

Protecting EST Payloads with OSCORE

draft-ietf-ace-coap-est-oscore-00

Göran Selander, Ericsson

Shahid Raza, RISE

Martin Furuhed, Nexus

Mališa Vučinić, Inria

Timothy Claeys

Status

- Adopted as draft-ietf-ace-coap-est-oscore on 19 April 2023
- Received a review from Marco Tiloca on 29 April 2023
 - <https://mailarchive.ietf.org/arch/msg/ace/iXUjFD3hsS1vL8X8rRJyudiMCZQ/>
 - A million thanks, Marco!
- Fixed non-controversial points
 - <https://github.com/EricssonResearch/EST-OSCORE/pull/8>
- Goal of this presentation
 - Discuss remaining Marco's comments

Marco's comment #1

As expected, the draft focuses on the EDHOC forward message flow, as it better maps against the EST expected workflow and ensures to protect the identity of the EST client. That said, can the use of the EDHOC reverse message flow be explicitly ruled out altogether?

- Context
 - There is no explicit mention of a forward or reverse EDHOC flow in the draft
 - Forward flow (EST client == EDHOC initiator) is implicitly assumed
- Reverse flow (EST client == EDHOC responder) does not seem to make sense
- **Proposed Action:** Explicitly specify in Section 3 (“Authentication”) that the EST client **MUST** play the role of the EDHOC initiator

Marco's comment #2

Section 1 says: "pre-shared OSCORE keying material would also be an option."

- In such a case, is channel binding simply not achievable?*
- Or is it somehow possible as long as the OSCORE keying material was established through some sort of interactive protocol (e.g., like the OSCORE profile of ACE, see RFC 9203)?*
- Context
 - EST-coaps specifies OPTIONAL channel binding to counter the Triple SHAKE attack on TLS 1.2
 - Section 3.3 specifies OPTIONAL use of EDHOC-Exporter interface to provide channel binding
- Issue: What if OSCORE Security Context is pre-shared and EDHOC was not executed prior to enrollment?
- **Proposed Action:** Explicitly specify that EDHOC-Exporter-based channel binding is applicable only to cases when EDHOC is executed prior to enrollment. State that channel binding is not supported when pre-shared OSCORE context is used.

Marco's comment #3

In scenarios using message_4, wouldn't it make sense to have the PKCS#10 request and response transported in an EAD_3 and EAD_4 item, respectively?

- Context
 - EST payloads are currently carried in OSCORE-protected messages
 - This is to be homogeneous with respect to re-enrollment and not require EDHOC
- Assessment is that carrying request and response in EDHOC's EAD items would complicate the protocol, as the flow would no longer be homogeneous
- **Proposed Action:** No action to take

Marco's comment #4

Per Section 9 of RFC 8613, the "osc" attribute is optionally included in a link to specify that a resource has to be accessed with OSCORE. Should it remain optional here too?

- Consider a setup where OSCORE and DTLS are combined. Especially when discovering EST resources on a non-default port number, the links to those resources would have URI scheme "coaps". Then, the absence of the "osc" attribute might wrongly suggest that the EST server is actually using EST-coaps.*
 - Therefore, it might be worth mandating the use of the attribute "osc" in links to EST resources accessed as in this specification.*
 - An alternative would be defining a new set of EST-OSCORE-related Resource Type values, such as "ace.est.osc.*".*
-
- Proposed Action:** Mandate the use of “osc” attribute in links to EST resources.

Marco's comment #5

Regarding the response from /skc, is it possible to deviate from what is defined in RFC 9148 and not encrypt the private key? After all, end-to-end encryption of the whole EST payload is ensured by OSCORE.

- If yes, that might open for a new Content-Format pair (284, 287), i.e., an unencrypted PKCS #8 private key together with a single certificate (not a PKCS#7 container).*
- Context: Contrary to EST-coaps where Registrar may terminate the DTLS connection, OSCORE protection is end-to-end between the EST client and the EST server
 - This allows the private key to be returned as unencrypted PKCS #8, because the key will later be encrypted by OSCORE
 - This needs to be specified in the document
- **Proposed Action:** Specify that the response to /skc can be PKCS #8 private key because OSCORE is used. Specify the new Content-Format pair.

