EDHOC Status & Open Issues

draft-ietf-lake-edhoc-11
draft-selander-lake-traces-01

LAKE WG interim, Oct. 05, 2021

Outline

- Main changes since IETF 111
  - –08 → –11
- Open Github issues
- Next steps

Main changes –08 → –11 1(2)

Key derivation

- MAC_2 and MAC_3 are now generated with EDHOC-KDF (was #121)
- info field "context" (bstr) is now general and explicit in EDHOC-KDF
- Removed edhoc_aead_id from info
  - was already included in transcript_hash
- Changed several of the KDF and Exporter labels

Cipher suites

- SUITES_I simplified to only contain the selected and more preferred by I
- Added EDHOC MAC length to cipher suite for use with static DH

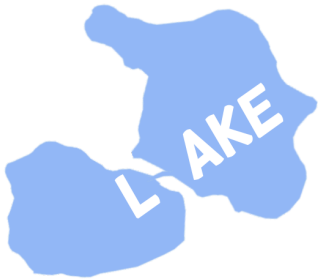
Message size related formatting

- G_Y and CIPHERTEXT_2 are now included in one CBOR bstr (was #103)
- Extension of 'kid' to int ('kid2' removed)
  - Propose to make this change in COSE
  - PR against ietf-cose-rfc8152bis-struct
  - On agenda for COSE interim next week

Main changes –08 → –11 2(2)

- CWT-related
  - Changed name of UCCS to CCS (CWT Claims Set, see RFC 8392)
  - Names and description of COSE header parameters for CWT/CCS
    - Separate header parameters for CWT ('kcwt') and CCS ('kccs')
    - signifying CWT / CCS with 'cnf' claim containing a COSE key (see RFC 8747)
  - More details on the use of CWT and UCCS
  - Added ‘kid’ to CCS example
- External Authorization Data
  - Clarified EAD type, EAD encoding now supports multiple ead types in one message
  - changed CDDL names and added value type to registry
- Section changes
  - Restructure of Section 4, Key Derivation
  - Restructure and clarification of section 3.5, Authentication Parameters
  - New Section 7 on mandatory-to-implement (MTI)
- Misc
  - Updated message sizes
  - Replaced "perfect forward secrecy" with "forward secrecy”
  - Added core.edhoc to CoRE Resource Type registry
  - Replaced prepended 'null' with 'true’ (instead of ‘nil’) in the CoAP transport of message_1
  - Updated CDDL definitions
  - Updated security considerations
  - Updated Figures 1, 2, and 3

Open Github Issues



#178 Security considerations of TOFU
#174 Use of confirmable messages in CoAP
#171/177 Make it clearer what is explanations of COSE
#169 Content of draft-selander-lake-traces
#167 Registration procedures for the new EDHOC registries
#162 COSE CWT and UCCS header parameters - tagged, untagged, or both
#161 Make it clear that ID_CRED_x are COSE header maps
#142 is 101 pages too many words?
#139 Maybe align with https://datatracker.ietf.org/doc/draft-harkins-cfrg-dnhpke/
#84 Make .well-known/edhoc specific to OSCORE
#81 Effects of limited amounts of randomness
#73 MTI section
#50 Add cipher suite with Wei25519
#47 Test vectors additions
#22 Mandatory to implement cipher suite

Use of confirmable messages in CoAP (#174)

— Tune down requirement to use CON

OLD
"EDHOC messages are carried in Confirmable messages"

NEW
"The underlying CoAP transport should be used in reliable mode"

- OK?

Registration procedures for the new EDHOC registries (#167)

— What registration procedures for the new EDHOC registries?

OLD

— A mixture of: "Expert Review" and "Specification Required" (EDHOC Error Code Registry)

NEW

— EDHOC Error Code Registry changed to "Expert Review" to align with the others.

- OK?

— Currently all parameters are expert review without any differentiation between small and big numbers.

— Right approach?

