Profiling EDHOC for CoAP and OSCORE

draft-ietf-core-oscore-edhoc

Francesca Palombini, Ericsson
Marco Tiloca, RISE
Rikard Höglund, RISE
Stefan Hristozov, Fraunhofer AISEC
Göran Selander, Ericsson

CoRE WG interim meeting – March 1st, 2023

Outcome of the WG Last Call

- **Received reviews from Christian and John – Thanks a lot!**
  - https://mailarchive.ietf.org/arch/msg/core/Rs9EMsszA-QzRue7QJDIZN280WU/
  - https://mailarchive.ietf.org/arch/msg/core/n6Kmomt6znH8y52C1-v3ufz7yPI/
  - https://mailarchive.ietf.org/arch/msg/core/8Cxad5Byb1qK07B00qQksPEJeiI/

- **The authors have discussed how to address the comments**
  - Already addressed non-controversial and editorial comments in the Editor's copy
  - https://core-wg.github.io/oscore-edhoc/draft-ietf-core-oscore-edhoc.html

- **Goal for today: discuss selected open points with the Working Group**
  - 6 comments from Christian (CA-x)
  - 5 comments from John (JPM-x)
  - 1 extra point

CA-1

- **Payload of the EDHOC+OSCORE request**
  - Currently a CBOR sequence of two CBOR data items
  - i) EDHOC message_3 (bstr), followed by ...
  - ii) OSCORE ciphertext (bstr)

- **CA: change the payload format, to not be a CBOR sequence**
  - EDHOC message_3 still as CBOR data item (bstr), followed by ...
  - OSCORE ciphertext **not** wrapped in a CBOR byte string
  - Save 1+ bytes (2 or 3 in most cases)

- **Authors' proposal: adopt the new payload format**

OK with that?

CA-2

- **Error handling at the server**
  - If the decrypted OSCORE request in turn includes an EDHOC option ...
  - ... respond with an error if an OSCORE option is also not present

- **CA: correct for the end-to-end case in question, but not future proof**
  - This can backfire when introducing nested OSCORE (and/or nested combined requests)
  - Avoid normative language to describe factual impossibilities
  - CA alternative text: *When the decrypted request is checked for any critical options (as it is during regular CoAP processing), the presence of an EDHOC option MUST be regarded as an unprocessed critical option, unless it is processed by some further mechanism.*

- **Authors' proposal: adopt the suggested alternative text**

OK with that?

CA-3

- **Web-linking**
  - Target attributes can “describe” an EDHOC resource
  - I.e., how the server can run EDHOC through that resource
- **CA: something is missing**
  - Support for forward and reverse EDHOC message flow
- **Authors: something more is missing**
  - Support for Initiator and/or Responder EDHOC role
- **Authors’ proposal**
  - Define four additional target attributes about the above
  - They are not repeatable; they do not have value
  - **OK with that?**

method
// supported EDHOC method

csuite
// supported EDHOC cipher suite

cred-t
// supported type of CRED

idcred-t
// supported type of ID_CRED

ead1, ead2, ead3, ead4
// supported type of EAD item

comb-req
// supported EDHOC+OSCORE request

CA-4

- **Web-linking**
  - Target attributes can “describe” an EDHOC resource
  - I.e., how the server can run EDHOC through that resource
- **CA: add indication of whole application profiles?**
  - One may compile an application profile “my-sdo.edhocp1”
- **Authors’ proposal**
  - In the EDHOC draft, define a new registry for EDHOC application profiles (Name | Description | Reference)
  - In this document, define a new target attribute, to indicate the application profile(s) of an EDHOC resource
  - Repeatable, with value the profile name from the registry
  - Single-feature target attributes can still be used to extend
  - **Ok with that?**

method
// supported EDHOC method

csuite
// supported EDHOC cipher suite

cred-t
// supported type of CRED

idcred-t
// supported type of ID_CRED

ead1, ead2, ead3, ead4
// supported type of EAD item

comb-req
// supported EDHOC+OSCORE request

CA-5

```
REQ: GET /.well-known/core

RES: 2.05 Content
     </sensors/temp>;osc,
     </sensors/light>;if="sensor",
     </edhoc/resA>;rt="core.edhoc";csuite="0";csuite="2";method="0";
     cred-t="c509";cred-t="ccs";idcred-t="4";comb-req,
     </edhoc/resB>;rt="core.edhoc";csuite="0";csuite="2";method="0";
     method="3";cred-t="c509";cred-t="x509";idcred-t="34"
```

- **Web-linking**
  - Target attributes can “describe” an EDHOC resource
  - I.e., how the server can run EDHOC through that resource
- **CA: why two EDHOC resources in the example?**
  - Either explain or (preferred) use /.well-known/edhoc
- **Authors’ proposal**
  - Change the example to use /.well-known/edhoc
  - Note: that was the case until v -02
  - It changed after the 2021-10-27 CoRE interim meeting [1]
    - The rationale was that a client knows how /.well-known/edhoc works, as well-known
    - Actually, path and use for EDHOC are well-known, but not the application profile

[1] https://datatracker.ietf.org/doc/minutes-interim-2021-core-13-202110271600/

OK with that?

CA-6

- **Web-linking**
  - Target attributes can “describe” an EDHOC resource
  - I.e., how the server can run EDHOC through that resource

- **CA: as a general point…**
  1. Is it worth having a well-known EDHOC application profile?
  2. If yes, should it be the default profile for /.well-known/edhoc ?

