CBOR Encoded X.509 (C509)
draft-ietf-cose-cbor-encoded-certs-11

John Preuß Mattsson, Göran Selander, Ericsson AB
Shahid Raza, Joel Höglund, RISE AB
Martin Furuhej, Nexus Group

IETF 120, COSE WG, July 23, 2024
Main changes -09 ➔ -11

— New C509 certificate types 2 & 3

— Several detailed improvement proposals from Lijun Liao
  — now part of design team

— Bug fixes

— More details in the following slides

— Feedback requested on selected issues
Updated certificate format

— Moved location of signature algorithm
  — Enables 1-pass parsing
  — Analogous change in C509 encoding of CSR

— Removed special encoding for PEN
  — Simplification
  — No major impact on size

— Optimized encoding of self-signed certs
  — If issuer == subject then issuer = null

— C509 certificate type 2 & 3 replacing 0 & 1
  — No compatibility issues
Updated certificate format (cont.)

— Removed null option from validityNotBefore

— Removed null option from keyIdentifier

(Examples updated to the new format)
Updated CSR format

— Definition of $c_{509CertificateRequestType} = 0, 1, 2$ or $3$:

<table>
<thead>
<tr>
<th>Signed object</th>
<th>Requested certificate</th>
<th>$c_{509CertificateType} = 2$</th>
<th>$c_{509CertificateType} = 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBOR encoded CSR</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>DER encoded CSR</td>
<td>1</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

— More details on challengePassword formatting
Issues pending feedback

— Do we need dedicated CBOR encoding of these extensions?
  — #187 IPAddrBlocks
  — #190 Certificate Transparency
    — Also EKU
  — #193 QCStatements
  — #201 CCC Digital Key extensions

— Default: No dedicated CBOR encoding is defined
  — Extensions still supported using CBOR OID encoding
C509 test and demo software implementation

— Version 0.4 supports C509 ↔ X.509 encoding/decoding
  — available at: https://github.com/cose-wg/CBOR-certificates/tree/master/c509_demo_impl

— Support for common key types and extensions

— Known bugs/shortcomings:
  — A handling error of uncommon IssuerAltName format
  — No graceful error handling of unexpected string types

— Feedback on additional features to prioritize is welcome!
  — Please provide sample certificates
Next steps

— Evaluate feedback from WG

— Close remaining issues

— WGLC