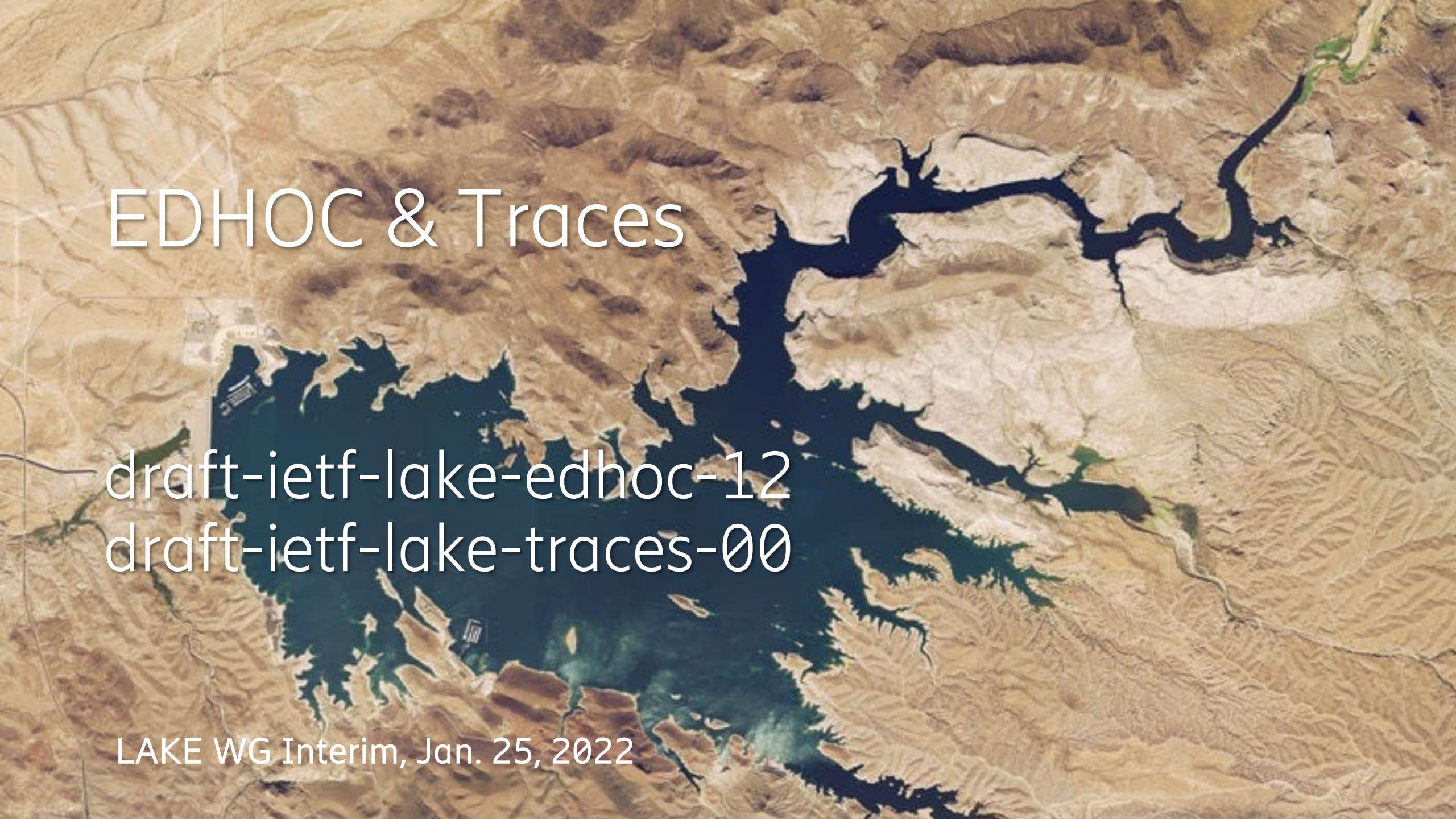

EDHOC & Traces

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

LAKE WG Interim, Jan. 25, 2022

Changes since December interim

- No new drafts
  - EDHOC
    - Still version -12
  - Traces
    - draft-ietf-lake-traces-00 == draft-selander-lake-traces-02

- https://github.com/lake-wg/edhoc
  - ~ 15 new issues
  - A number of merged PRs
  - New test vectors for P256 (thanks Marek!)

