

A full-page background image showing a sunset over a body of water. The sun is a bright orange circle on the horizon, with its light reflecting on the water's surface. The sky is filled with soft, orange and yellow clouds. In the distance, there are dark silhouettes of land or islands. The overall mood is calm and serene.

Open Issues & Next Steps

IETF 108, LAKE WG, July 31, 2020

Open Issues

- LAKE repo
 - <https://github.com/lake-wg/edhoc>

Self-contained specification (#1)

- Martin Disch: "expanding on the COSE constructs would be helpful"
- Current draft:
 - Appendix A.2. "COSE" lists the COSE constructs used
- Action: Provide more details without duplicating specification

Ciphersuites requiring multiple SHA (#2)

- Comment by Rene Struik: "why enforcing both SHA512 and SHA256 at the same time"
- Current draft:
 - Ciphersuite 0 and 1 includes Ed25519 which specifies SHA512.
 - Ciphersuite 0 and 1 additionally requires SHA256.

```
0.(AES-CCM-16-64-128, SHA-256, X25519, EdDSA, Ed25519, AES-CCM-16-64-128, SHA-256)
1.(AES-CCM-16-128-128, SHA-256, X25519, EdDSA, Ed25519, AES-CCM-16-64-128, SHA-256)
```

- Options:
 1. No change (require both)
 2. Change hash algorithm to SHA512
 3. Ed25519 with SHA256 ?
 4. ...

Replace PSK ECDHE (#3)

- PSK ECDHE is not in the initial scope
- Specify a non-DH based PSK scheme providing forward security
 - See thread starting with
https://mailarchive.ietf.org/arch/msg/lake/-Fx-NVLrZohQ7p8Wy8VNpsDC_-M/
- Actions:
 - Remove Section 5. "EDHOC Authenticated with Symmetric Keys"
 - Consequential changes
- What kind of practical attacks on IoT settings should the PSK scheme protect against?
 - Assume long-term keys more protected than session keys?
 - Does the attacker have access to all the traffic information? Some IoT traffic is local.
 - Passive or active attacker?
- Other
 - What layer for the PSK scheme, within EDHOC or on top of?
 - Key rotation between "sessions" or within "sessions"?

Next Steps

- Submit new version w/o PSK ECDHE
- Add issues based on the Tamarin modelling by Norrman, Sundararajan and Bruni
 - <https://arxiv.org/abs/2007.11427>
- Migrate relevant issues from old repo
 - <https://github.com/EricssonResearch/EDHOC/issues>
- Fix issues
- More reviews welcome!
- Plan plug test