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

draft-tiloca-lake-app-profiles-03

Marco Tiloca, RISE
Rikard Höglund, RISE

IETF 121 Meeting – Dublin – November 4th, 2024

Motivation

- **Peers have to agree about how to run EDHOC and on certain parameters**
  - Some are exchanged during the protocol execution, when a few can be negotiated

- **In general, two peers have to rely on an EDHOC application profile, specifying:**
  - The intended use of EDHOC, including relevant processing and verification
  - Parameters for the EDHOC execution, both in-band and out-of-band ones

- **How to facilitate the definition and discovery of EDHOC application profiles to use?**
  - Related points first raised during the WG Last Call of *draft-ietf-core-oscore-edhoc*
  - Agreed that it was better to address this topic in the LAKE WG

- **From the LAKE Charter:**

  The working group will also work on a Standard Track means for coordinating the use and discovery of EDHOC application profiles, the definition of a well-known application profile …

Updates since version -01

- **High-level improvements**
  - Clearer and more linear section ordering
  - Aligned with developments of the EDHOC and OSCORE profile of ACE [1]
  - Revised IANA considerations as to registration policies and early allocation

- **Current contribution:**
  - Identification of EDHOC application profiles by “Profile ID” // UPDATED
    - Values from the new IANA registry “EDHOC Application Profiles”
  - Additional parameters for the description of EDHOC application profiles // NEW
  - CBOR-based canonical representation of EDHOC application profiles
  - Set of well-known EDHOC application profiles // NEW
  - Actions for IANA // UPDATED

[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

Updates since version -01

Identification of EDHOC application profiles by Profile ID

- **Parameter "ed-prof" (1 or more; int)**
  - As link target attribute, e.g., in links to EDHOC resources at a CoAP server
  - As URI query parameter to discover EDHOC resources
- **Parameter "app_prof" in an EDHOC_Information object**
  - E.g., in the EDHOC and OSCORE profile of ACE [1]
  - Entry added to the "EDHOC Information" registry defined in [1]
- **Restrictions // UPDATED**
  - A profile can be either (i) identified or (ii) fully described
  - In (i), the identifier can be optionally accompanied only by a list of additionally supported EAD items
  - Avoid registrations of (many) very similar EDHOC profiles differing only about supported EAD items

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

RES: 2.05 Content
    </sensors/temp>;osc,
    </sensors/light>;if=sensor,
    </.well-known/edhoc>;rt=core.edhoc;ed-csuite=0;ed-csuite=2;
        ed-method=0;ed-cred-t=1;ed-cred-t=3;ed-idcred-t=4;
        ed-i;ed-r;ed-comb-req,
    </edhoc-alt>;rt=core.edhoc;ed-prof=500;ed-ead=333
```

Figure 1: The Web Link.

Name	CBOR label	CBOR type	Registry	Description
app_prof	18	int or array	EDHOC Application Profiles Registry	Set of supported EDHOC Application Profiles

Table 1: EDHOC_Information Parameter "app_prof"

[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

Updates since version -01

Additional parameters for description of EDHOC application profiles // NEW

- **Aligned with suggestions from RFC 9528 on what information can characterize a profile**
  - Separately for use in web links (e.g., as target attributes) and in the EDHOC_Information object
- **"ed-max-msgsize" (uint) / "max_msgsize" (uint)**
  - Maximum size of EDHOC messages in bytes
- **"ed-coap-cf" (no value) / "coap_cf" (True or False)**
  - Requested use of the CoAP Content-Format Option in CoAP messages transporting an EDHOC message
- **"ed-idep-t" (1 or more; int) / "id_ep_types" (int or array)**
  - Supported types of endpoint identifiers for EDHOC
- **"ed-tp" (1 or more; int) / "transports" (int or array)**
  - Supported means for transporting EDHOC messages

Name	CBOR label	Description	Reference
EUI-64	0	An EUI-64 identity	[RFC-XXXX][RFC4291]

Table 4: EDHOC Endpoint Identity Types **NEW**

Transport ID	Name	Description	Reference
0	CoAP over UDP	EDHOC messages are transported as payload of CoAP messages, in turn transported over UDP	[RFC7252], Appendix A.2 of [RFC9528]
1	CoAP over TCP	EDHOC messages are transported as payload of CoAP messages, in turn transported over TCP	[RFC7252] [RFC8323]
2	CoAP over WebSockets	EDHOC messages are transported as payload of CoAP messages, in turn transported over WebSockets	[RFC7252] [RFC8323]

Table 5: EDHOC Transports **NEW**

Updates since version -01

CBOR-based canonical representation of EDHOC application profiles

- **No major changes since last time**
- **Possible entries (i.e., considered namespace)**
  - Same of the EDHOC_Information_Object
  - Same CBOR map keys from the “EDHOC Information” registry

