EDHOC & Traces

draft-ietf-lake-edhoc-12
draft-ietf-lake-traces-00

LAKE WG interim, Dec. 15, 2021

Outline

- EDHOC
  - Still version -12
  - Updates to master branch, issues and PRs
- Traces
  - Now adopted
  - draft-ietf-lake-traces-00 == draft-selander-lake-traces-02
- Open Github issues
  - Reviews
  - Traces
  - Other

Reviews

closed/merged

- Marco Tiloca (#192, PR #199)
- Stefan Hristozov (#194, PR #200)
- Kathleen Moriarty (#196, Commit a4b182a)
- Stephen Farrell (#202, PR #211)
- Sean Turner (#217, PR #)

- Additional issues (re-)opened

New GH Issues

#215 Verification of identities in X.509 and CWT
- Apply same processing independent of credential (dependent on #212)

#214 Security considerations on generating secret material and public material such as connection IDs.
- Leaking information from public random material

#213 Security considerations on connection IDs
- Tracking based on connection IDs

#212 Shorten 3.5
- 6 pages about authentication parameters can be shortened

#210 Add appendix about the use of EAD
- Separate slide

#209 Change MTI cipher suite to (0 AND 1) OR (2 AND 3)
- Separate slide

#208 Error message => Discontinue
- Needed because errors may be sent for various reasons. Add “left to implementer” in text.

#204 Length of labels, removal of master
- OSCORE_Master_Secret -> OSCORE_Secret, avoiding extra calls with hash function in KDF. PR #205.

Suite (0 AND 1) OR (2 AND 3) (#209)

Related to #22 MTI cipher suites

- For many constrained IoT devices it is problematic to support several crypto primitives.
- Existing devices can be expected to support either ECDSA or EdDSA.
- Cipher suites **0** (AES-CCM-16-64-128, SHA-256, 8, X25519, EdDSA, AES-CCM-16-64-128, SHA-256) and **1** (AES-CCM-16-128-128, SHA-256, 16, X25519, EdDSA, AES-CCM-16-64-128, SHA-256) only differ in size of the MAC length, so supporting one or both of these is no essential difference.
- Similarly for cipher suites **2** (AES-CCM-16-64-128, SHA-256, 8, P-256, ES256, AES-CCM-16-64-128, SHA-256) and **3** (AES-CCM-16-128-128, SHA-256, 16, P-256, ES256, AES-CCM-16-64-128, SHA-256).
- To enable as much interoperability as we can reasonably achieve, less constrained devices SHOULD implement all four cipher suites **0-3**.
- Constrained endpoints SHOULD implement cipher suites **0 and 1, or** cipher suites **2 and 3**.

EAD use cases / example content (#210)

red = protected outside EDHOC
orange = may be protected outside EDHOC

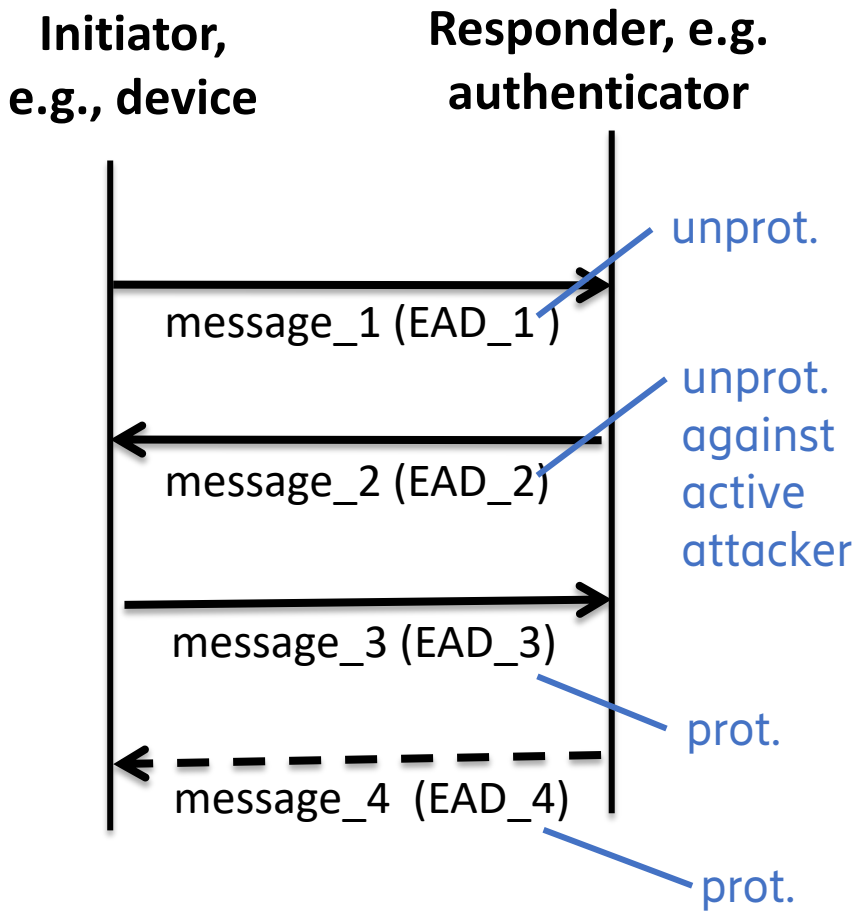
1. TTP authorization
   - EAD_1
     - URI of TTP
     - Encrypted identity
   - EAD_2
     - Voucher

