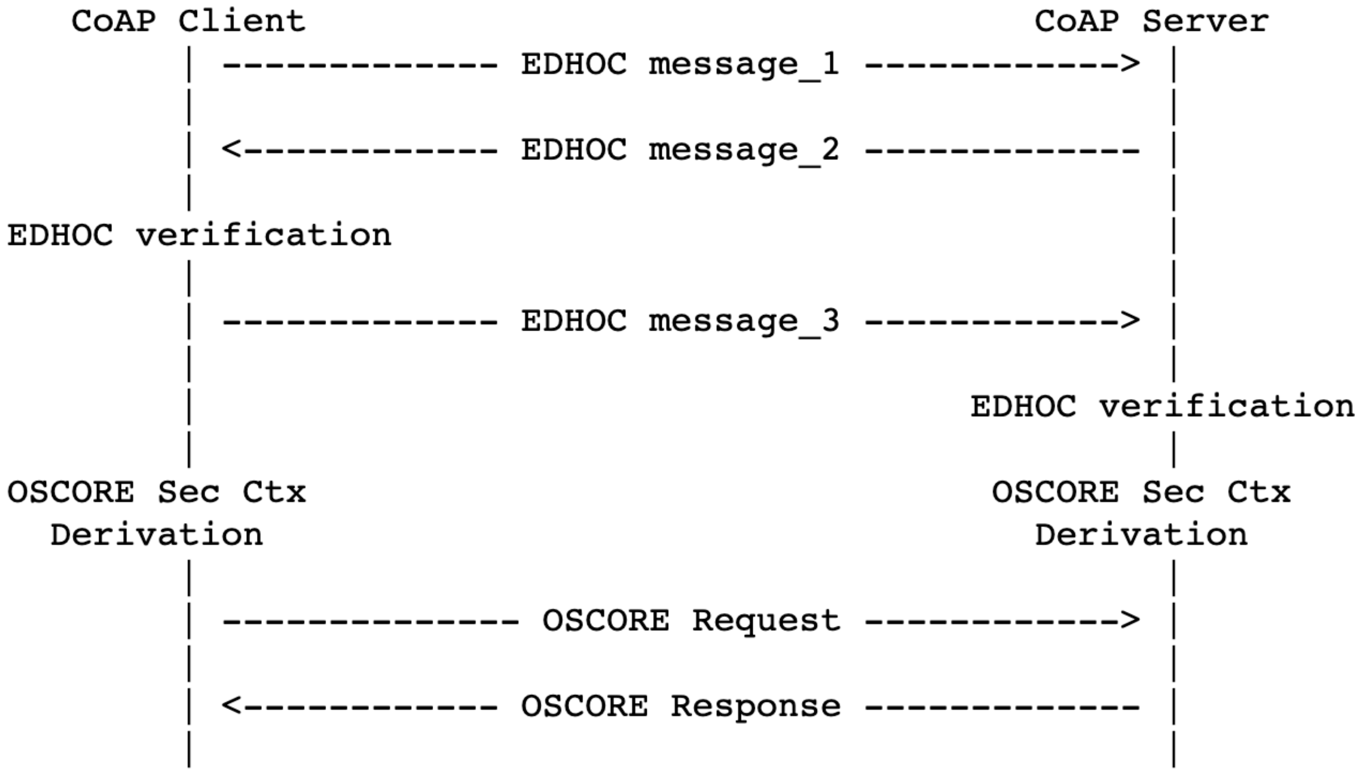
Combining EDHOC and OSCORE draft-palombini-core-oscore-edhoc-01

Francesca Palombini,
Marco Tiloca,
Rikard Höglund,
Stefan Hristozov,
Göran Selander

