CBOR Certificates

draft-raza-ace-cbor-certificates-01

Prague,
IETF 104,
March 2019,
SECDISPATCH

Background

- 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.
- Presented at T2TRG IETF 103 Bangkok.

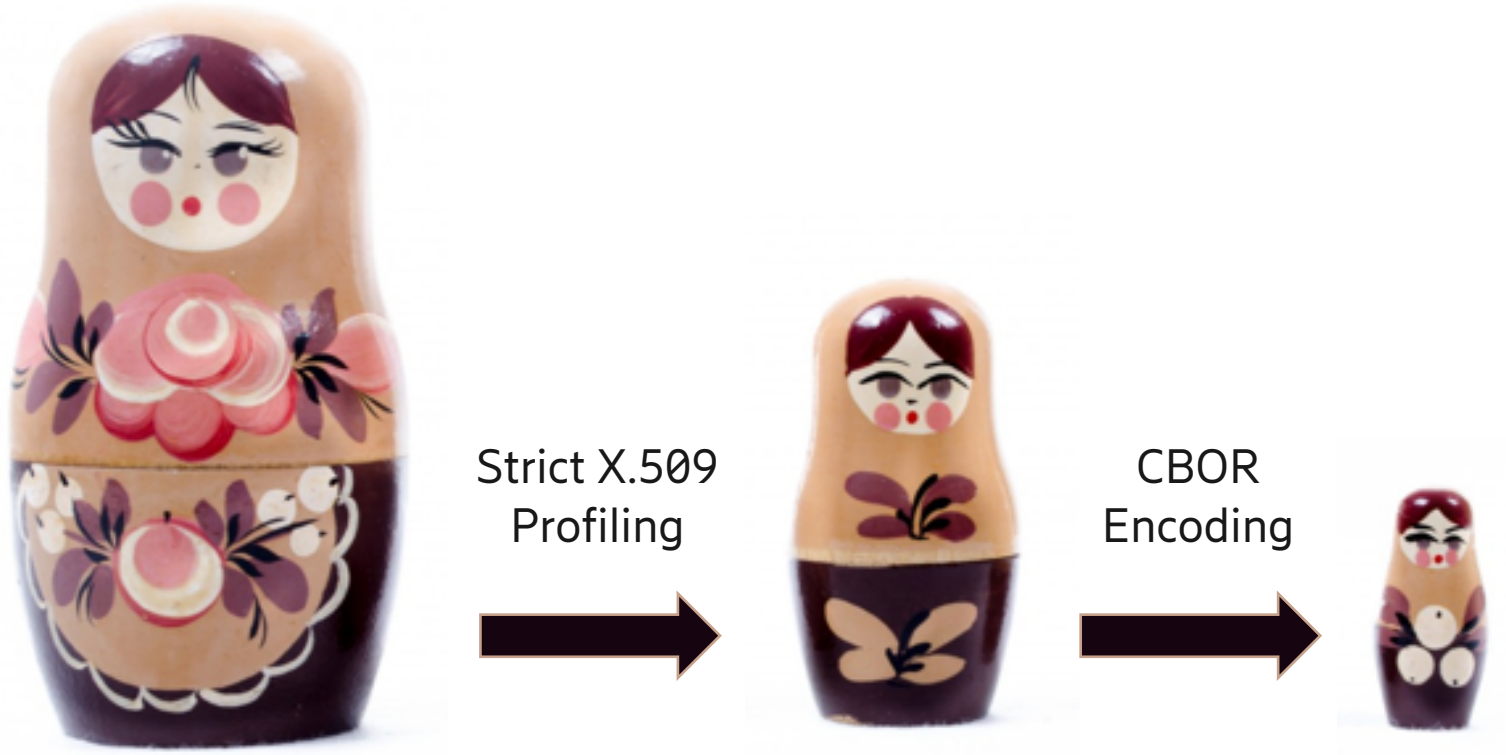
- We would like to start work on a lightweight (message size, code size, memory, storage, processing, etc.) X.509 certificate encoding/lossless compression algorithm with potential applications
  - Gateway to Gateway compression when (D)TLS 1.2 is used.
  - TLS client to TLS server compression when TLS 1.3 is used.
  - Lightweight CBOR certificate format.

CBOR Encoded X.509 certificates
draft-raza-ace-cbor-certificates

CBOR encoding of X.509 certificates in two steps:

1) A very strict X.509 profiling based on RFC 7925

2) An encoding from profiled X.509 to CBOR.



