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

draft-ietf-lake-app-profiles-03

Marco Tiloca, RISE
Rikard Höglund, RISE

IETF 124 Meeting – Montreal – November 6th, 2025

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**
  - <u>À la carte</u>: list individual EDHOC features; and/or
  - <u>Set menu</u>: 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 -02

- **Minor clarifications and editorial improvements**

- **Fixed 3 errors in the <u>CDDL notations</u> – Thanks, Carsten!**
  - Typical mix-up of CDDL and CBOR diagnostic notation, e.g.:
    - OLD: PATH_BSTR = << PATH_SEQ >>
    - NEW: PATH_BSTR = bytes .cborseq PATH_SEQ

- **Addressed comment from IANA**
  - The registration of the “app_prof” parameter was incomplete
  - Added “Type” = NP (non-prescriptive)
    - Section 3.2 (parameter definition)
    - Section 10.4 (parameter registration)

Updates since version -02

- **Section 2 - EDHOC_Application_Profile object**
  - Version -02 was overly restrictive on the object scope
  - Also got feedback from Mališa at IETF 123

- **Removed a paragraph to relax restrictions on the scope:**
  - *An EDHOC_Application_Profile object does not convey information that does not play a role in completing an EDHOC execution. For instance, this includes ... properties and features of protocols other than EDHOC itself that build on the results from an EDHOC session (e.g., the version of the application protocol subsequently used).*

Updates since version -02

- **Parameters indicating EDHOC features can be prescriptive or non-prescriptive**
  - Prescriptive: authoritative statement on how to execute EDHOC (e.g., “message_4”)

- **New: added explicit expectation of compliance with prescriptive parameters**
  - When present in the new EAD item “Supported EDHOC application profiles”

- **Section 5.1 - Use of the EAD item in EDHOC message_1 and/or message_2**
  - Forbidden violations of <u>prescriptive</u> indications in the EAD item
    - *If the EAD item ... is included in EDHOC message_1 and/or message_2 during an EDHOC session, the peers MUST NOT act in violation of what is indicated by <u>prescriptive parameters</u> that are specified in those EAD items.*
  - The EDHOC session fails if such a violation is detected
    - *Upon receiving an EDHOC message, a peer MUST check whether the other peer has violated such indications. <u>If any violation is found, the peer MUST abort</u> the EDHOC session and MUST reply with an EDHOC error message with error code (ERR_CODE) 1.*

Updates since version -02

- **In terms of EDHOC application profiles, the Initiator might:**
  - have a complete knowledge about the Responder; or
  - have only a partial knowledge about the Responder, or none at all

- **Additional, new EAD item? Not needed!**

- **New: extended semantics of the EAD item "Supported EDHOC application profiles"**
  - Only for its use in EDHOC message_1

- **When including the EAD item in EDHOC message_1, the Initiator can also say:**
  - (a) Please tell me about you in the EAD item or in an EDHOC error message; or
  - (b) Don’t bother telling me about you in the EAD item or in an EDHOC error message

…

Updates since version -02

- **When including the EAD item in EDHOC message_1, the Initiator can also say:**
  - (a) Please tell me about you in the EAD item or in an EDHOC error message; or
  - (b) Don't bother telling me about you in the EAD item or in an EDHOC error message

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

- **Original content of ead_value (APP_PROF_SEQ)**
  - In message_1, it can be prepended by reply_flag
  - In message_2, no changes

- **No changes to APP_PROF_SEQ in itself**
  - Still reusable as-is, in the EDHOC error message and in the SVCB Resource Records (RR) for DNS

```
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 = [?reply_flag, APP_PROF_SEQ]

reply_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 -02

- **[1] defines the in-band negotiation of output lengths for the EDHOC_Exporter interface**
  - Based on a dedicated EAD item, used in EDHOC message_1 and/or message_2

- **Feedback from IETF 123**
  - Concerns on defining yet another EAD item specifically for this feature
  - The feature could be useful, if provided by the same toolbox of *draft-ietf-lake-app-profiles*

- **New: defined parameter "exporter_out_len" – Type: prescriptive**
  - Registered in the usual parameter namespace defined in [2]
  - To be used <u>only in the EAD item</u> "Supported EDHOC application profiles"
    - Like in [1]: either peer can say something; the Responder cannot amend what the Initiator has said
  - <u>Not intended</u> for:
    - CBOR Object "EDHOC_Application_Profile"
    - EDHOC error message
    - SVCB Resource Records (RR) for DNS
    - CBOR Object "EDHOC_Information" used in the ACE framework [2]

[1] https://datatracker.ietf.org/doc/html/draft-tiloca-lake-exporter-output-length
[2] https://datatracker.ietf.org/doc/html/draft-ietf-ace-edhoc-oscore-profile

Updates since version -02

- **Section 6 – Coordination through SVCB Resource Records (RR)**
  - A client can do name resolution through DNS and discover support for EDHOC at the server

- **Based on two SvcParamKeys, already defined in version -02**
  - "edhocpath"
    - Set of URI path components, each for one EDHOC resource
  - "edhoc-app-prof"
    - Set of EDHOC-related information about the server
    - Each element of the set is paired with one URI path component of "edhocpath" (if any)

- **New: specified wire-format and presentation format for the SvcParamKeys**
  - Thanks to Martine for the discussion at IETF 123!

…

Updates since version -02

- **“edhocpath” wire-format**
  - Binary representation of the CBOR data item edhocpath-value

```
edhocpath-value = PATH_BSTR / [2* PATH_BSTR]

PATH_BSTR = bytes .cborseq PATH_SEQ

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

path_segment = tstr
```

- **“edhocpath” presentation format**
  - Comma-separated list of one or more absolute paths
  - See also Section 7.1.1 and Appendix A.1 of RFC 9460
  - i-th path: textual representation of the path specified by the i-th CBOR sequence PATH_SEQ in the wire-format value
  - The textual representation of each path follows the semantics of path-absolute from the ABNF definition in Section 3.3 of RFC 3986

```
path-absolute = "/" [ segment-nz *( "/" segment ) ]

segment       = *pchar
segment-nz    = 1*pchar

pchar = unreserved / pct-encoded / sub-delims / ":" / "@"

unreserved    = ALPHA / DIGIT / "-" / "." / "_" / "~"
pct-encoded   = "%" HEXDIG HEXDIG
sub-delims    = "!" / "$" / "&" / "'" / "(" / ")"
             / "*" / "+" / "," / ";" / "="
```

...

Updates since version -02

- **“edhoc-app-prof” wire-format**
  - Binary representation of the CBOR data item edhoc-app-prof-value

```
edhoc-app-prof-value = 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
```

- **“edhoc-app-prof” presentation format**
  - CBOR extended diagnostic notation of edhoc-app-prof-value in the wire-format value
  - Care must be taken:
    - When representing Unicode with the limited ASCII character subset (e.g., through Punycode, see RFC 3492);

    AND
    - In removing unnecessary common blank spaces within the CBOR extended diagnostic notation

Next steps

- **All the intended parameters and features should have been included**
  - Is there anything else to consider adding?

- **Add examples in CBOR diagnostic notation, e.g., for:**
  - ead_value for the EAD item “Supported EDHOC application profiles” (Section 5.1)
  - ERR_VALUE for the EDHOC error message with the new error code (Section 5.2)
  - The SvcParamKeys “edhocpath” and “edhoc-app-prof” in SVCB Resource Records (Section 6)

- **Add security considerations**

- **Comments and reviews are welcome!**

Thank you!

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