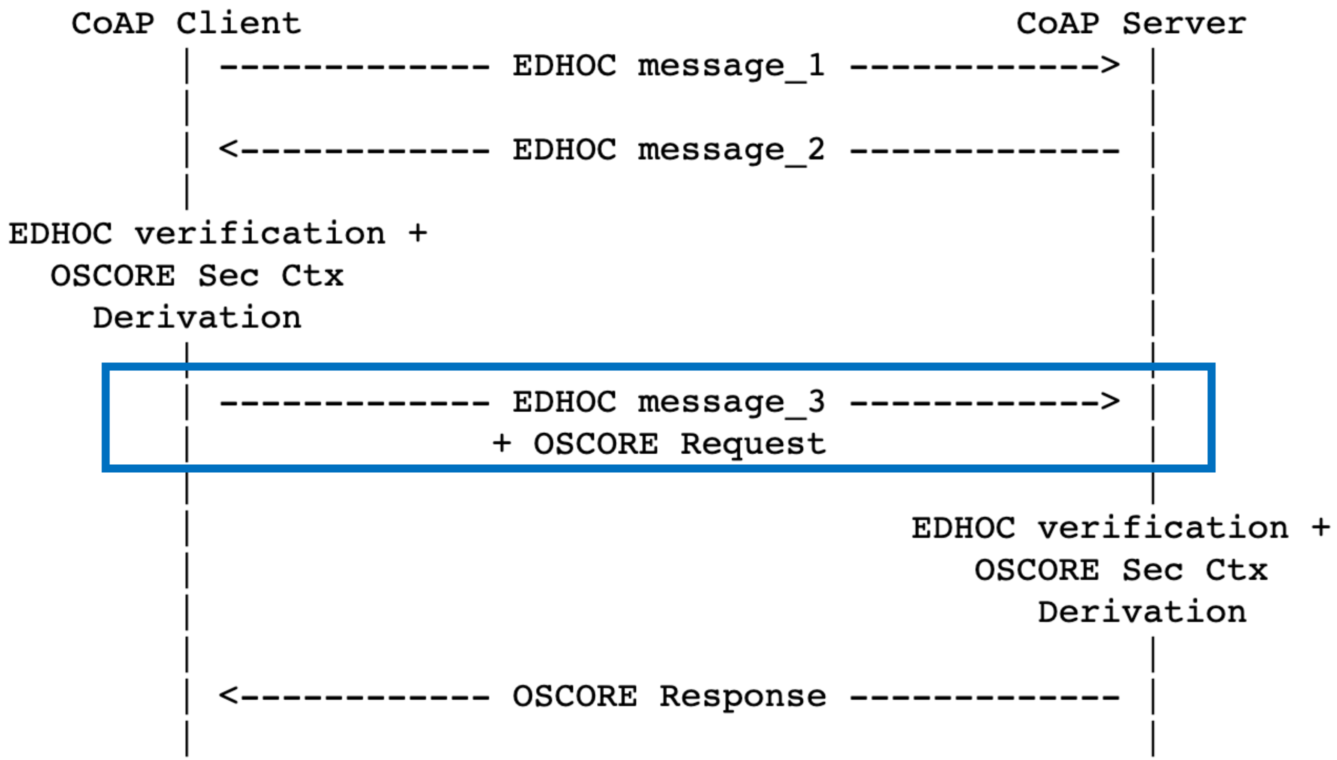
EDHOC then OSCORE over CoAP



```
   CoAP Client                                       CoAP Server
        | ------------- EDHOC message_1 ------------> |
        |                                             |
        | <------------ EDHOC message_2 ------------- |
        |                                             |
EDHOC verification                                    |
        |                                             |
        | ------------- EDHOC message_3 ------------> |
        |                                             |
        |                                    EDHOC verification
        |                                             |
OSCORE Sec Ctx                                  OSCORE Sec Ctx
  Derivation                                      Derivation
        |                                             |
        | -------------- OSCORE Request ------------> |
        |                                             |
        | <------------ OSCORE Response ------------- |
        |                                             |
```

Figure 1: EDHOC and OSCORE run sequentially

Optimized – EDHOC message 3 + OSCORE Req



```
   CoAP Client                                        CoAP Server
        | ------------- EDHOC message_1 ------------> |
        |                                             |
        | <------------ EDHOC message_2 ------------- |
        |                                             |
EDHOC verification +                                  |
  OSCORE Sec Ctx                                      |
    Derivation                                        |
        |                                             |
        | ------------- EDHOC message_3 ------------> |
        |              + OSCORE Request               |
        |                                             |
        |                                  EDHOC verification +
        |                                     OSCORE Sec Ctx
        |                                       Derivation
        |                                             |
        | <------------ OSCORE Response ------------- |
        |                                             |
```

Figure 2: EDHOC and OSCORE combined

How to send those 2 messages together?

