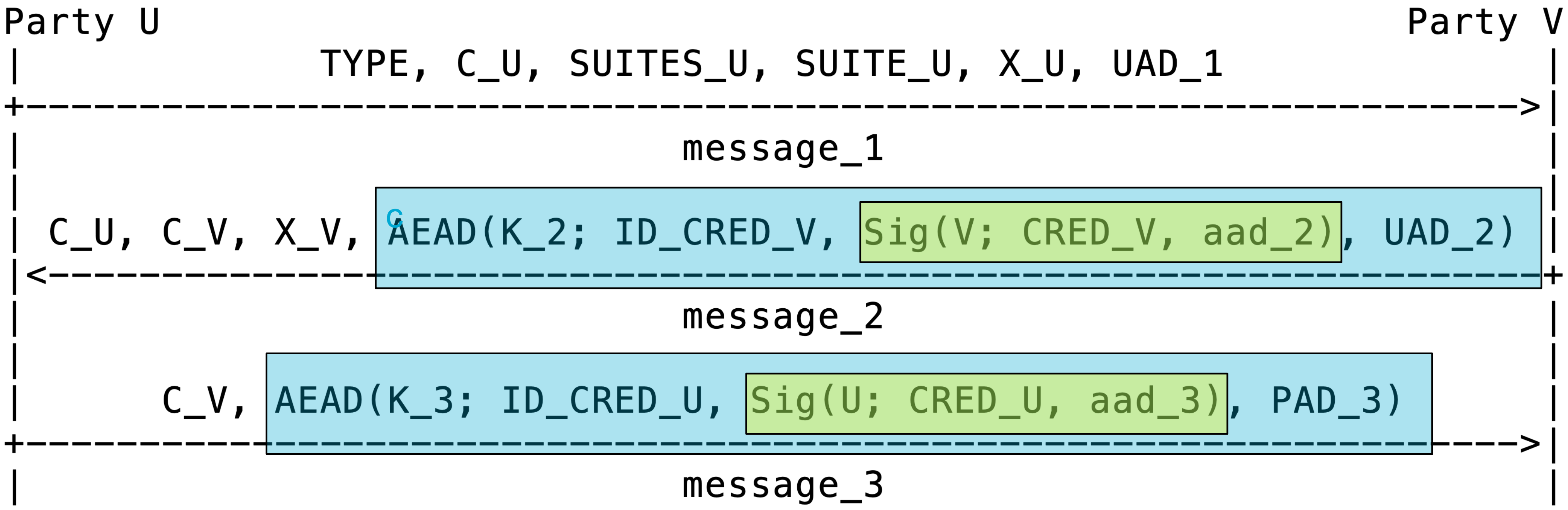
# Ephemeral Diffie-Hellman Over COSE (EDHOC)

## draft-selander-ace-cose-ecdhe-13

IETF 105, LAKE BoF, July 22, 2019
Göran Selander et al.

# EDHOC overview

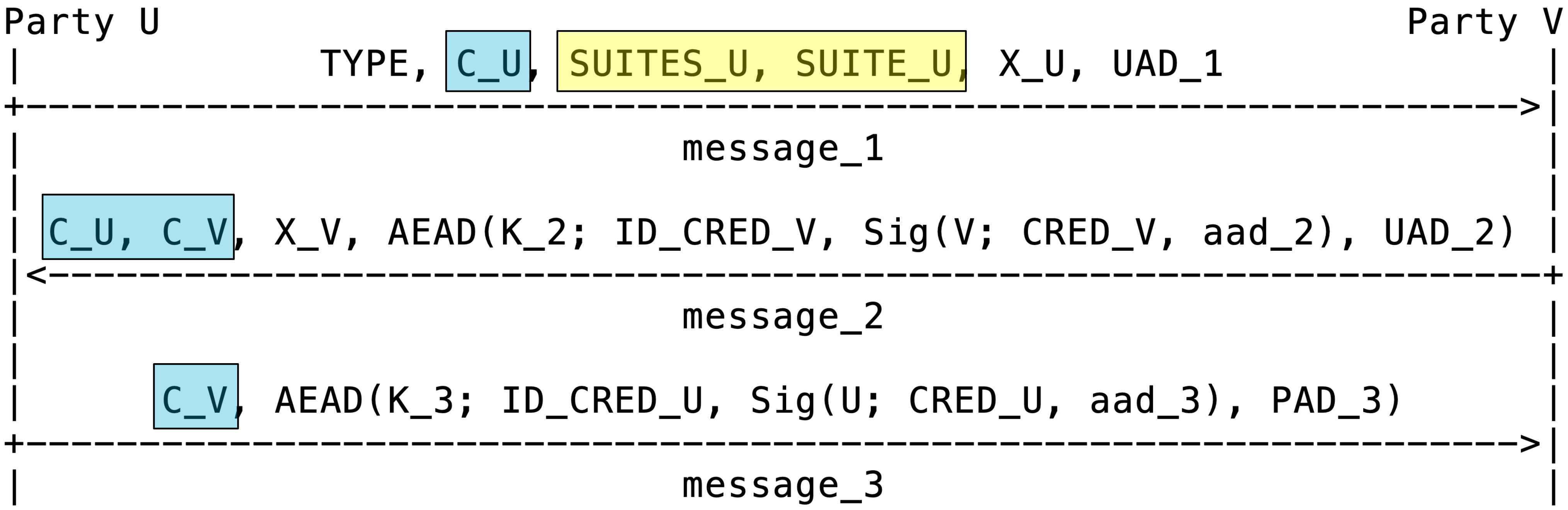
- SIGMA-I based
- Messages are sequences of CBOR elements
- Uses COSE constructs
- Symmetric and asymmetric versions are very similar (+KID, -Sig, ...)



```
Party U                                                    Party V
|         TYPE, C_U, SUITES_U, SUITE_U, X_U, UAD_1                |
+--------------------------------------------------------------->|
|                          message_1                              |
|                                                                 |
| C_U, C_V, X_V, AEAD(K_2; ID_CRED_V, Sig(V; CRED_V, aad_2), UAD_2) |
|<---------------------------------------------------------------+
|                          message_2                              |
|                                                                 |
|     C_V, AEAD(K_3; ID_CRED_U, Sig(U; CRED_U, aad_3), PAD_3)     |
+--------------------------------------------------------------->|
|                          message_3                              |
```

