CBOR Encoded X.509 (C509)

draft-ietf-cose-cbor-encoded-certs-14

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

IETF 123, Madrid, COSE WG, July 21, 2025

Main Changes -13 → -14

- C509 Certificate Request Template
- Changed type of C509Certificate to use in chains and hashes
- Extended use of optimized text encodings: SpecialText
- Review of CBOR encoded extensions
- C509 Private Key Types
- IANA updates
- Editorials

C509 Certificate Request Template

- Request from Mališa Vucinic #223 to define **CBOR structure for csrattrs** (RFC 9148)

- Based on RFC 8295 (EST Extensions)
  - The CA provides a CSR with some pre-filled fields
    and some empty fields to be filled in by the client

  - Use CBOR simple value null (0xf6) to encode empty fields

    → null not allowed to distinguish fields which are filled in and which are not

    - Define NonNull = any .ne null

(WGLC comment by Lijun Liao #257: null interfers with exension encoding
Remedy: replace null → CBOR simple value undefined (0xf7) to encode empty fields)

Type of C509Certificate to use in chains etc.

Type of C509Certificate to use in certificate chains, in certificate hash, and as TLS Certificate Type

— In -13
  — COSE_C509 = **C509Certificate** / [2* **C509Certificate**]
  — COSE_CertHash: Hash of a **C509Certificate**
  — Certificate Type: **~C509Certificate** (the unwrapped C509Certificate)

— Request by Brian Sipos #222 to align and simplify handler processing

— In -14:
  — **~C509Certificate** as common denominator

(WGLC request by Lijun Liao #258: Align to **C509Certificate**)

Misc

New term for optimized text encodings:

- **SpecialText** = text / bytes / tag
- Applied to Name, CBOR encoded Attribute value and Certificate Request

- Fixed missing **extension values** of CBOR encoded extensions
  - OCSP No Check, Precertificate Signing Certificate, TLS Features
- Removed CBOR encoded extensions without specified extension value
  - Biometric Information, Qualified Certificate Statements, S/MIME Capabilities

Encoding of private keys #159

- New field C509PrivateKeyType to allow updates
- Two private key types: Asymmetric Key Package, COSE Key

(WGLC update #263: c509CertificateRequestTemplateType: int)

IANA updates

- Added MAC address to C509 Attributes Registry
- Added EKU Precertificate Signing Certificate
- Removed hash-based signature algorithms from CBOR encoded signature algorithms registry
- Defined Content-Formats for c5b, c5c, c5t, c5u (request from Mališa Vucinic #226)

Editorials

- More details in the introduction
- Clarifications of Name encoding, section 3.1.4
- Moving text on extensions between 3.3 and 3.1.10, removing duplicate text
- Added subsections in 4. C509 Certificate Signing Request
- Moved defintion of C509 Certificate Request to the top
- Updated table with certificate sizes
- Clarifying text on IANA registrations
- Updated references
- Updated examples and clarifications

WGLC

— Reviews by Ivaylo, Marco, Lijun: Thanks!

—PRs in progress

— Main remaining issues:

#258: Common denominator for certificate chains, certificate hash and use in TLS Certificate Types: C509Certificate or ~C509Certificate

#260: Allowing multiple-choice in Certificate Request Template.