GitHub Issues

- Vectors.cpp app build is not cross-platform friendly [traces and test vectors]
  #229 opened 4 days ago by malishav
- Not clear which test vectors are in draft-ietf-lake-traces [traces and test vectors]
  #228 opened 4 days ago by malishav
- Inconsistent test vectors [traces and test vectors]
  #227 opened 4 days ago by malishav
- State diagram [Close?] [PR exists]
  #224 opened 14 days ago by gselander
- [x] Changes needed in 3.5 (identity, credential, trust achor) [3.5 Cluster]
  #223 opened 14 days ago by emanjon
- Feedback regarding test vectors [traces and test vectors]
  #222 opened on 22 Dec 2021 by StefanHri
- Sean Turner's review of -12 [Merged to master]
  #217 opened on 15 Dec 2021 by gselander
- Verification of identities in X.509 and CWT [3.5 Cluster]
  #215 opened on 11 Dec 2021 by gselander
- Security considerations on gererating secret material and public material such as connection IDs. [PR exists]
  #214 opened on 10 Dec 2021 by emanjon
- Shorten 3.5 [3.5 Cluster]
  #212 opened on 8 Dec 2021 by gselander
- Add appendix about the use of EAD [EAD cluster]
  #210 opened on 7 Dec 2021 by gselander
- Change MTI cipher suite to (0 AND 1) OR (2 AND 3) [Cipher Suite cluster] [Close?] [Interim 25 Jan 2022] [Merged to master]
  #209 opened on 7 Dec 2021 by gselander

- Error message => Discontinue [Interim 25 Jan 2022] [PR exists]
  #208 opened on 3 Dec 2021 by gselander
- Stephen Farrell 's review of -12 [Merged to master]
  #202 opened on 11 Nov 2021 by emanjon
- Missing SUITES_R in the test vectors [traces and test vectors]
  #188 opened on 26 Oct 2021 by StefanHri
- Test vector documentation [traces and test vectors]
  #187 opened on 22 Oct 2021 by StefanHri
- Test Vectors - more suits [traces and test vectors]
  #185 opened on 19 Oct 2021 by stoprocent
- Security considerations of TOFU [3.5 Cluster]
  #178 opened on 27 Sep 2021 by emanjon
- Content of draft-selander-lake-traces [traces and test vectors]
  #169 opened on 13 Sep 2021 by emanjon
- Registration procedures for the new EDHOC registries
  #167 opened on 10 Sep 2021 by emanjon
- EAD is underspecified [EAD cluster]
  #149 opened on 5 Aug 2021 by emanjon
- is 101 pages too many words?
  #142 opened on 29 Jul 2021 by sftcd
- Add cipher suite with Wei25519 [Cipher Suite cluster] [Close?] [Interim 25 Jan 2022]
  #50 opened on 18 Dec 2020 by emanjon
- Test vectors additions [traces and test vectors]
  #47 opened on 14 Dec 2020 by fpalombini 10 of 12 tasks
- Mandatory to implement cipher suite [Cipher Suite cluster] [Interim 25 Jan 2022]
  #22 opened on 5 Nov 2020 by gselander

Test Vectors

Three things to distinguish

1. Test vectors in github.com/lake-wg/
   - https://github.com/lake-wg/edhoc/tree/master/test-vectors-11
     - Files: vectors.txt, vectors-json.txt
     - code in vectors.cpp
   - https://github.com/lake-wg/edhoc/tree/master/test-vectors-11/p256
     - File: vectors-json.txt
     - code in https://github.com/stoprocent/edhoc/tree/feature/mbedtls/test-vectors-11

2. Test vectors in draft-ietf-lake-**traces**
   - Annotated processing steps with printout of CBOR diagnostic notation

3. Cipher suites implemented to claim compliance (issue #22, discussed later)

Content of -traces (#169)

