EDHOC Status, Open Issues

draft-ietf-lake-edhoc-12
draft-selander-lake-traces-02

LAKE WG interim, Nov. 12, 2021
Content

— Main changes since IETF 111
   -08 → -12

— Open Github issues
   — Reviews
   — Test vectors
   — Other
Main changes -08 → -11

Key derivation
- MAC_2 and MAC_3 are now generated with EDHOC-KDF
- 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
- 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

Discussed at LAKE WG interim Oct. 05
Main changes -08 → -11

— 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
  — message_1 prepended with ‘true’ in CoAP transport
  — Updated CDDL definitions
  — Updated security considerations
  — Updated Figures 1, 2, and 3

Discussed at LAKE WG interim Oct. 05
Main changes -11 → -12

Clarifications
- COSE “—sender” parameters are not used
- KEMs (incl. PQC KEMs) can later be added to method 0
- All COSE signatures (incl. PQC signatures) are supported
- Initiator selection of ciphersuite
- Updated MTI compliance requirements
  - MUST support ‘kid’ of type int
- COSE internal processing moved to appendix C.3
- Fixed internal references
Open Github Issues (excl. issues about test vectors and reviews)

# 201 Minor cryptographic explanations
- The MAC length MUST be at least 8 bytes.
- Compact representation only for G_X and G_Y
- nonce also for binding with the event that triggered KeyUpdate
- Explanation of no running hash

# 198 Updated Internet Threat Model considerations
- Security considerations based on draft-arkko-arch-internet-threat-model-guidance

#193 Allow COSE HPKE algorithms for method 0?
- Only considered if COSE quickly decides that this is the future for PQC KEMs in COSE.
- Would not effect current G_X, G_Y KEM

#191 Correct the information about non-repudiation.
- Need input and output of the signature function, not ephemeral key.

#189 Optional padding to hide length of ID_CRED_I and ID_CRED_R? (slide 8)
Open Github Issues (excl. issues about test vectors and reviews)

#186 EAD internal structure and the EAD API
   — Input to the API should likely be non-CBOR int and non-CBOR byte string
   — More analysis of how EAD is likely to be used and what the int label refers to needed.

#178 Security considerations of TOFU

#142 is 101 pages too many words?

#139 Maybe align with https://datatracker.ietf.org/doc/draft-harkins-cfrg-dnhpke/
   — Mail sent to CFRG pointing out the different activities in the area: EDHOC, HPKE, TLS

#84 Make .well-known/edhoc specific to OSCORE

#81 Effects of limited amounts of randomness
   — PR #197 with reference to Appendix B.1.1 of OSCORE RFC 8613

#50 Add cipher suite with Wei25519

#22 Mandatory to implement cipher suite
Optional padding to hide length of ID_CRED_I and ID_CRED_R? (#189)

— Missing privacy considerations that EDHOC leaks info about ID_CRED and EAD lengths

— Should we provide an option to conceal the length of the identifiers ID_CRED_I and ID_CRED_R?
  — OPTIONAL padding
  — Included in TLS 1.3, IKEv2

— Proposal in PR #190:
  — Updated security considerations
  — Padding:
    — plaintext = ( ? PAD, ID_CRED_y / bstr / int, Signature_or_MAC_x, ? EAD_x )
    — PAD = 1*true
    — Using sequence of CBOR simple value ‘true’ (0xf5)
Issues about test vectors

#169 Content of draft-selander-lake-traces
   - Discussed earlier in the meeting

#188 Missing SUITES_R in the test vectors
   - List of I and R supported cipher suites?
   - Flow with message_1, error, message_1, message_2, message_3?

#187 Test vector documentation
   - Table of content

#185 Test Vectors - more suites

#47 Test vectors additions (see slide 10)
Test vectors additions (#47)

- 10 / 12 done
- Latest done: JSON encoding
- Remains:
  - Add real certificates to test vectors
    - X509 DER and C509 0:CBOR native (and possibly later C509 1:ASN.1 translated)
  - Add cipher suites 2 and 3 to test vectors
Reviews

— Marco Tiloca (#192)
— Stefan Hristozov (#194)
— Kathleen Moriarty (#196)
— Stephen Farrell (#202)
Selected comments by Stefan  1(2)

— 3.8. EAD
   — Who is supposed to encode/decode EAD, the application or the EDHOC implementation?

— 6. Error Handling
   — What is the use case for a success error code?
   — Probably it is good to give some example or reference why it is useful to log successes using a predefined error code and encoding.
   — Is logging the only use case for the success error code? For example, my implementation logs many things for debugging purposes. However, I never needed a success error code.

— 7. Mandatory-to-Implement Compliance Requirements
   — "Constrained endpoints SHOULD implement cipher suite 0 or cipher suite 2."
   — The difference between 0 and 1 and between 2 and 3 is only the size of the tag, i.e. the used algorithms are the same.
   — suggest changing to "...suite 0/1 or cipher suite 2/3" or similar.
Selected comments by Stefan 2(2)

— 8.7 Implementation consideration
   — "The selection of trusted CAs should be done very carefully and certificate revocation should be supported."

— Should OCSP (RFC6960) be used for certificate revocation checking?
— How to accomplish revocation with C509?
— How OCSP and EDHOC interact?
— Can OCSP stapling be used with EDHOC?
— Can we combine OCSP stapling with EAD?

— Additionally, to verify a certificate the device should be aware of the time, which is often problematic on constrained devices, i.e. when certificates are used the device must have a Real-Time Clock (RTC).
Selected comments by Kathleen

— 9. IANA Considerations
  — I see for the registries created that Expert review [RFC8126] is required.
  — What documentation is required?
  — Is it also Specification required or is there other guidance for the experts when considering updates?
  — I see this is discussed in 9.14, but perhaps adding specification recommended in each of the places a registry is created would be helpful.

(Relates to #167 (currently closed) discussed at the Oct 5 interim)
Selected comments by Stephen 1(2)

— Connection identifiers
  — Connection identifiers (which can be byte-strings) are sent in clear which could enable various network observer attacks for protocols that later send values obviously derived from connection IDs in clear.
  — If some proxy (that just muxes packets) sits between I and R then those cleartext identifiers could allow an observer on that link to more easily do traffic analysis of a specific initiator's traffic. Was any consideration given to deriving such identifiers in a less obvious manner?

— 1.5. Terminology
  — Which is normative, CDDL or English language text?
  — We seem to have a bit of a mixture.
Selected comments by Stephen  2(2)

— 3.6. Cipher Suites
  — Does EDHOC *really* support hash based sigs?
  — What’d be the consequence for EDHOC of using a private key too many times or loss of state?
  — (Are you missing a reference to rfc8778 there too or is one embedded in COSE stuff somewhere?)

— 8.7 (or somewhere):
  — If some random values are visible (connection identifiers?) then it can make sense to derive those from a different random stream compared to that used for randomly picking secrets.
  — That way the publicly visible random numbers are less likely to leak information about the state of the PRNG used for secrets.