2. Remote attestation
   - EAD_2
     - Request for EAT
   - EAD_3
     - EAT

3. Certificate enrollment
   - EAD_3
     - CSR
   - EAD_4
     - Certificate (or reference)

4. OCSP stapling?
   - EAD_2, EAD_3
     - OCSP response

Processing steps
- Pass EAD to security application, appendix TBD
- Verify allowed identity
- Verify signature or MAC



Updated old GH issues

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

- Note G_X collision already in processing of message_1
- Security considerations on 64 and 128 bit MACs
- Add MTI cipher suite considerations

198 Updated Internet Threat Model considerations

PR #207, merged

- Security considerations based on draft-arkko-arch-internet-threat-model-guidance

#193 Allow COSE HPKE algorithms for method 0?

Proposal: no change

- 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.

Done in master

- 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?

PR #190

OLD
"OPTIONAL to support"
NEW
"OPTIONAL to support when sending
MANDATORY to support when received"

Updated old GH issues

#186 EAD internal structure and the EAD API — PR #206, closed/merged

- 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 — Add use case, pending input

#167 Registration procedures for the new EDHOC registries — Reopened, next slide

#142 is 101 pages too many words?

#139 Maybe align with https://datatracker.ietf.org/doc/draft-harkins-cfrg-dnhpke/ — No reaction, close?

- Mail sent to CFRG pointing out the different activities in the area: EDHOC, HPKE, TLS

#84 Make .well-known/edhoc specific to OSCORE — Not clear why in this draft

#81 Effects of limited amounts of randomness — Done, if the creator of the issue agrees ☺

- PR #197 with reference to Appendix B.1.1 of OSCORE RFC 8613

#50 Add cipher suite with Wei25519 — Not critical for this draft, can be registrered later

#22 Mandatory to implement cipher suite — Updated per #209. Ready for decision?

Comment 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.

— Discussed at the Oct 5 interim (#167)
— Conclusion: Expert review would be sufficient as a general scheme for these registers
— But surely we would want a specification for a new EDHOC method type
— Any other registers that require a spec.?
— Reopened #167

Proposed traces

old
new

1.
- method 3 (stat-stat)
- suite 0 (X25519)
- I CCS
- R CCS
- ID_CRED_I kid
- ID_CRED_R kid

2.
- method 0 (sig-sig)
- ~~suite 0 (X25519)~~ suite 2 (ECDSA)
- I Cert X.509
- R Cert X.509
- ID_CRED_I x5t
- ID_CRED_R x5t

3.
- wrong selected cipher suite (ERR-CODE 2)
- method 1 (sig-stat)
- suite 1 (EdDSA, X25519)
- I Cert X.509
- R CCS
- ID_CRED_I x5t
- ID_CRED_R kid

4.
- method 2 (stat-sig)
- suite 3 (P-256, ECDSA)
- I Cert X.509
- R CCS
- ID_CRED_I x5chain
- ID_CRED_R kccs

Selected comments by Sean 1(2)

- s1.2/s3.9
  - Applicability statement in the context of RFC 2026

No. Change term?

- s4.4/s5.1 (question): Do you need to provide advice on when to delete the old PRK_4x3m? I.e., does the peer that sent this need to wait for some kind of confirmation before deleting it?
  - Verify message with new context before discarding old context
  - Ref to draft-ietf-core-oscore-key-update-00.html#section-4.3.1
- s5.2.3, s5.3.3, s5.4.3, s5.5.3, last sentence (question - probably being pedantic): If there is an error but an error message is not sent, is the session discontinued? How does the peer know it was discontinued if an error is not sent?

Related to #208

- s6.2 (nit): It's really more "Freeform" than unspecified right? I mean the string is required so it's definitely not unspecified per se.

