Coordinating the Use of Application Profiles for Ephemeral Diffie-Hellman Over COSE (EDHOC)

draft-ietf-lake-app-profiles-04

Marco Tiloca, RISE
Rikard Höglund, RISE

IETF 125 Meeting – Shenzhen – March 16th, 2026

Recap

- **Two peers have to agree on an EDHOC application profile, specifying:**
  - The intended use of EDHOC, as to relevant processing and verification of messages
  - Parameters playing a role in the execution of EDHOC

- **Facilitate the definition, discovery, and coordinated use of EDHOC application profiles**
  - À la carte: list individual EDHOC features; and/or
  - Set menu: point to registered EDHOC application profiles, identified by integer ID

- **“Venues” of coordination:**
  - CBOR Object “EDHOC_Application_Profile” (for descriptions to store/retrieve and refer to)
  - Target attributes for web linking, e.g., in CoRE Link Format
  - New EDHOC EAD item “Supported EDHOC application profiles”
  - New error code (ERR_CODE) for the EDHOC error message
  - SVCB Resource Records (RR) for DNS

Updates since version -03

- **Editorial fixes and improvements**

- **Section 5.1 – Clarification about using the new EAD item**
  - Forbidden violations of prescriptive indications in the EAD item (always been the case)
  - The EDHOC session fails if such a violation is detected at any time (noted at IETF 124)
    - *Upon receiving an EDHOC message and throughout the session, a peer MUST check whether the other peer has violated such indications. If any violation is found, the peer MUST abort the EDHOC session and MUST reply with an EDHOC error message with error code (ERR_CODE) 1.*

Updates since version -03

- **Grammar fix in the CDDL definition of ead_value for the new EAD item**
  - OLD: `EDHOC_Information : map`
  - NEW: `EDHOC_Information = map`

- **Added CDDL definitions of two parameters, both in the CBOR-encoded EDHOC_Information object**
  - Section 3.2: "app_prof"
  - Section 5.1.2: "exporter_out_len"

```
app_prof_parameter = (
  ? 23 => int / [2* int]          ; app_prof
)
```

```
exporter_out_len = (
  ? 22 => [1* [uint, uint]]       ; exporter_out_len
)
```

Oops! In the draft, the comment on the right says ";app_prof". Will fix in the next version.

Updates since version -03

- **Removed mentioning/use of not-so-necessary parameters**
  - Based on issue #1 raised by Christian – Thanks!

- **Parameters in the EDHOC_Information object**
  - “max_msgsize”; “coap_ct”; “ep_id_types”; “transports”
  - Their actual definition was removed in *draft-ietf-ace-edhoc-oscore-profile*

- **Corresponding link target attributes in this document**
  - 'ed-max-msgsize'; 'ed-coap-ct'; 'ed-epid-t'; 'ed-tp
  - Section 3.1 – Removed their definition
  - Section 11.3 – Removed their registration requests to IANA

Updates since version -03

- **Section 5.1 – Use of advertise_flag in the new EAD item within message_1**
  - Was “reply_flag”; the new name better fits its use in SVCB Resource Records (see next slide)

- **Same semantics. The Initiator says:**
  - (a) Tell me about you in the next message; or
  - (b) Don’t bother telling me about you

- **Optional and only for EDHOC message_1**
  - true → meaning (a) → info must follow-up
  - false → meaning (b) → info may still follow-up

- **Discussed special case where:**
  - The Initiator wants to use advertise_flag, but …
  - The Initiator has nothing to advertise about itself
  - → The CBOR sequence APP_PROF_SEQ only consists of the empty CBOR map

```
ead_value = ead_1_value / ead_2_value

ead_1_value = bytes .cborseq OUTER_SEQ

ead_2_value = bytes .cborseq APP_PROF_SEQ

; This defines an array, the elements of which
; are to be used in the CBOR Sequence OUTER_SEQ:
OUTER_SEQ = [?advertise_flag, APP_PROF_SEQ]

advertise_flag = bool

; This defines an array, the elements of which
; are to be used in the CBOR Sequence APP_PROF_SEQ:
APP_PROF_SEQ = [1* element]

element = profile_id / profile_id_with_eads / EDHOC_Information

profile_id = int

profile_id_with_eads = [profile_id, 1* uint]

; The full definition is provided in
; draft-ietf-ace-edhoc-oscore-profile
EDHOC_Information = map
```

Updates since version -03

- **Section 6 – Defined used of advertise_flag also in SVCB Resource Records**
  - Based on issue #2 raised by Christian – Thanks!

