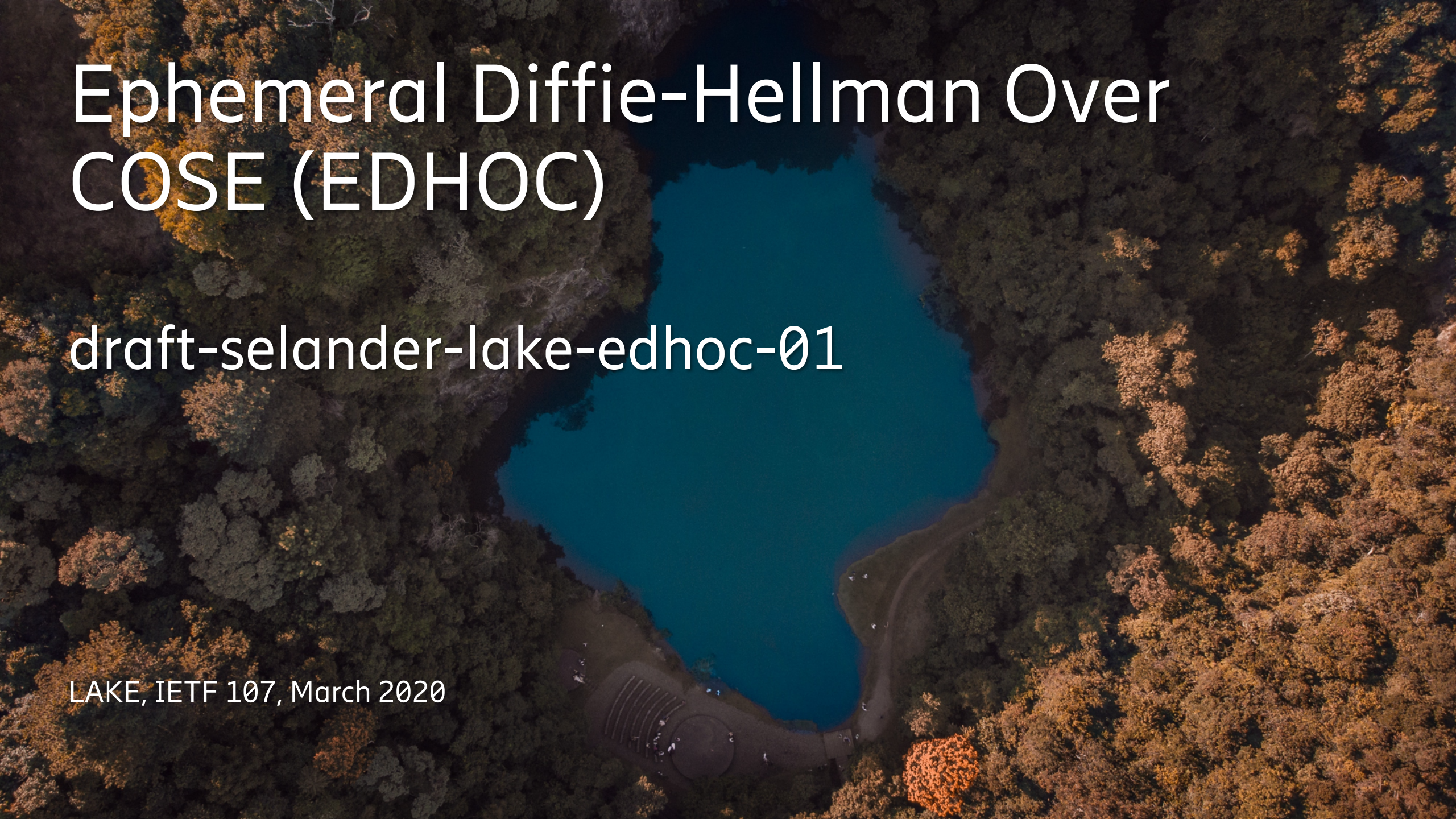

Ephemeral Diffie-Hellman Over COSE (EDHOC)

draft-selander-lake-edhoc-01

LAKE, IETF 107, March 2020

Changes since -01

- The cryptographic algorithms used in EDHOC and OSCORE are now independent of each other.
- New mixed methods for combinations of signature and static DH authentication.
- Serial key derivation for static DH authentication based on a suggestion from Karthik Bhargavan.
- MAC-then-Sign instead of Sign-then-MAC.
- Optimized identifier encoding allows more single byte identifiers.
- IND-CPA encryption for asymmetric message_2.
- Optional integrity protected subject name for RPKs.
- Several clarifications based on suggestions from people implementing and formally verifying EDHOC.
- Large set of test vectors.