	X.509	X.509 Profiled	CBOR Encoded
Certificate Size	~0.5kB	342 bytes	164 bytes

CBOR Encoded X.509 certificates
draft-raza-ace-cbor-certificates

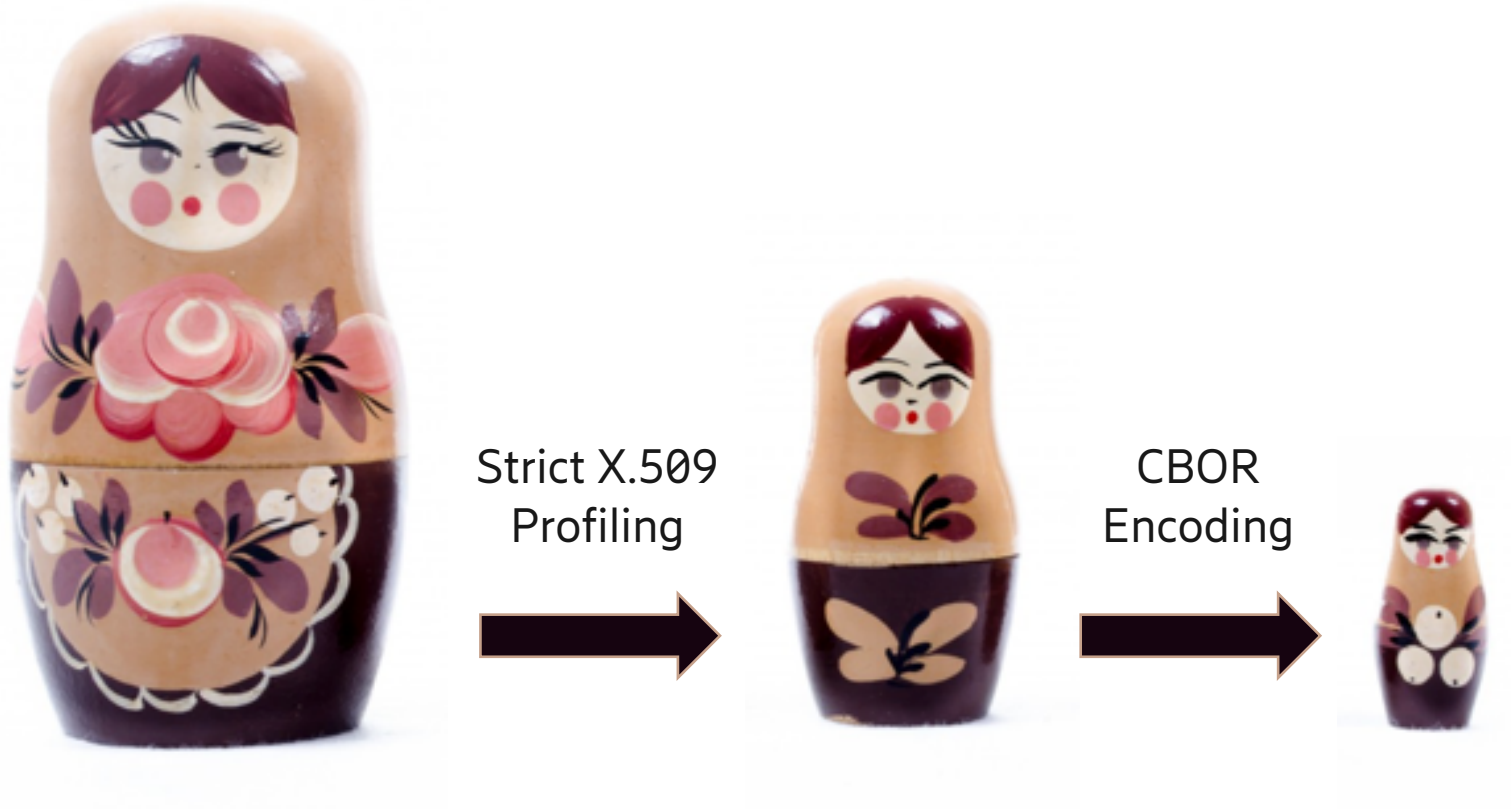
CBOR certificates brings:

1) Compactness

2) Compability with and migration path from X.509

3) Smaller footprint than general compression algs.

4) Larger footprint than X.509 unless signatures are made over CBOR instead of ASN.1.



	X.509	X.509 Profiled	CBOR Encoded
Certificate Size	~0.5kB	342 bytes	164 bytes