Protecting EST Payloads with OSCORE draft-ietf-ace-coap-est-oscore-07

Göran Selander, Ericsson
Shahid Raza, RISE
Martin Furuhed, Nexus
Mališa Vučinić, Inria
Timothy Claeys

ACE @ IETF 122 – 19/03/2025

Status

- Published -07 on 3 March 2025
  - Resolving remaining issues from Esko’s review
  - 18 issues closed
  - 3 issues still open (1 editorial)
- Goal of the presentation
  - Present the remaining open issues and proposals to go forward

Open Issues

#69: Transporting certificates by reference 1/3

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
  - Core idea is that the client never needs to see the actual certificate
  - EST-server send to the EST-client a reference
  - EST-client uses the cert reference in all communications beyond enrollment
  - Saves bandwidth (we don't need to transport cert over a constrained link)
  - Burden on the non-constrained device to resolve the cert 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?

#69: Transporting certificates by reference 2/3

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

Discussions during the Hackathon @ IETF 122

- Use the CoAP Accept option
- EST-client indicates in the Accept option the preference for a cert by reference
- Cert by reference from the point of view of EST-client
  1. EST-client may treat the reference as an opaque byte string
     - EST-client may indicate preference for **any** of the formats
     - All of the formats above fit **application/cbor** content type
  2. EST-client may also need to parse the reference
     - EST-client needs to know the format of the response

Option 1

- Define special semantics in EST-oscore that application/cbor in the Accept option means any cert by reference

Option 2

- Register a new media type (potentially in draft-ietf-cose-cbor-encoded-certs) specifically for the purpose of indicating preference for **any** format

Option 3

- Register new media types and content format ids for each of the specific content types (x5u, x5t, c5u, c5t)

Provide feedback at C509/#226

#69: Transporting certificates by reference 3/3

Interoperability beyond enrollment (constrained device previously acting as EST-client and its peers)

Discussions during the Hackathon @ IETF 122

- Facilitate interoperability by ensuring that the response returned by EST-server (cert by reference) is usable in other contexts (e.g. establishing an EDHOC session)
- Whether the other communication peer supports certificates by reference is really a system design question (could be specified by a profile such as draft-ietf-lake-app-profiles)

Proposal

- Ensure the format returned by EST-server is usable in EDHOC (RFC 9528)
  - ID_CRED_x format specified in Section 3.5.3 of RFC9528

#104: Considerations on retrieving certificates by reference

How to resolve the certificate references?

- Important from the point of view of general interoperability
- x5u and c5u indicate the URI of the referenced certificate
  - RFC9360 specifies that the cert may be retrieved through a GET request over HTTP or CoAP
- x5t and c5t indicate the hash of the certificate
  - No indication how the certificate is intended to be retrieved
  - Assuming local usage
- Application may use multiple references of different formats
- Out of scope of EST-oscore

Proposal

- Add considerations on these aspects in the EST-oscore draft

#52: CDDL Structure of /csrattrs

Context

- EST-client issues a GET on /csrattrs to retrieve the list of attributes it should include in the CSR
  - Semantics defined in RFC 7030
  - Clarified in draft-ietf-lamps-rfc7030-csrattrs
- Discussion ongoing whether to include the CDDL definition in EST-oscore or in draft-ietf-cose-cbor-encoded-cert
- Carsten already provided input in https://github.com/cose-wg/CBOR-certificates/issues/223
  - Thanks Carsten!

Proposal

- Keep the issue as open until the CDDL definition of csrattrs response is merged

Next Steps

- Close #69 and #104
  - Then, WGLC?

Thank you!