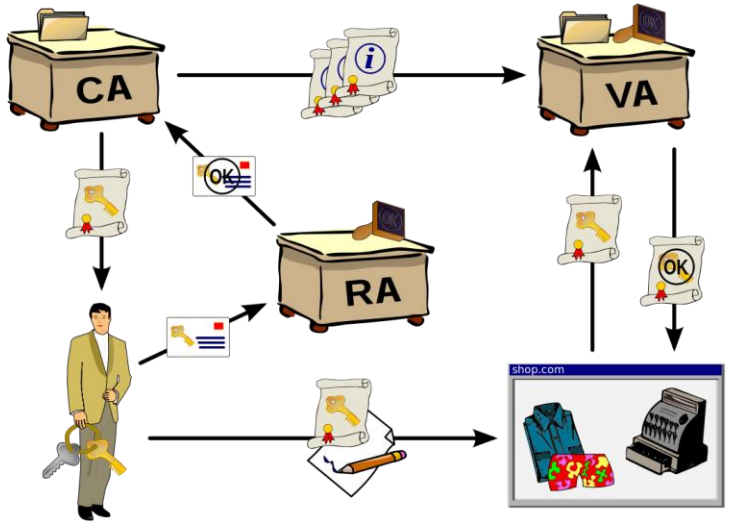
Joel Höglund, S. Raza (RISE),

G. Selander, J. Mattsson (Ericsson AB),

M. Furuhed (Nexus Group)



+



RI.
SE

draft-mattsson-cose-cbor-cert-compress-01

Merger of

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

Introduction

- Challenge with PKI for IoT: size and encoding of X.509 public key certificates
- Based on RFC 7925, which specifies a certificate profile for IoT deployments
- Encoding with CBOR reduces the certificate size significantly with known performance benefits
- This draft specifies CBOR encoding/compression of RFC 7925 profiled X.509 certificates
  - Two variants, CBOR compressed X.509 certificate & native, differing only in what is being signed.
  - Achieves over 50% compression in many cases

Overall design objectives

- Very compact certificate encoding for cases where this is needed
  - Compare LAKE benchmarks (draft-ietf-lake-reqs)
  - Targeting non-IoT as well, but must enable optimized format for constrained IoT
- Restrict to reasonable subset of certificates suitable for IoT
  - Not targeting general certificates, e.g. containing a lot of human readable data
  - The application area motivates a restricted scope
  - Trade-offs for discussion

Restrictions

- From the RFC 7925 profile:
  - Only EC public keys for all certificates in the chain, including CA certificates.
  - Subject contains EUI64 or FQDN
  - Only four certificate extensions (SubjectAltName, BasicConstraints, Key Usage, Extended Key Usage)
- In addition
  - Subject is EUI64 or FQDN
  - Issuer encoding:
    - DN must be possible to encode as CBOR map
    - If only CN is present then as text

Main updates in version-01

- Simplified encodings
  - Invertible formula for representation of Validity
- Number of clarifications
- IANA registry entries for COSE and TLS

Overall discussion theme

- Compactness / saving bytes
- Generality, how to encode as many IoT relevant X.509 certificates as possible
- Comments on the mailing list from
  - Henk Birkholz, HB
  - Ilari Liusvaara, IL
  - Russ Housley, RH
  - Michael Richardson, MR
  - Carsten Bormann, CB

Comments and discussions (1 of 5)

Encoding of the issuer field (HB, IL, MR)

- Current draft: CBOR map (int => bytes)
- Discussion on the representation of types
  - Need to handle repeated attribute types?
  - Need to encode PrintableString and Utf8String?
    - If so, what is the preferred encoding?

Comments and discussions (2 of 5)

Encoding of algorithm types and parameters (IL, MR, CB)

- Current draft:
  - signatureAlgorithm : int,
  - subjectPublicKeyInfo_algorithm : int
  - Support by Ilari that int-encoding is sufficient for relevant cases
- Discussion on the need of RSA code points.
  - NOTE that RFC 7925 restricts signature type to EC:
  - "certificates are signed using ECDSA in this profile. This is not only true for the end-entity certificates but also for all other certificates in the chain, including CA certificates"

Comments and discussions (3 of 5)

Encoding of extensions (HB, IL, RH)

- Current draft: 4 bits encoding of Extensions
  - Would require ordering of extensions, to recreate original content
- ExtendedKeyUsage, EKU: discussion of how to uniquely order extensions and content
  - Proposals for encoding of EKU
    - use array of pairs
    - further details on the list
  - New value of EKU needed for EDHOC

Comments and discussions (4 of 5)

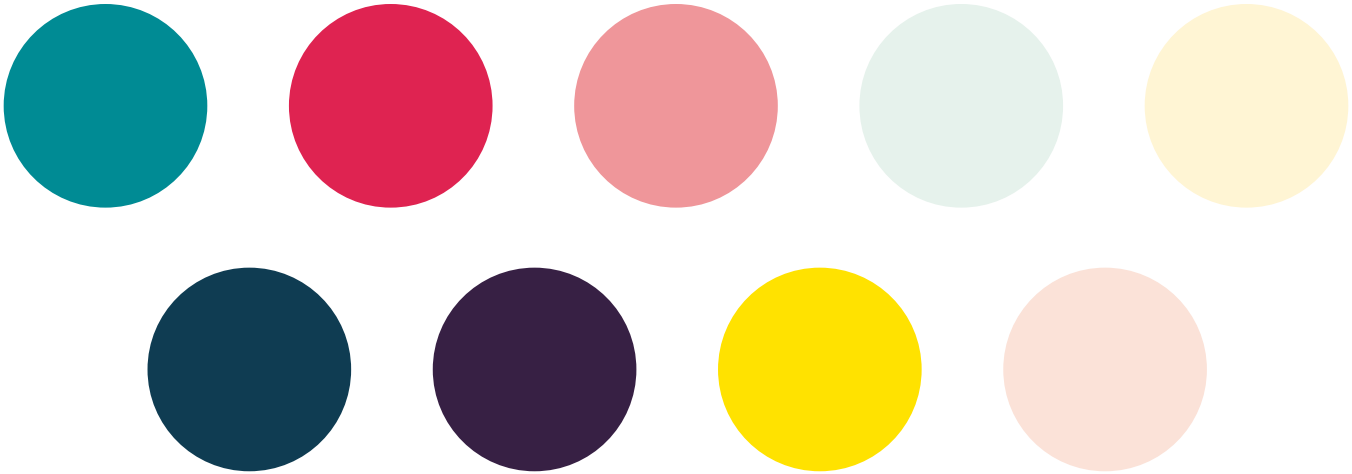
Encoding of extensions (HB, IL, RH)

- BasicConstraints and encoding of CA certificate
  - Current draft: Only supports CN field of subject
    - Works only if CAs create self-signed domain specific certificates for issuing new CBOR certificates
  - Alternatively, explicit encoding of Pathlen + distinguish between no BasicConstraints & BasicConstraints with cA=False and pathLen absent
  - Alternatively, remove CA flag entirely

Comments and discussions (5 of 5)

Comment regarding classification:

- TLS certificate compression or TLS certificate type
  - Further input is welcome



Joel Höglund

joel.hoglund@ri.se