Protecting EST Payloads with OSCORE
draft-ietf-ace-coap-est-oscore-03

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

• Received review from John Mattsson on 19 September 2023
  • [https://mailarchive.ietf.org/arch/msg/ace/h85KdNLkMxqzCZjIY-fGlPEyVw/](https://mailarchive.ietf.org/arch/msg/ace/h85KdNLkMxqzCZjIY-fGlPEyVw/)
• Published -03 on 23 October 2023
  • Partial resolution of issues raised in John’s review
• Goal of the presentation
  • Present the resolutions to the notable issues raised in John’s review
  • Discuss open issues
#15: How does a Client obtain the DH key of a Server (Enrollment of Static DH Keys)

John’s comment

➢ "The EST client obtained the CA certs including the CA's DH certificate using the /crts function"

\[\text{This seems very inefficient. Why not just use } G_Y \text{ from EDHOC? The Client/Initiator can use the cipher suite to get the curve it wants. I think this should be added as an option.}\]

Context

• When enrolling static DH key, Proof-of-possession is a MAC (RFC 6955)
• MAC is computed with a key generated from a shared ECDH secret
• To compute the secret, Client needs the Server’s public DH key (certificate)
• EST uses the /crts functions for the Client to retrieve the certificates

Action taken

• Optimization when EDHOC and combined EDHOC-OSCORE delivery precedes enrollment
  • “... the client MUST use the public ephemeral key of the EDHOC Responder, } G_Y \text{, as the recipient public key...”}
  • PR #32 merged: https://github.com/ace-wg/est-oscore/pull/32
#9 Connection-based proof-of-possession

**John’s comment**
- *Connection-based proof-of-possession*, I assume this means the client might not be authenticated (verify identity) in EDHOC. In that case this needs to be described and discussed.

**Context**
- Refers to the binding between the CSR and the underlying secure transport layer
- Achieved by including the challengePassword attribute in the CSR that depends on the ongoing security session
- When EDHOC is used for enrolling static DH keys, the CSR PoP is now generated with an EDHOC ephemeral key
  - Binds the EDHOC session to the CSR without the need for additional bytes in challengePassword

**Action taken**
- Removed the specification on how to generate edhoc-unique byte string that was used as challengePassword
- Made the usage of challengePassword OPTIONAL for non-EDHOC use cases
  - “How challengePassword” is generated is outside of the scope of this specification and can be specified by an application profile.”
- Added security consideration how this binding is achieved when using EDHOC (usage of the ephemeral key to compute the MAC)
- PR #33 merged: [https://github.com/ace-wg/est-oscore/pull/33](https://github.com/ace-wg/est-oscore/pull/33)
  - Closes #10 raised by John on the length of the edhoc-unique byte string
Fixed editorials

• **#5**: Consolidate references [Closed]
• **#6**: Fix BCP14 boilerplate [Closed]
• **#11**: Explicitly state the type of certificate in “Optimizations” [Closed]
• **#12**: Illustrate the use of draft-ietf-core-oscore-edhoc [Closed]
• **#13**: Update figures [Closed]
• **#16**: Delete the sentence on HKDF [Closed]
• **#21**: Add acks [Closed]
• **#28**: Additional optimization in 3.4 [Closed]
Open Issues
#35: Normative requirements on Content-Format support (ASN.1 / CBOR)

Context

• EST-oscore may transport ASN.1 or CBOR objects
• Content type negotiation happens through CoAP’s Accept option
• Need to specify normative requirements on what is supported
• Aim at keeping backward compatibility

Proposed text

➢ “EST-server SHOULD support both ASN.1 and CBOR-encoded objects. It is up to the client to support only ASN.1, CBOR encoding, or both. As a reminder, Content-Format negotiation happens through CoAP's Accept option present in the requests.”
#34: Payload formats should explicitly mention CBOR-encoded objects

**Context**
- Table 2 gives a summary of ASN.1 media types carried within request and responses for each of the supported EST functions

**Proposal**
- Add an equivalent for CBOR-encoded objects as registered in I-D.ietf-cose-cbor-encoded-cert
- Currently missing from I-D.ietf-cose-cbor-encoded-cert
  - media-type registration for PKCS#10
  - CBOR encoding and media type for PKCS#8
#17: Use of EAD fields of EDHOC to transport EST

John’s comment

> “External Authorization Data (EAD) fields of EDHOC are intentionally not used to carry EST payloads because EDHOC needs not be executed in the case of re-enrollment.”

This seems to me like the wrong decision. Using EAD would be much more efficient for the first enrollment. How common and important is re-enrollment? By using EDHOC efficiently I think the client might be able to send the CSR in message_3 and get the cert in message_4.

Context

- IoT device lifetime on the order of several years -> need to support re-enrollment
- Separate code paths for enrollment and re-enrollment complicate the implementation
- Possible to do enrollment with combined EDHOC-OSCORE delivery
- That way, initial enrollment can happen in EDHOC message_3 and message_4

Proposal

- Keep enrollment in OSCORE, option for combined EDHOC-OSCORE delivery is already present in the draft
#14: Update RFC9148?

John’s comment

- EST with hop-by-hop protection over a proxy seems like a very bad security architecture. Unless RFC 9148 makes this NOT RECOMMENDED, I think this draft should update RFC 9148 and do that. Server generated private keys visible to proxies should be MUST NOT. I have not read RFC 9148.

Context

- Section 5 of RFC9148 discusses the HTTPS-CoAPs “Registrar” which acts as a HTTP-CoAP proxy
- Enables the EST-server to talk only HTTP/TLS
- In case of server-generated private keys which are not encrypted at the object level, key is visible to the proxy
- OSCORE traverses proxies

Proposal

- Add a security consideration on this in EST-oscore
- Do not update RFC 9148
Open editorial issues

• **#7**: Terminology rewrite to account for static DH keys
• **#8**: Trust Anchor database is always required
• **#18**: Clarify that issuing C509 certs is optional
• **#19**: Clarify scope in the introduction
• **#20**: Use Oxford comma
• **#29**: Adding message flow example
Next Steps

• Resolve remaining open issues
• More reviews?
Thank you!