- **Authors’ proposal**
  - YES on (1) → The EDHOC draft can define a well-known EDHOC application profile
    - And then register the application profile in the new registry (see slide 6)
  - NO on (2) → Neither for /.well-known/edhoc nor for other EDHOC resources
    - Sort-of suggestion of what is mandatory to implement (which is very little in EDHOC)

OK with that?

JPM-1

- **Document title**
  - “Profiling EDHOC for CoAP and OSCORE”

- **JPM: Better title? This document does not really profile EDHOC**

- **Authors’ proposal**
  - Change the title to: “Using EDHOC with CoAP and OSCORE”

OK with that?

JPM-2

- **Error handling on the server**
  - If EDHOC fails with the combined request, an EDHOC error message is sent as response
- **JPM: Say clearly if the EDHOC error message can be protected with OSCORE**
  - Related to issue #8 → https://github.com/core-wg/oscore-edhoc/issues/8
- **Authors' proposal (also based on early discussion with John)**
  - The EDHOC error message is always sent unprotected
  - New text for the second from last paragraph of Section 3.3:
    - *If step 4 (EDHOC processing) fails, the server discontinues the protocol as per Section 5.4.3 of [I-D.ietf-lake-edhoc] and responds with an EDHOC error message with error code 1, formatted as defined in Section 6.2 of [I-D.ietf-lake-edhoc].* ***The server MUST NOT establish a new OSCORE Security Context from the present EDHOC session with the client, hence the CoAP response conveying the EDHOC error message is not protected with OSCORE. Furthermore,*** *the CoAP response conveying the EDHOC error message MUST have Content-Format set to application/edhoc+cbor-seq defined in Section 9.9 of [I-D.ietf-lake-edhoc].*

OK with that?

JPM-3

- **Error handling on the server**

- **JPM: is it clear what happens if the EDHOC+OSCORE request is retransmitted?**

- **Authors' proposal**
  - We are inheriting and not repeating what is defined in the EDHOC draft, which says:
    - *Different instances of the same message MUST NOT be processed in one session. Note that processing will fail if the same message appears a second time for EDHOC processing in the same session because the state of the protocol has moved on and now expects something else.*
  - We are pointing to and not repeating the error handling in 5.4.3 and 6.2 of the EDHOC draft
  - It should already be clear → No action to take

OK with that?

JPM-4

- **Web-linking**
  - Target attributes can “describe” an EDHOC resource
  - I.e., how the server can run EDHOC through that resource

…

ead1, ead2, ead3, ead4
// supported type of EAD item

…

- **JPM: (ead1, ead2, ead3, ead4) not useful this way**
  - You need to know what kind of EAD
  - This should use values from the EDHOC “External Authorization Data” registry.

- **Authors’ proposal**
  - This is actually our intention and we already refer to the registry. Planned updates/additions:
    - *‘ead1’, ‘ead2’, ‘ead3’ and ‘ead4’, specifying, if present, that the server supports **specific External Authorization Data (EAD) items to use** in the EDHOC message fields EAD_1, EAD_2, EAD_3 and EAD_4, respectively (see Section 3.8 of [I-D.ietf-lake-edhoc]).*
    - *For example, the following set of target attributes (ead1=5;ead2=10;ead3=5;ead3=42) denotes that the server supports: the use of the EAD item with ead_label 5 in EAD_1 and EAD_3; the use of the EAD item with ead_label 10 in EAD_2; and the use of the EAD item with ead_label 42 in EAD_3.*

OK with that?

JPM-5

- **Web-linking**
  - Target attributes can “describe” an EDHOC resource
  - I.e., how the server can run EDHOC through that resource

…

cred-t
// supported type of CRED

…

- **JPM: register values that ‘cred-t’ can take**
  - New registry under "Ephemeral Diffie-Hellman Over COSE (EDHOC)" registry group
  - Either in this document or in *draft-ietf-lake-edhoc*

- **Authors’ proposal**
  - Yes; creation preferred in *draft-ietf-lake-edhoc*
  - Value
    - -24..23 : Standards Action With Expert Review
    - -65536..-25 : Specification Required
    - 24..65535 : Specification Required
  - Description
  - Reference

Value	Description	Reference
0	CBOR Web Token (CWT) containing a COSE_Key in a 'cnf' claim	[RFC8392]
1	CWT Claims Set (CCS) containing a COSE_Key in a 'cnf' claim	[RFC8392]
2	X.509 certificate	[RFC5280]
3	C509 certificate	[I-D.ietf-cose-cbor-encoded-cert]

OK with that?

Extra point

- **Prefixing the name of the defined target attributes**
  - They are not generic, but very specific to EDHOC

- **Proposed prefix: “ed-”**
  - ed-method, ed-csuite, ... // already defined
  - ed-fflow, ed-rflow, ed-i, ed-r // new ones in slide 5
  - ed-prof // new one in slide 6
  - **OK with that?**

- **Any other renaming to consider?**

method
// supported EDHOC method

csuite
// supported EDHOC cipher suite

cred-t
// supported type of CRED

idcred-t
// supported type of ID_CRED

ead1, ead2, ead3, ead4
// supported type of EAD item

comb-req
// supported EDHOC+OSCORE request

Summary and next steps

- **Address all the WG Last Call comments**
- **Submit v -07 before the upcoming cut-off**
- **Submit PR to *draft-core-ietf-target-attr***
  - Consistent with renaming and addition of target attributes

Thank you!

Comments/questions?

https://github.com/core-wg/oscore-edhoc/

EDHOC + OSCORE request