

Protecting EST Payloads with OSCORE

draft-ietf-ace-coap-est-oscore-08

Göran Selander, Ericsson

Shahid Raza, RISE

Martin Furuhed, Nexus

Mališa Vučinić, Inria

Timothy Claeys

Status

- Published -08 on 07 July 2025
 - Resolves the issue on enrolling certificate references
 - Resolves the issue on response to /csratts (/att)
- Goal of the presentation
 - Present the resolution to the issues
 - Ask for WGLC

Resolved Issues

#69: Transporting certificates by reference

Context

- RFC9360 defines COSE header parameters that allow **referencing** a certificate
 - x5t: hash of an X.509 cert
 - x5u: URI of an X.509 cert
- draft-ietf-cose-cbor-encoded-cert defines
 - c5t: hash of an C509 cert
 - c5u: URI of an C509 cert
- EDHOC (RFC9528) may use these in its ID_CRED_x field (one or multiple)
- EST-oscore (this draft) aims to support enrollment of certificates by reference
 - EST-server sends to the EST-client **reference(s)**
 - When needed, EST-client resolves the reference to an actual certificate, same as any other party using the certificate reference

Issues

- Interoperability during enrollment (EST-client and EST-server)
- Interoperability beyond enrollment (constrained device previously acting as EST-client and its peers)
- How to resolve the certificate references?

} Out of scope

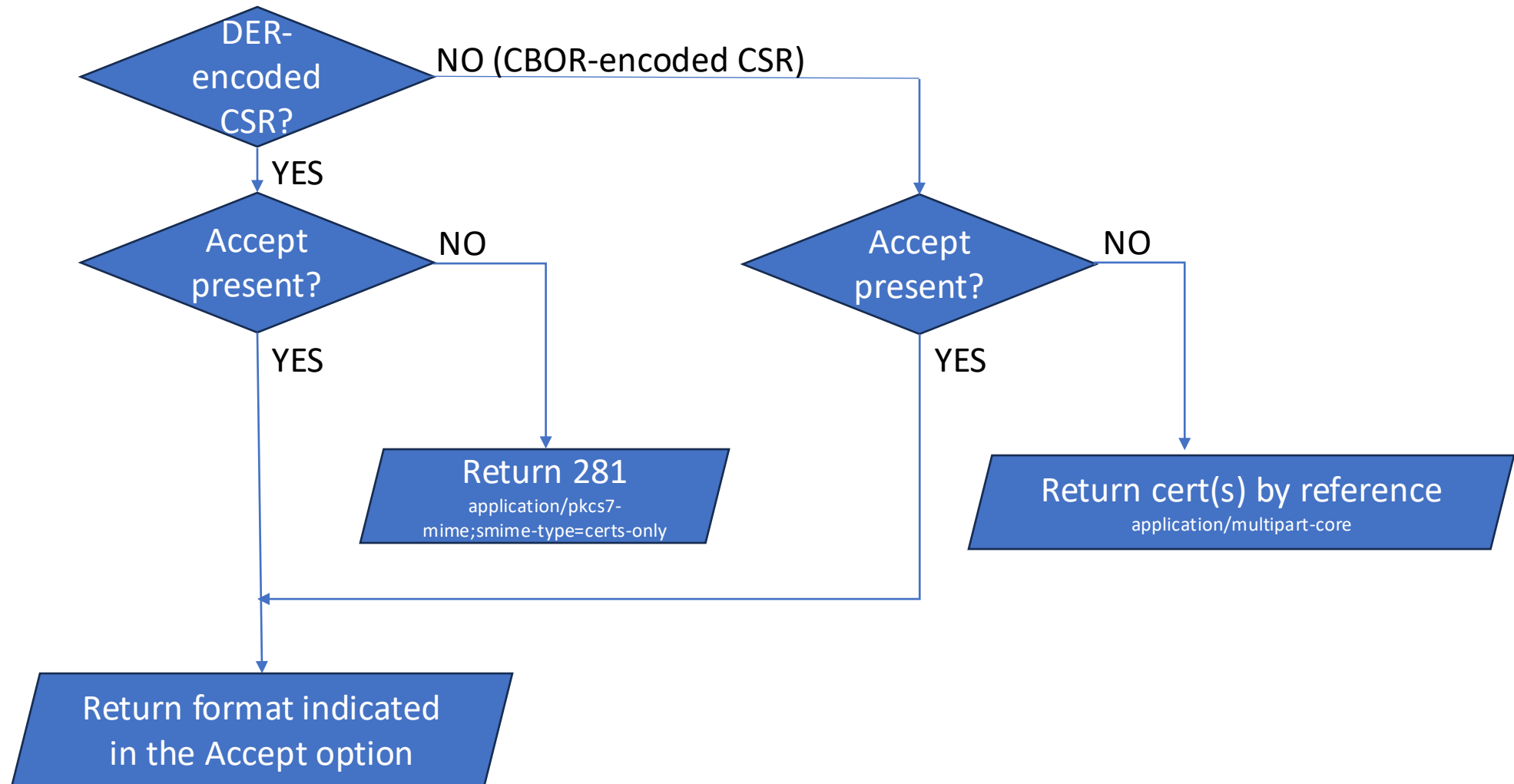
#69: Transporting certificates by reference

Interoperability during enrollment (EST-client and EST-server)

- Since IETF 122, authors of **draft-ietf-cose-cbor-encoded-certs** have specified the media types and CoAP Content-Formats for transporting certificates by reference (application/cose-certhash)
 - Thanks!
- At IETF 122, we also had a discussion how to support certificate by reference in **any** format
 - Resolved in the current document, version -08 through the **absence** of the Accept option when CSR is CBOR-encoded
- In case of **any**, EST-client receives application/multipart-core containing (multiple) references allowing it to resolve the certificate when needed.
 - Application/multipart-core MAY also contain the actual certificate apart from the reference
 - What gets included depends on the application profile

#69: Transporting certificates by reference

Interoperability during enrollment (EST-client and EST-server)



#52: CDDL Structure of /csrattrs (/att)

Context

- EST-client issues a GET on /csrattrs (/att) to retrieve the list of attributes it should include in the CSR
 - Semantics defined in RFC 7030
 - Clarified in [draft-ietf-lamps-rfc7030-csrattrs](#)
 - Alternative approach based on a CSR template based on RFC8295 also defined in [draft-ietf-lamps-rfc7030-csrattrs](#)
 - [Section 4.4 of draft-ietf-cose-cbor-encoded-cert](#) specifies a CBOR-encoded CSR template (C509CertificateRequestTemplate)
 - Adopted the alternative approach from RFC8295 and draft-ietf-cose-cbor-encoded-cert

Resolution

- For the format and the semantics of response to /csratts (/att), pointing to Section 4.4 of draft-ietf-cose-cbor-encoded-cert

Next Steps

- WGLC?

Thank you!