

# Protecting EST Payloads with OSCORE

## draft-ietf-ace-coap-est-oscore-10

Göran Selander, Ericsson

Shahid Raza, RISE

Martin Furuhed, Nexus

**Mališa Vučinić, Inria**

Timothy Claeys

ACE @ IETF 125 – 17/03/2026

draft-ietf-ace-coap-est-oscore

# Status

- In WGLC since 18 September 2025
- 2 reviewers
  - Marco Tiloca on 9 October 2025
  - Esko Dijk on 22 October 2025
- Published -10 on 2 March 2026
  - Addresses the remaining open issues
- Goal of the presentation
  - Discuss resolved issues

# Resolved Issues

# Resolved Issues since -09

- [#112: Example 4.1 fix & optimization](#)
- [#113: Section 4.2.1: "bag" mandatory or not?](#)
- [#114: Section 3 normative language](#)
- [#118: Eexpected CFs for certificate URIs in the multipart response - and how to distinguish?](#)
- [#119: Using /crtS with unauthenticated EST server](#)

# #113:Section 4.2.1: "bag" mandatory or not?

- Conclusion of the [discussion](#) with Esko is that supporting an explicit chain of certs does not make sense
  - Explicit chain does not allow us to rekey CA certificates
  - For specific use cases, bag can contain a chain
  - cose-c509-cert supports either a single cert or multiple certs, thus a bag can be returned
- Made application/cose-c509-cert **MUST** support for both EST-oscore client and EST-oscore server
- Aligned TBD numbers with draft-ietf-cose-cbor-encoded-cert
- Editorial fixes in the example

# #118: Expected CFs for certificate URIs in the multipart response - and how to distinguish?

- Clarified that mixing x5u and c5u cert references in the same multipart response is not supported
  - They are of the same type application/cbor so it would be ambiguous to carry them in the same multipart-core response
- Avoid mentioning x5t and x5u references
  - Cert references are supported for enrollment for CBOR-encoded certs

# Next Steps

- Ship?

Thank you!