Method types

- One LAKE requirement is to support mixed cerificate and RPK modes. To minimize the overhead for such modes, we have merged the signature and static DH modes into an asymmetric mode which allows mixed signature and static DH authentication.
- With the new mixed mode it was more optimal to use a MAC-then-Sign approach instead of Sign-then-MAC. This is also more aligned with the SIGMA paper.

Value	Initiator	Responder	Reference
0	Signature Key	Signature Key	[[this document]]
1	Signature Key	Static DH Key	[[this document]]
2	Static DH Key	Signature Key	[[this document]]
3	Static DH Key	Static DH Key	[[this document]]
4	PSK	PSK	[[this document]]

Figure 10: Method Types

Mixed Asymmetric Methods

- Based on method (0, 1, 2, or 3), the Singature_or_MAC fields contains a Signature or a MAC calculated with an ephemeral-static shared secret (G_RX or G_IY).
  - Some tradeoffs between different security properties and performance.
- As disucssed in the SIGMA paper, the second message only requires IND-CPA encryption.

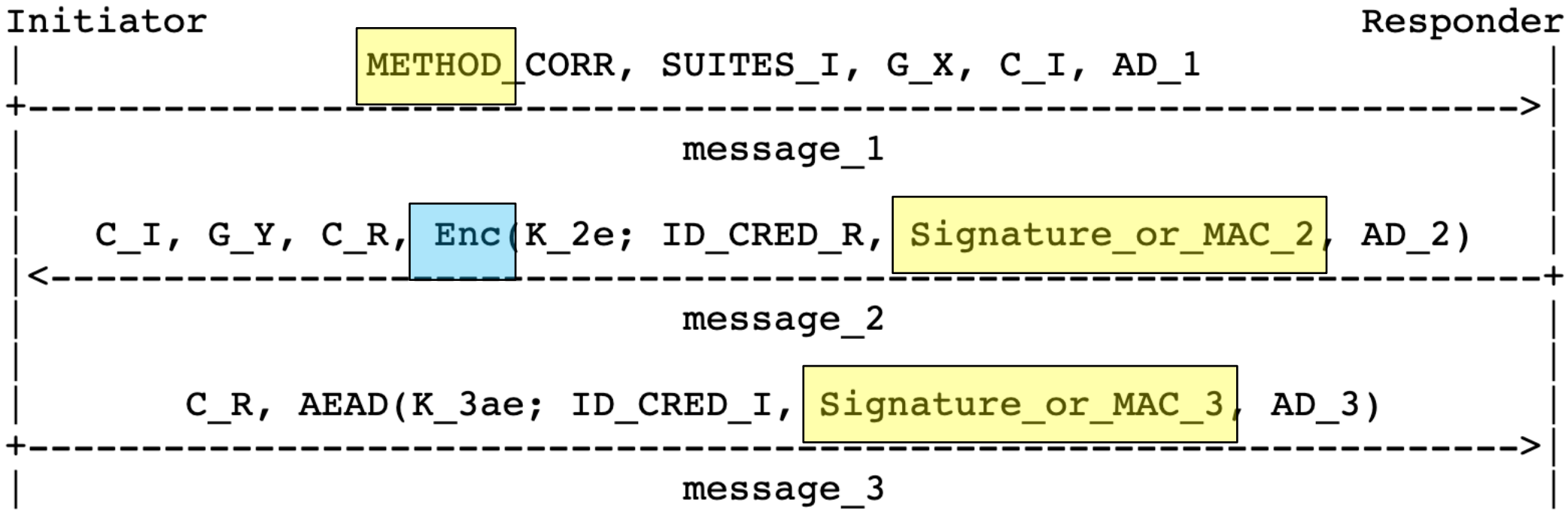

Figure 4: Overview of EDHOC with asymmetric key authentication.

Message sizes

- A few more bytes can be saved by not sending known field lengths.
- EDHOC will be able to do PSK or RPK authentication with ECDHE over 3 unfragmented frames in 5-hop 6TiSCH (45 bytes CoAP payload) and 51 byte LoRaWAN (51 bytes - SCHC header). This is optimal.

	PSK+ECDHE	RPK+ECDHE	x5t+ECDHE	x5chain+ECDHE
message_1	38	37	37	37
message_2	44	46	117	110 + Certificate
message_3	10	20	91	84 + Certificate
Total	92	103	245	231 + Certificates

Figure 1: Typical message sizes in bytes