- **In the SvcParamKey "edhoc-app-prof" ...**
  - ... edhoc-app-prof-value is a CBOR byte string, with value ...
  - ... the binary representation of the CBOR sequence SVCB_EDHOC_APP_PROF

```
edhoc-app-prof-value = bytes .cborseq SVCB_EDHOC_APP_PROF

; This defines an array, the elements of which
; are to be used in the CBOR Sequence SVCB_EDHOC_APP_PROF:
SVCB_EDHOC_APP_PROF = [?advertise_flag, server_info]

advertise_flag = bool

server_info = APP_BSTR / [2* APP_BSTR]

; The full definition of APP_PROF_SEQ
; is provided in Section 5.1
APP_BSTR = bytes .cborseq APP_PROF_SEQ
```

- **In SVCB_EDHOC_APP_PROF:**
  - Optional first element: advertise_flag = true
  - Required second element: server_info, i.e., instances of APP_PROF_SEQ (already in v -03)

- **Meaning of advertise_flag = true**
  - A peer that runs EDHOC with the server is encouraged to advertise the EDHOC application profiles that it supports, when sending its first EDHOC message in an EDHOC session

Updates since version -03

- **Section 4, Figure 4 – Added example of response in CoRE link-format**
  - Using the target attributes 'ed-ta-edcred-*'

- **Section 5.1.3 – Added examples of ead_value in the new EDHOC EAD item**
  - Figure 7, for EDHOC message_1
  - Figure 8, for EDHOC message_2

- **Section 5.2.1, Figure 9 – Added example of ERR_INFO**
  - For the EDHOC error message with the new Error Code TBD_ERROR_CODE

- **Section 6.1 – Added examples of wire-format values in SVCB Resource Records**
  - Figure 13, for the SvcParamKey "edhocpath“
  - Figure 14, for the SvcParamKey "edhoc-app-prof“

Updates since version -03

Section 10 – Added security considerations

- **Inherit considerations from RFC 9528 and RFC 9668**
- **Some advertisement/discovery approaches do not use secure communication**
  - Potential consequences are also discussed
- **Information obtained in an unsecured way should be treated as a hint**
- **Manipulated/bogus information → Wrong expectations on that peer's capabilities**
- **No impact on the security of EDHOC in itself**
  - Same security guarantees, as per the way the EDHOC session is run

Updates since version -03

Section 9 – Added operational considerations

- **This toolbox is meant to make network operations smoother**
- **No significant impact expected on network performance and network operations**
- **Operators can observe unprotected advertisement of EDHOC application profiles**
  - Fine-tuning allocation of network resources
  - Knowledge sharing to identify “trends” in EDHOC application profiles and their use
- **An EDHOC peer should remember what has learned about other peers**
  - To avoid re-learning, at least in the short term
- **An EDHOC peer can report an EDHOC session that fails ...**
  - ... if the failure is in spite an understanding of common support
  - Helpful to detect misbehaviors and outdated information about supported profiles

Next steps

- **All the intended content should be present now; no open points or issues**
- **This version should be ready for a WG Last Call**
- **Two normative references are Internet Drafts**
  - (A) https://datatracker.ietf.org/doc/draft-ietf-cose-cbor-encoded-cert/
    - In IESG Evaluation
  - (B) https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/
    - Still ongoing WG activities
- **Until (B) is also sent to the IESG …**
  - Hold on or have the WG Last Call on this document?
  - Hold on the publication request for this document?
- **Directions from WG Chairs and AD?**

Thank you!

https://github.com/lake-wg/app-profiles