Marco's comment #6

I suppose your intention is for the EST client and server to support Content-Formats just like in RFC 9148, i.e.:

- *"Content-Format 281 MUST be supported by EST-coaps servers. Servers MAY also support Content-Format 287. It is up to the client to support only Content-Format 281, 287 or both."*
- *I think it is good to have an explicit statement here too.*

Proposed Action: Add an explicit statement on the Content-Format support

Like RFC 9148 does in its Table 3, it is good to also recap the Content-Format identifiers used for the different parts of the responses from /skg and /skc.

Proposed Action: Add a Table similar to RFC9148 Table 3.

Marco's comment #7

Section 4.4: The list of requirements is preceded by "It is RECOMMENDED that". However, isn't it a MUST for (at least) the CoAP options OSCORE and Uri-Path?

- **Proposed Action:** Mandate the requirements listed in Section 4.4:

The EST-oscore message characteristics are identical to those specified in Section 4.4 of [RFC9148]. It is REQUIRED that ¶

- The EST-oscore endpoints support delayed responses ¶
- The endpoints supports the following CoAP options: OSCORE, Uri-Host, Uri-Path, Uri-Port, Content-Format, Block1, Block2, and Accept. ¶
- The EST URLs based on https:// are translated to coap://, but with mandatory use of the CoAP OSCORE option. ¶

Marco's comment #8

"The EST URLs based on https:// are translated to coap://, but with mandatory use of the CoAP OSCORE option."

- *The scheme "coap" is the translation target only if DTLS is not additionally used.*
- **Proposed Action:** Explicitly mention that if DTLS is used, scheme is "coaps"

Marco's comment #9

"this specification mandates the implementation of CoAP option Block1 and Block2 fragmentation mechanism [RFC7959]"

- *This is good, but it contradicts the text in Section 4.4 where the support of the CoAP option Block1 and Block2 is only RECOMMENDED.*
- **Proposed Action:** Mandate Block1 and Block2 in Section 4.4, as per slide #9.

Marco's comment #10

Section 5: If a secure association is needed between the EST Client and the CoAP-to-HTTP Proxy, this may alternatively and more conveniently rely on OSCORE as well, see

<https://datatracker.ietf.org/doc/draft-tiloca-core-oscore-capable-proxies/>

- Context
 - See figure
- **Proposed Action:** Informatively reference [draft-tiloca-core-oscore-capable-proxies](https://datatracker.ietf.org/doc/draft-tiloca-core-oscore-capable-proxies/) as a way to establish a secure association between the EST client and CoAP-to-HTTP proxy.

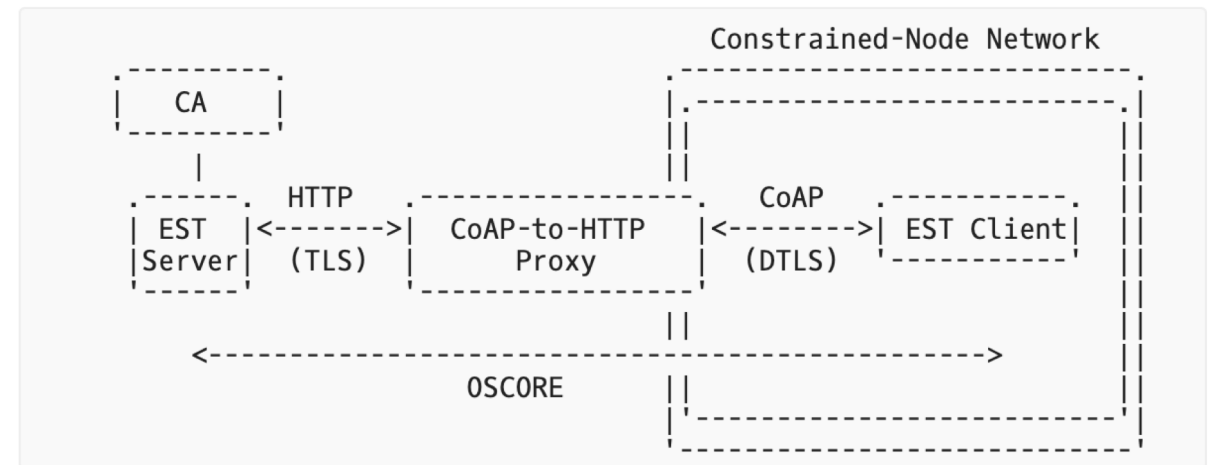


Figure 2: CoAP-to-HTTP proxy at the CoAP boundary.

Thank you!