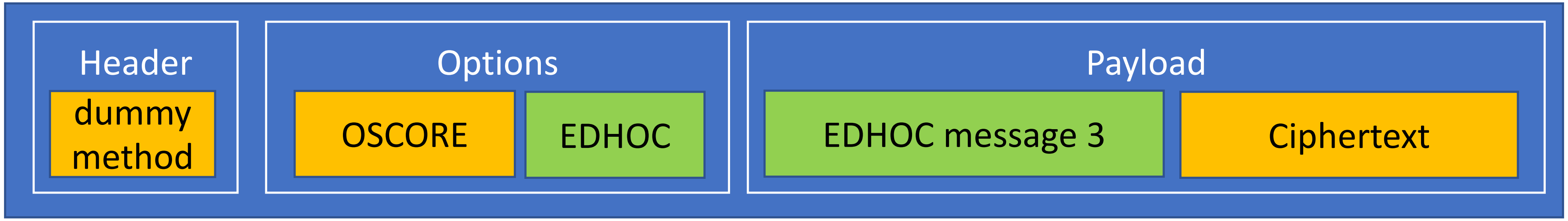
- **Send EDHOC in OSCORE 🡐 preferred option from IETF 108**
    1. Signalling in a new CoAP option
    2. Signalling in the OSCORE option (use a bit in the flagbits)

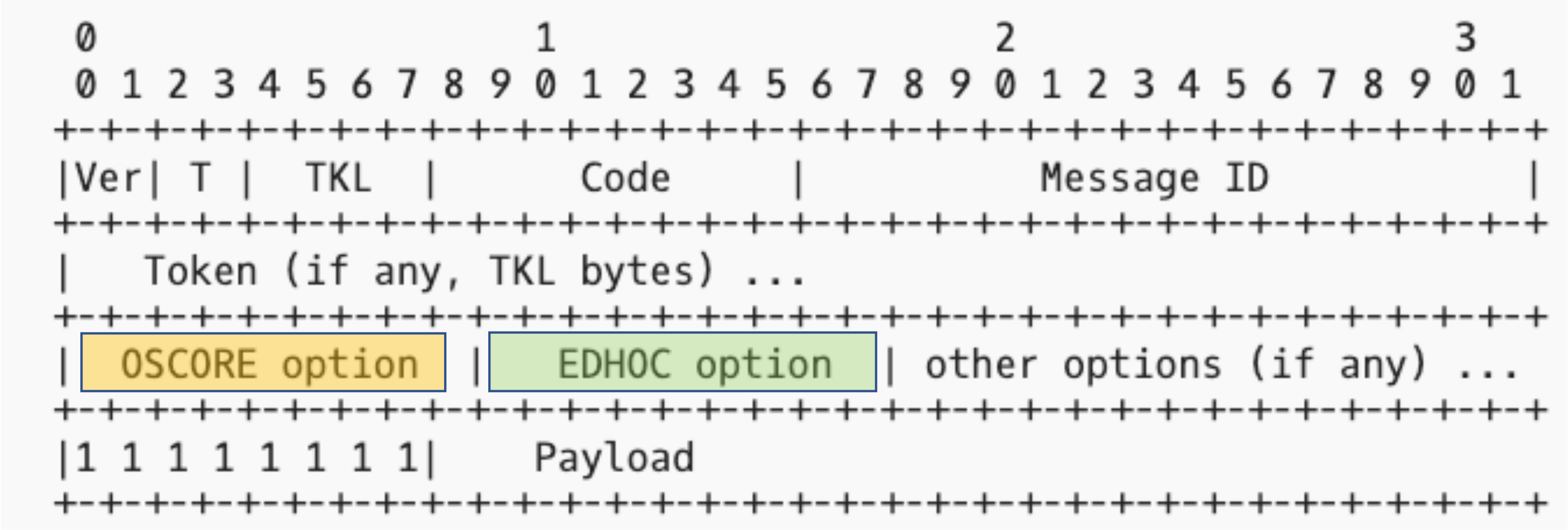
- ~~**Send OSCORE in EDHOC**~~

EDHOC in OSCORE – Signalling in new option

CoAP message

1.