```
EDHOC_Application_Profile = {
      1 => int / array,     ; methods
      9 => int / array,     ; cred_types
     18 => int,             ; app_prof
   * int / tstr => any
}
```

EDHOC_Application_Profile object (CBOR map)

- **Restrictions on possible entries**
  - MUST be present: ‘app_prof’, ‘methods’, and ‘cred_types’
  - MUST NOT be present: ‘session_id’, ‘uri_path’, ‘initiator’, and ‘responder’
  - MAY be present: any other from the “EDHOC Information” registry
- **Clearer motivation and benefits in Section 1 “Introduction” // UPDATED**
  - Largely built on feedback from Brian Sipos [2] – Thanks!
  - Transport- and setup-independent; no need to reinvent an encoding for the available options to run EDHOC
  - Retrievable during a discovery process, provisioning of credentials, or device on-boarding/registration

[2] https://mailarchive.ietf.org/arch/msg/lake/GQmnLrn1R29o5u3Xy8CVEQT7KYo/

Updates since version -01

Set of well-known EDHOC application profiles // NEW

- **What they are supposed to mean**
  - Reflect what is most common and expected to use for EDHOC
  - NOT "default profiles" to use if nothing else is said
  - NOT overriding what is mandatory to implement
  - NOT necessarily supported by the resource *./well-known/edhoc* if nothing else is said
- **Entries in the "EDHOC Application Profiles" registry**
- **Represented as EDHOC_Application_Profile objects**

```
{
       e'methods' : 3, / EDHOC Method Type 3 /
  e'cipher_suites' : 2, / EDHOC Cipher Suite 2 /
     e'cred_types' : 1, / CWT Claims Set (CCS) /
  e'id_cred_types' : 4, / kid /
      e'app_prof' : e'APP-PROF-WK-MINIMAL-CS-2'
}
```

```
{
       e'methods' : [0, 1, 2, 3], / EDHOC Method Types
                                    0, 1, 2, and 3 /
  e'cipher_suites' : [0, 1, 2, 3], / EDHOC Cipher Suites
                                    0, 1, 2, and 3 /
     e'cred_types' : [1, 0, 2, e'c509_cert'], / CWT Claims Set (CCS),
                                                CWT, X.509 certificate,
                                                and C509 certificate /
  e'id_cred_types' : [4, 14, 13, 34, 33, e'c5t', e'c5c'], / kid, kccs,
                                                            kcwt, x5t,
                                                            x5chain,
                                                            c5t, and
                                                            c5c /
      e'app_prof' : e'APP-PROF-WK-ADVANCED'
}
```

Profile ID	Name	Description	Reference
0	WK-MINIMAL-CS-2	Method 3; Cipher Suite 2; CCS; kid	[RFC-XXXX]
1	WK-MINIMAL-CS-0	Method 3; Cipher Suite 0; CCS; kid	[RFC-XXXX]
2	WK-BASIC-CS-2-X509	Methods (0, 3); Cipher Suite 2; (CCS, X.509 certificates); (kid, x5t)	[RFC-XXXX]
3	WK-BASIC-CS-0-X509	Methods (0, 3); Cipher Suite 0; (CCS, X.509 certificates); (kid, x5t)	[RFC-XXXX]
4	WK-BASIC-CS-2-C509	Methods (0, 3); Cipher Suite 2; (CCS, C509 certificates); (kid, c5t)	[RFC-XXXX]
5	WK-BASIC-CS_0-C509	Methods (0, 3); Cipher Suite 0; (CCS, C509 certificates); (kid, c5t)	[RFC-XXXX]
6	WK-INTERMEDIATE-CS-2	Methods (0, 3); Cipher Suite 2; (CCS, X.509/C509 certificates); (kid, kccs, x5t, x5chain, c5t, c5c)	[RFC-XXXX]
7	WK-INTERMEDIATE-CS-0	Methods (0, 3); Cipher Suite 0; (CCS, X.509/C509 certificates); (kid, kccs, x5t, x5chain, c5t, c5c)	[RFC-XXXX]
8	WK-ADVANCED	Methods (0, 1, 2, 3); Cipher Suites (0, 1, 2, 3); (CCS, CWT, X.509/C509 certificates); (kid, kccs, kcwt, x5t, x5chain, c5t, c5c)	[RFC-XXXX]

Next steps

- **Move out the new parameters for the EDHOC_Information object to [1]**
  - Except for “app-prof”, which pertains to the main scope of this document
- **Specify a further way to advertise supported EDHOC capabilities and application profiles**
  - In EDHOC itself: in EAD_1/EAD_2, or in an EDHOC error message replying to EDHOC message_1
  - For the actual encoding, rely on the same parameters and objects already in use
- **Address a comment from IANA**
  - *If appropriate, please specify the range the CoAP Content-Format value should be assigned from: https://www.iana.org/assignments/core-parameters/core-parameters.xhtml*
  - 0-255 (Expert review) should be appropriate
- **Got good feedback and input on the way forward during the Hackathon – Thanks!**
- **Ready for Working Group Adoption?**

[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

Thank you!

https://gitlab.com/crimson84/draft-tiloca-lake-app-profiles