# Suitability for LAKE

- Explicit connection identifiers can give arbitrarily short OSCORE Sender Ids
- Simple negotiation of ciphersuites: supports negotiation of COSE algorithms for OSCORE
- Same COSE algorithms and IANA registries as OSCORE and Group OSCORE
- Small code footprint: reuses CBOR, COSE encrypt and sign structures, COSE HKDF Context



```
Party U                                                        Party V
|             TYPE, C_U, SUITES_U, SUITE_U, X_U, UAD_1                |
+------------------------------------------------------------------->|
|                             message_1                               |
|                                                                     |
| C_U, C_V, X_V, AEAD(K_2; ID_CRED_V, Sig(V; CRED_V, aad_2), UAD_2) |
|<-------------------------------------------------------------------+
|                             message_2                               |
|                                                                     |
|      C_V, AEAD(K_3; ID_CRED_U, Sig(U; CRED_U, aad_3), PAD_3)       |
+------------------------------------------------------------------->|
|                             message_3                               |
```

# Other constrained features

- Supports COSE constructs especially suitable for IoT
- RPK may be identified with a COSE kid
- Certificates are identified with x5t, x5u, x5chain, x5bag (draft-ietf-cose-x509)
- Certificates/RPK (CRED_U and CRED_V) need not be transported in message

```
Party U                                                       Party V
|             TYPE, C_U, SUITES_U, SUITE_U, X_U, UAD_1               |
+------------------------------------------------------------------>|
|                             message_1                             |
|                                                                   |
| C_U, C_V, X_V, AEAD(K_2; ID_CRED_V, Sig(V; CRED_V, aad_2), UAD_2) |
|<------------------------------------------------------------------+
|                             message_2                             |
|                                                                   |
|      C_V, AEAD(K_3; ID_CRED_U, Sig(U; CRED_U, aad_3), PAD_3)      |
+------------------------------------------------------------------>|
|                             message_3                             |
```

# Security

- Main security properties from SIGMA-I:  PFS, mutual authentication, identity protection, KCI …
- Credentials under signature, good to prevent DSKS-type attacks
- Transcript hashes used in key derivation and external_aad
- In case of PSK, session keys are derived from both ECDH Secret and PSK
- Downgrade protection of cipher suite negotiation
- Uses CoAP for reliable ordered transport, handling message duplication, fragmentation, DoS, …

- A number of reviews since `-00` (2016)
- Formal verification by Alessandro Bruni et al. (IT-University of Copenhagen)
- Two reviews by CFRG crypto panel
  - https://mailarchive.ietf.org/arch/msg/cfrg/6WN2C2RYGTIAInE2jIUco6L9pO8
  - https://mailarchive.ietf.org/arch/msg/cfrg/2OY2om1FjhNNBmUzwYJroHv7eWQ
    - The latter provides a good overview
- All review comments have been addressed in later versions of the draft

# Evaluation of EDHOC-13 against benchmarks B1-B3

| EDHOC-13 PSK ECHDE | B1 (bytes) | B2 (packets) | B3 (frames) |
|---|---|---|---|
| message_1 | 40 | 1 | 1 |
| message_2 | 45 | 1 | 1 |
| message_3 | 11 | 1 | 1 |
| **Total** | **96** | **3** | **3** |
| | | Optimal | Optimal |

| EDHOC-13 RPK ECHDE | B1 (bytes) | B2 (packets) | B3 (frames) |
|---|---|---|---|
| message_1 | 38 | 1 | 1 |
| message_2 | 114 | 3 | 2 |
| message_3 | 80 | 2 | 2 |
| **Total** | **232** | **6** | **5** |
| | | Optimal | Optimal |

| ”SIGMA-I skeleton” RPK ECHDE | B1 (bytes) | B2 (packets) | B3 (frames) |
|---|---|---|---|
| message_1 | 32 | 1 | 1 |
| message_2 | 32+64+8=104 | 3 | 2 |
| message_3 | 64+8=72 | 2 | 2 |
| **Total** | **208** | **6** | **5** |

Common crypto object sizes

— Ephemeral DH-key: 32 bytes

— EC signature: 64 bytes

— AES-CCM with MAC truncated to 8 bytes

# EDHOC complies with the LAKE requirements

- The AKE shall support PSK, RPK, and certificate based authentication (A1)
- The AKE shall support negotiation of algorithms for OSCORE and AKE, and support the same transport as OSCORE (C1,O2)
- After the AKE protocol run, the peers shall agree on OSCORE Master Secret with PFS and good amount of randomness, OSCORE Sender IDs (potentially short), and COSE algorithms to use (O1)
- The AKE shall reuse CBOR, CoAP and COSE primitives and algorithms for low code complexity of a combined OSCORE and AKE implementation (L1)
- The AKE shall be 3-pass/1 RTT,  the messages as small as reasonably achievable and fit into as few LoRaWAN packets and 6TiSCH frames as possible (L2,B1,B2,B3)
- New proposed requirement: mixed public key authentication (A2)