ID_CRED_x are COSE header maps (#161)

- EDHOC relies on COSE for identification of authentication credentials
  - EDHOC supports all credential types for which COSE header parameters are defined
- New header parameters defined for CWT / CCS*) containing a COSE Key:

Name	Label	Value Type	Description
kcwt	TBD1	COSE_Messages	A CBOR Web Token (CWT) containing a COSE_Key in a 'cnf' claim
kccs	TBD2	map / #6(map)	A CWT Claims Set (CCS) containing a COSE_Key in a 'cnf' claim

- OK?

*) CCS = CWT Claims Set (a.k.a. UCCS)

CWT / CCS header parameters – tagged, untagged or both (#162)

- CRED_x needs to be defined such that it is **identical** when used by Initiator or Responder.
- When the authentication credential is a
  - **X.509:** CRED_x SHALL be the **end-entity DER encoded certificate wrapped in a CBOR bstr**
  - **C509:** CRED_x SHALL be the **end-entity C509Certificate (see draft-ietf-cose-CBOR-encoded-cert)**
  - **COSE_Key in a CWT:** CRED_x SHALL be the **untagged CWT**
  - **COSE_Key but not in a CWT:** CRED_x SHALL be an **untagged CCS**
    - Naked COSE_Keys are thus dressed as CCS when used in EDHOC which is done by prefixing the COSE_Key with 0xA108A101. - OK?

- The Initiator and Responder SHOULD **use an available authentication credential** (transported in EDHOC or otherwise provisioned) **without re-encoding**. - OK?

- **If re-encoding** of the authentication credential **may occur**, then **a common encoding** for CBOR based credentials is **bytewise lexicographic order of their deterministic encodings**
  - Section 4.2.1 of [RFC8949] - OK?

- Do CWT and CCS need several header parameter each similar to x5u x5t x5chain x5bag?

Content of draft-selander-lake-traces (#169)

- Annotated traces of EDHOC protocol runs
- Input, output and intermediate processing results
- To simplify testing of implementations
- Complement to test vectors
  - For -11: https://github.com/lake- wg/edhoc/tree/master/test-vectors-11
- Currently there are two traces
  1. Method 0, authentication with signatures, X.509 identified by 'x5t'
  2. Method 3, authentication with static DH, CCS identified by 'kid'
  - For each trace:
    - message_1
    - message_2
    - message_3
    - message_4
    - OSCORE Parameters
    - Key Update

- OK?

Effects of limited amounts of randomness (#81)

— Request to:

  "outline how a monotonous counter (similar to that of OSCORE B.1.1) can be used together with a private secret to obtain sufficient randomness."

— Include example or provide reference?

Which parts of the spec are MTI? (#73)

- New Section 7
  - may support only Initiator or only Responder
  - may support only a single method. None of the methods are mandatory-to-implement.
  - MUST support the EDHOC-Exporter.
    - SHOULD support EDHOC-KeyUpdate.
  - MAY support message_4.
  - Error codes 1 and 2 MUST be supported.
  - MUST support 'kid' parameters of type int.

- **Are any COSE header parameters (kid, kcwt, kccs, x5t, c5c, etc.) MTI?**

- **Is any credential type (CCS, CWT, X.509, C509) MTI?**

- **Is support of EAD MTI?**

Test vectors (#47)

- 10 / 12 done
- Latest done: JSON encoding
- **Remains:**
  - Add real certificates to test vectors
    - 0:CBOR native and DER (and possibly later 1:ASN.1 translated)
  - Add ciphersuites 2 and 3 to test vectors
    - ECDSA keys should print out full y coordinate

Github issues not mentioned so far

#178 Security considerations of TOFU
#171/177 Make it clearer what is explanations of COSE
#142 is 101 pages too many words?
#139 Maybe align with https://datatracker.ietf.org/doc/draft-harkins-cfrg-dnhpke/
#84 Make .well-known/edhoc specific to OSCORE
#50 Add cipher suite with Wei25519
#22 Mandatory to implement cipher suite

- minor / straightforward
- independent from protocol
- pending decision from LAKE WG

Next steps

- Progress issues (close those confirmed with WG, fix minor, …)
- Submit edhoc−12
  - No need to update traces-01

The authors think the protocol is in good shape for reviewing, testing and analyzing

- Volunteers to review?
- Who wants to participate in the next interop?
- Time plans for additional security analysis?
  - Announcement?
- Ready for (1st) WGLC?