- Purpose of draft-ietf-lake-traces:
  - Help implementers with one or a few examples of detailed printouts with intermediate steps
  - Not a complete set of test vectors (see files on github)
- Current version (draft-ietf-lake-traces-00) contains two traces
  1. Method 3 (static DH), cipher suite 0 (EdDSA), RPK encoded as CCS identified by 'kid' (key id)
  2. Method 0 (signature), cipher suite 0 (EdDSA), dummy X.509 identified by 'x5t' (hash of cert)
- Different proposals for content, no clear consensus:
  - All methods 0-3 (note that methods 1 and 2 are mix of 0 and 3)
  - Multiple cipher suites for each method (e.g. suite 0 and 2 for both method 0 and 3)
- **Propose to maintain two traces, replace second above with**
  2. Method 0 (signature), cipher suite 2 (ECDSA), X.509 identified by 'x5t' (hash of cert)

More on -traces

- Marek incoming co-author
- Intended status: Informational (fixed on github)
- Proposal to include supported cipher suites of I (in order of preference) and R
  - Trace 1. For example: I: (0) R: {0, 1}
  - Trace 2. For example: I: (3,2) R:{2}
    - Would add error message with SUITES_R = 2
- Minor changes in test vectors following change in EDHOC exporter labels
  - "OSCORE_Master_Secret" → "OSCORE_Secret"
  - "OSCORE_Master_Salt" → "OSCORE_Salt"
  - To align drafts, need to submit new version of -edhoc

Misc. on testing

- #227-229 Comments by Mališa
  - Cross platform generator
  - PRNG produces different outputs
  - Parametrize test vectors (relates to #187 documentation of test vectors)

- #222 Feedback by Stefan
  - Script for testing on microcontrollers
  - Use deterministic ECDSA in test vectors?

Thanks all!

- Interop testing in planning
  - Hackaton at IETF 113, or online
  - Contact: Marco

Reviews

- Marco Tiloca (#192, PR #199)
- Stefan Hristozov (#194, PR #200)
- Kathleen Moriarty (#196, Commit a4b182a)
- Stephen Farrell (#202, PR #211)
- Sean Turner (#217, PR #225)

open
closed
merged

(Additional issues were opened as result of specific review comments.)

Thanks, again!

#208 Error message => Discontinue

- Comments by Marco and Sean
  - New text (in PR #234):

    ”If any processing step fails, the Responder MUST send an EDHOC error message back, formatted as defined in {{error}}, and the session MUST be discontinued.”
- Observation
  - HTTP and CoAP defines errrors into two classes "client error" (there is something wrong with you) and "server error" (there is something wrong with me).
  - EDHOC does currently not follow this design and only has a single error:
    - 1 | tstr | Unspecified

- Proposed new error codes (work in progress)

  1 | tstr | Sender error
  2 | tstr | Receiver error

  1 → "something wrong done by the sender of the message that resulted in this error message"

  2 → "something locally wrong happened at the receiver of the message that resulted in this error message"

  Mail thread: https://mailarchive.ietf.org/arch/msg/lake/ABtedw5eR2M66563D5qI0Op1Unc/

Cipher suite cluster

- Compliance requirements
  - #22, Mandatory to implement cipher suite
  - #209, Change MTI cipher suite to (0 AND 1) OR (2 AND 3)

- #50, Add cipher suite with Wei25519
  - Added text about about how to transform curve25519 and edward25519 to Weierstraß format to enable acceleration on existing HW

New text/structure

- Section 3.5 cluster
  - #223, Changes needed in 3.5 (identity, credential, trust anchor)
  - #215, Verification of identities in X.509 and CWT
  - #212, Shorten 3.5
  - #178, Security considerations of TOFU
- Purpose: Better distinguish between EDHOC protocol (PoP, transfer credential info) and other authentication related operations (identity verification, chain validation, etc.)

- EAD cluster (discussed at previous interim)
  - #210, Add appendix about the use of EAD
  - #149, EAD is underspecified
- Purpose: Clarify use of EAD with examples

Next steps

- For discussion
  - Possible target for IETF 113:
    - Close all issues (may need help with test vector related)
    - Submit edhoc-13 and traces-01