Combining EDHOC and OSCORE
draft-palombini-core-oscore-edhoc-00

Francesca Palombini,
Marco Tiloca,
Rikard Höglund,
Stefan Hristozov,
Göran Selander
How to run EDHOC and OSCORE over CoAP?

Figure 1: EDHOC and OSCORE run sequentially
Can we optimize this 3 round-trips exchange?

Figure 1: EDHOC and OSCORE run sequentially
Can we optimize? Yes!

Figure 2: EDHOC and OSCORE combined
How to send those 2 messages together?

2 options:

• Send EDHOC in OSCORE
• Send OSCORE in EDHOC
EDHOC in OSCORE or OSCORE in EDHOC?

**EDHOC in OSCORE**

- **Header**: dummy method
- **Options**: OSCORE
- **Payload**: EDHOC message 3

**OSCORE in EDHOC**

- **Header**: POST
- **Options**: Uri-path = /edhoc
- **Payload**: EDHOC message 3, OSCORE option, Ciphertext
How to send those 2 messages together?

4 sub-options:

• **Send EDHOC in OSCORE**
  1. Signalling in a new CoAP option
  2. Signalling in the OSCORE option (use a bit in the flagbits)

• **Send OSCORE in EDHOC**
  3. Signalling in a new CoAP option (with processing different from 1.)
  4. Signalling based on the number of elements in CoAP payload (and possibly a specific Content-Format)
EDHOC in OSCORE – Signalling options

1. 
**CoAP message**

- **Header**
  - dummy method

- **Options**
  - OSCORE
  - EDHOC

- **Payload**
  - EDHOC message 3
  - Ciphertext

*EDHOC in OSCORE - Signalling in new CoAP option*

2. 
**CoAP message**

- **Header**
  - dummy method

- **Options**
  - OSCORE
  - E

- **Payload**
  - EDHOC message 3
  - Ciphertext

*EDHOC in OSCORE - Signalling in OSCORE option*
OSCORE in EDHOC – Signalling options

3. CoAP message

Header
POST

Options
Uri-Path = /edhoc
EDHOC + OSCORE

Payload
EDHOC message 3
OSCORE option
Ciphertext

OSCORE in EDHOC - Signalling in new CoAP option

4. CoAP message

Header
POST

Options
Uri-Path = /edhoc
C-F = edhoc-oscore

Payload
EDHOC message 3
OSCORE option
Ciphertext

OSCORE in EDHOC - Signalling with new Content-Format
Using multipart-core

4.bis

CoAP message

Header

POST

Options

Uri-Path = /edhoc
C-F = application/multipart-core

Payload

OSCORE in EDHOC - Signalling with multipart-core Content-Format

[ edhoc, , oscore-opt, , oscore, Ciphertext ]

Payload

EDHOC message 3

OSCORE option

[ edhoc, , oscore-new, , oscore, Ciphertext ]

Payload

EDHOC message 3

OSCORE option

Ciphertext
Way Forward

• Get feedback + reviews

• Pick one option and progress it