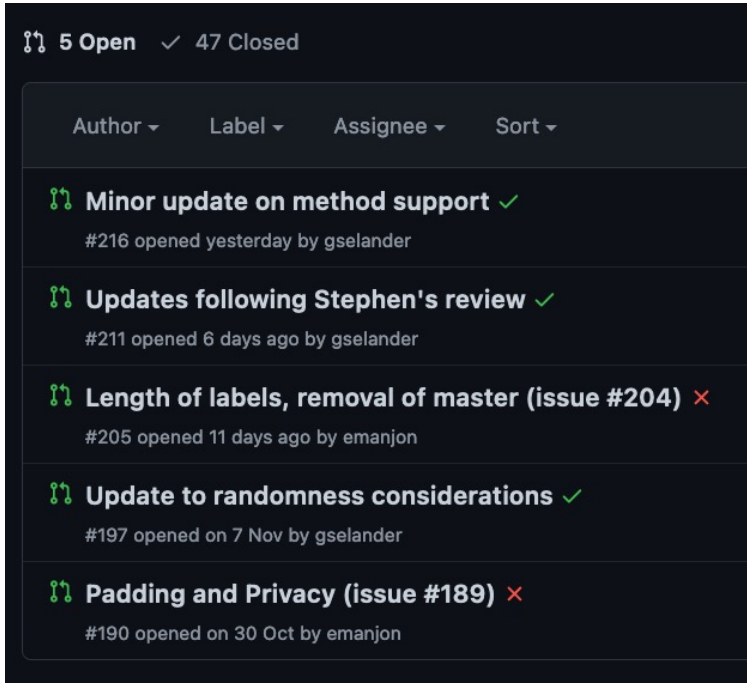
New description instead of "Unspecified"?

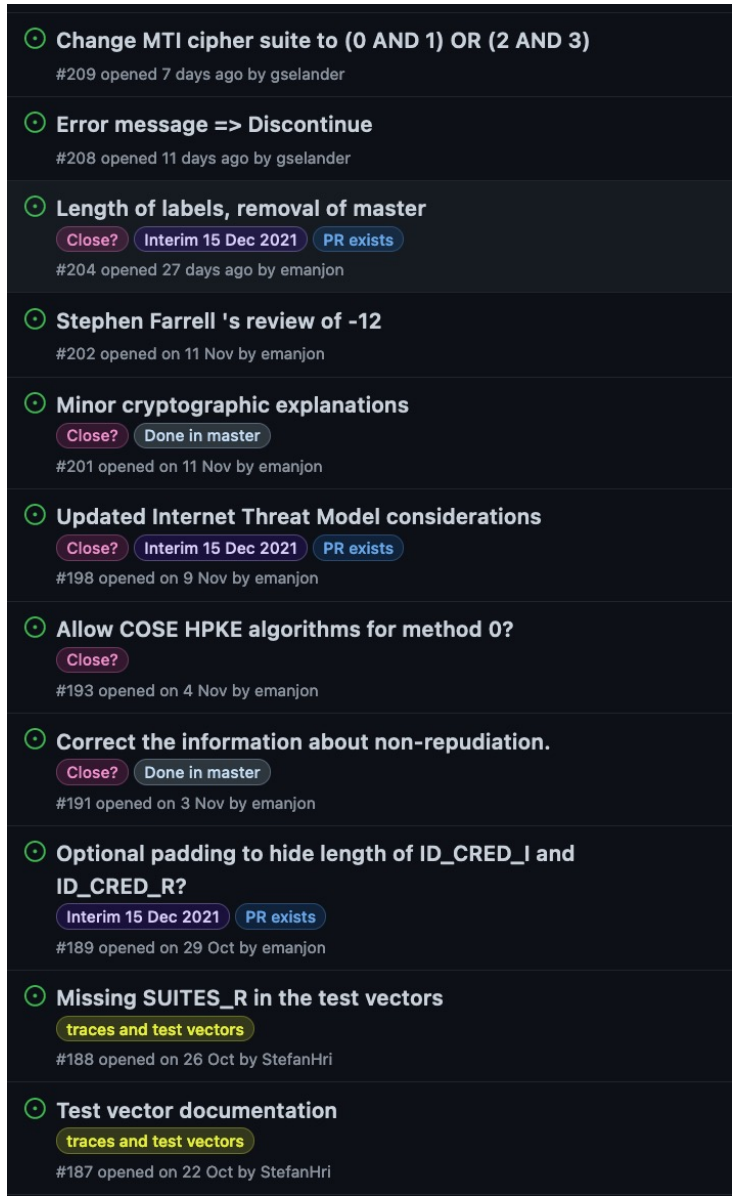
Selected comments by Sean 2(2)

— s5.1 (question): Is a state diagram needed? One thing people clamored for from TLS was a state machine. Maybe a diagram isn’t needed because there are so few states?

Next steps

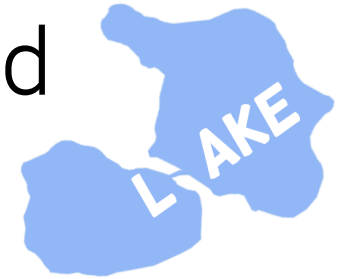
- Complete review updates
- Send mail about old issues to be closed / PRs to be merged
- Update of -traces
  - additional methods
  - P-256 based cipher suites





Slides from IETF 112

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 XX)

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

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 toderive 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.