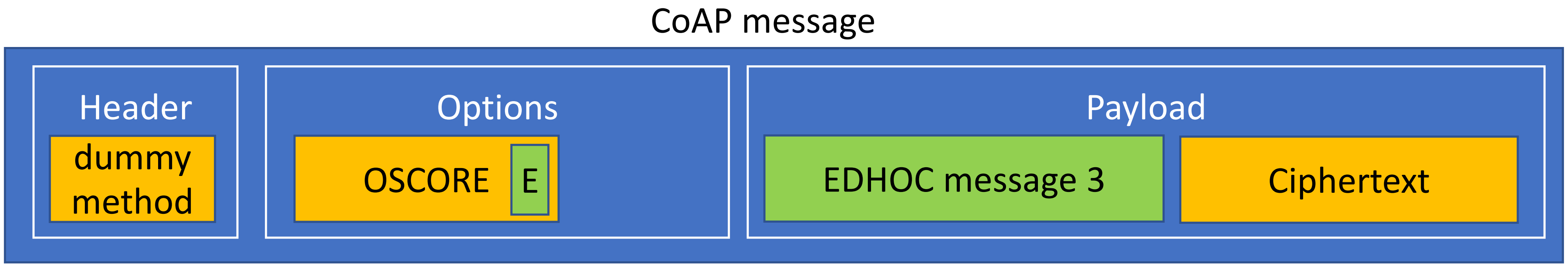


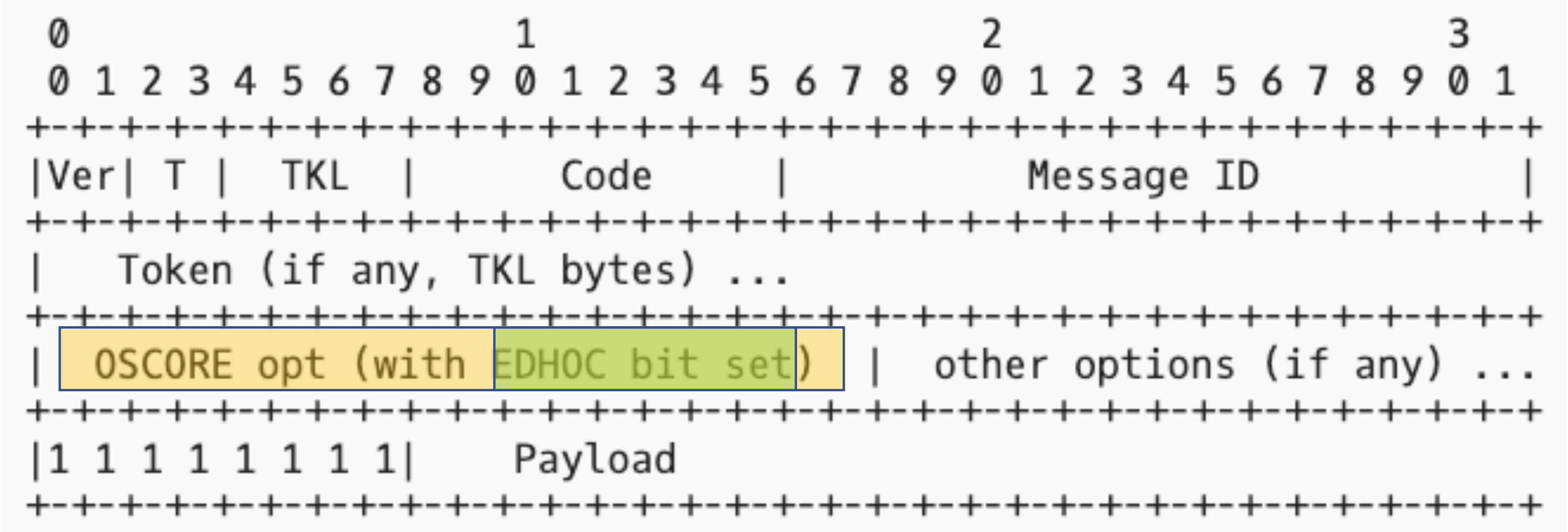


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Ver| T |  TKL  |      Code     |          Message ID           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Token (if any, TKL bytes) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  OSCORE option  |  EDHOC option  | other options (if any) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1 1 1 1 1 1 1 1|    Payload
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

EDHOC in OSCORE – Signalling in OSCORE

2.





```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Ver| T |  TKL  |      Code     |          Message ID           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Token (if any, TKL bytes) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  OSCORE opt (with EDHOC bit set)  |  other options (if any) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1 1 1 1 1 1 1 1|    Payload
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Comparison

(based on Appendix C.4 of RFC8613 and Appendix B.2 of EDHOC test vectors)

1. 58 bytes in total (empty option)
2. 57 bytes in total (using bit 1 in the first byte of OSCORE Flag Byte)
    - 58 if we need to expand the flag byte, and use bit >7

Way Forward

- Pick one
- Get feedback + reviews
- WG adoption?