EDHOC & Traces

draft-ietf-lake-edhoc-latest
draft-ietf-lake-traces-latest

IETF 113, LAKE WG, March 21, 2022

Since IETF 112

- As decided, no new versions submitted
  - Still edhoc-12 and traces-00
- Progress documented on https://github.com/lake-wg/edhoc
- Comments from 5 reviews have been integrated
- Almost all current open issues relate to test vectors

Updates to -edhoc-latest

Main changes

- Section 3.5 updated, new appendix D
  - Distinguish between
    - EDHOC protocol (PoP, transfer credential info)
    - other authentication related operations (identity verification, chain validation, etc.)
      - Previously in 3.5.1, now in appendix D
- Section 3.8 updated, new appendix E
  - ead_value is now byte string (was any)
  - EAD is considered unprotected by EDHOC
  - Examples of EAD use in appendix E
- Update to processing (section 5) related to changes in 3.5 & 3.8
  - Make ID_CRED and EAD (if present) available to the application for authentication- and EAD processing
- Compliance requirements (next slide)

Update to 7. Compliance Requirements

- General precondition:
- “In the absence of an application profile specifying otherwise:“
- “Implementations MUST support cipher suite 2 and 3 “
  - P-256 / ES256
- “MUST be able to parse padded messages“
  - MAY support when sending, MUST support when receiving
  - plaintext = (? PAD, …)
    - PAD = 1*true is padding that may be used to hide the length of the unpadded plaintext

Rename:

“applicability template”
→
“application profile”

Other updates

- Updated error handling
  - Clarified normative text
  - Renamed error code 1 “Unspecified” →”Unspecified Error”
  - Clarifications of cipher suite negotiation
- Change of exporter label to not exceed 20 characters requiring an additional hash iteration
  - “OSCORE_Master_Secret” → “OSCORE_Secret”
  - “OSCORE_Master_Salt” → “OSCORE_Salt”
- An endpoint MAY choose to select only a specific range of connection identifiers, e.g., only int or only bstr.
- Updated security considerations
- Updated IANA considerations
- Clarifications

-traces-latest

Content of -traces

- Purpose:
  - Help implementers with detailed printouts and intermediate steps
  - Not a complete set of test vectors (see next slide)
- Version -00:
  - Method 3 (static DH), cipher suite 0 (X25519), RPK encoded as CCS identified by ‘kid’ (key id)
  - Method 0 (signature), cipher suite 0 (EdDSA), dummy X.509 identified by ‘x5t’ (hash of cert)
- Updates github master branch:
  - Method 3 (static DH), cipher suite **2** (**P-256**), RPK encoded as CCS identified by ‘kid’ (key id)
    - Cipher suite negotiation (error with SUITES_R)
    - Explicit ‘y’ coordinate of public keys
  - Method 0 (signature), cipher suite 0 (EdDSA), **real** X.509 identified by ‘x5t’ (hash of cert)
  - Reversed order of the two traces

Test vectors in general

- Traces generated from code by John and Marek
- More test vectors available in lake-wg/edhoc github repo
  - Need for more structure (as of pre-Hackathon)

< input from Hackathon >

Next steps

- Submit edhoc-13
- Address review comments
- WGLC?

- Submit traces-01
- Review?

- Progress test vectors