Protecting EST Payloads with OSCORE draft-ietf-ace-coap-est-oscore-05

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

ACE @ IETF 120 – 22/7/2024

Status

- Published -05 on 8 July 2024
  - Miscellaneous fixes throughout the document
- Goal of the presentation
  - Present the resolutions of closed issues

Closed Issues

#36: Consider the use of challengePassword for signature keys without EDHOC

Closed

Context

- challengePassword field is used to implement the connection-based channel binding between transport and app objects
- When a static DH key is enrolled, connection-based channel binding is not needed
- In the draft, use of challengePassword is optional and left to the application profile
- Issue refers to the clarification of the use of challengePassword when the EDHOC session and enrollment are executed with different keys

Action performed

- Clarified security considerations on Channel Binding

```
-In other cases, including pre-shared OSCORE contexts, this specification makes explicit channel binding based on the challengePassword attribute in PKCS#10 requests OPTIONAL.
-The challengePassword attribute could be used for freshness in the case of pre-shared OSCORE contexts and a re-enrollment request.
+
+Other cases include pre-shared OSCORE contexts and the case where the signature key used for signing the CSR is different from the key used in the EDHOC run.
+In these other cases, this specification makes explicit channel binding based on the challengePassword attribute in PKCS#10 requests OPTIONAL.
+For example, the challengePassword attribute could be used for freshness in the case of pre-shared OSCORE contexts and a re-enrollment request.
```

#19: Clarify scope in the introduction and the abstract 1/2

Closed

Context

- Clarify credential(s) used for initial authentication
- Rewrite abstract

Action performed

- New abstract

```
- This document specifies public-key certificate enrollment procedures protected with lightweight application-layer security protocols suitable for Internet of Things
  (IoT) deployments.
- The protocols leverage payload formats defined in Enrollment over Secure Transport (EST) and existing IoT standards including the Constrained Application Protocol
  (CoAP), Concise Binary Object Representation (CBOR), and the CBOR Object Signing and Encryption (COSE) format.
+ Enrollment over Secure Transport (EST) is a certificate provisioning protocol over HTTPS.
+ This document specifies how to carry EST over the Constrained Application Protocol (CoAP) protected with Object Security for Constrained RESTful Environments (OSCORE).
+ The specification builds on the EST-coaps {{RFC9148}} specification, but uses OSCORE and Ephemeral Diffie-Hellman over COSE (EDHOC) instead of DTLS.
+ The specification also leverages the certificate structures defined in {{I-D.ietf-cose-cbor-encoded-cert}}.
```

#19: Clarify scope in the introduction and the abstract 2/2

Closed

Action performed

- Clarified the use of initial auth credentials to stress that a trust relation between the EST Client and the EST server must exist, but how it is established is out of scope

```
- In order to protect certificate enrollment with OSCORE, the necessary keying material (notably, the OSCORE Master Secret, see {{RFC8613}}) needs to be established
  between the EST-oscore client and EST-oscore server.
- For this purpose we assume by default the use of the lightweight authenticated key exchange protocol EDHOC {{I-D.ietf-lake-edhoc}}, although pre-shared OSCORE keying
  material would also be an option.
+ Prior to running EST-oscore, the protocol defined in this specification, there must exist a trust relation between the EST-oscore client and the EST-oscore server.
+ This trust relation may be based on the pre-shared OSCORE security context, or based on the common root of trust.
+ In case there is a pre-shared OSCORE security context, the CoAP exchange carrying EST payloads can occur immediately.
+ In case there is a common root of trust, a security handshake based on the Ephemeral Diffie-Hellman over COSE (EDHOC, {{RFC9528}}) protocol needs to occur prior to
  running CoAP.
+ How this trust relation is established is out of scope of this document.
```

#29: Adding message flow example

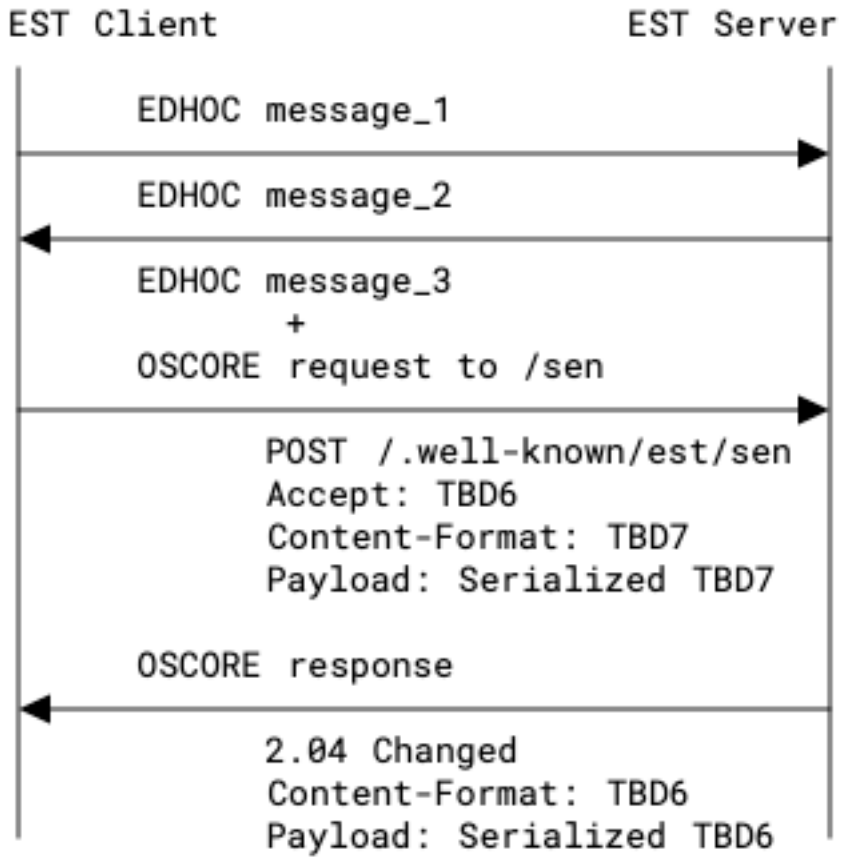
Closed

Context

- An example message flow was missing from the draft

Action performed

- Added an example that includes optimizations (OSCORE and EDHOC in the same message)
- TBDs are placeholders for draft-ietf-cose-cbor-encoded-cert-11 registrations



Misc updates

- Align the private key container with draft-ietf-cose-cbor-encoded-cert-11 structure
  - Use of application/cose-c509-privkey media type
- Misc fixes on references

Open Issues

- #52: CDDL structure of /csrattrs
- #54: Selection of the type of enrollment credentials
  - What type of credential to enroll during the enrollment request?
  - Consider leveraging EDHOC cipher suite negotiation to help with the decision

Next Steps

- Resolve remaining open issues
- WGLC?

Thank you!