Using the Extensible Authentication Protocol with Ephemeral Diffie-Hellman over COSE (EDHOC)

Advances and Changes for draft-ietf-emu-eap-edhoc-03

Dan García-Carrillo, University of Oviedo
Rafael Marín-López, University of Murcia
Göran Selander, Ericsson
John Preuß Mattsson, Ericsson
Francisco López Gómez, University of Murcia

IETF 122

Summary

- Quick recap
- Reviews
- Main updates
  - Key Hierarchy
  - Security Considerations
    - Channel Binding
    - Fast reconnect
- Questions

Quick recap

Context

EDHOC [**RFC 9528**] provides a compact and lightweight authenticated Diffie-Hellman key exchange

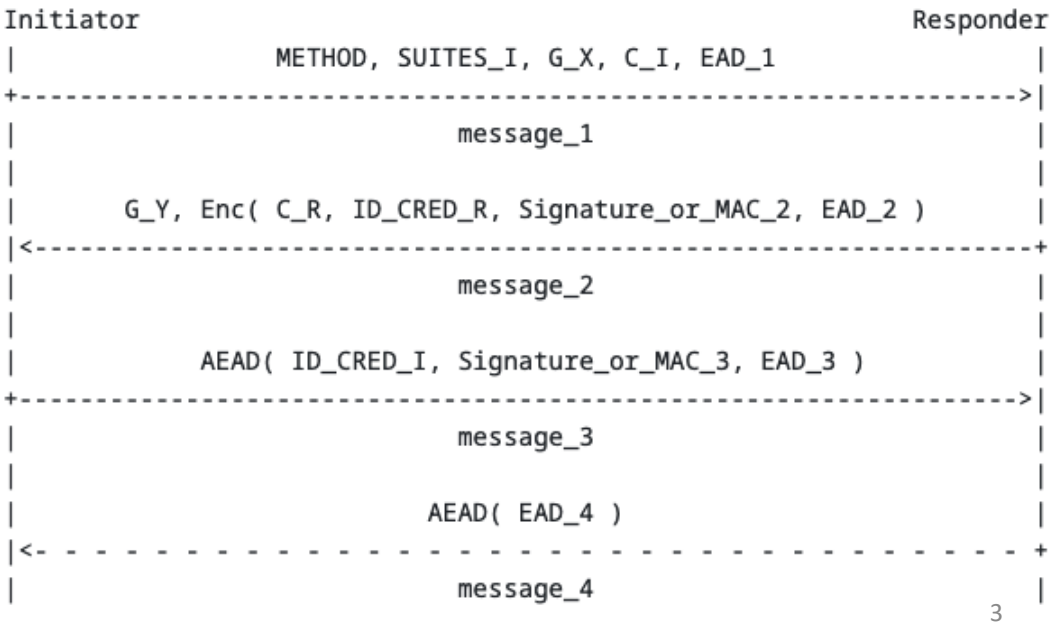
Use of CBOR and COSE

Credentials

Certificates, RPK, and all

credential types for which COSE

header parameters are defined



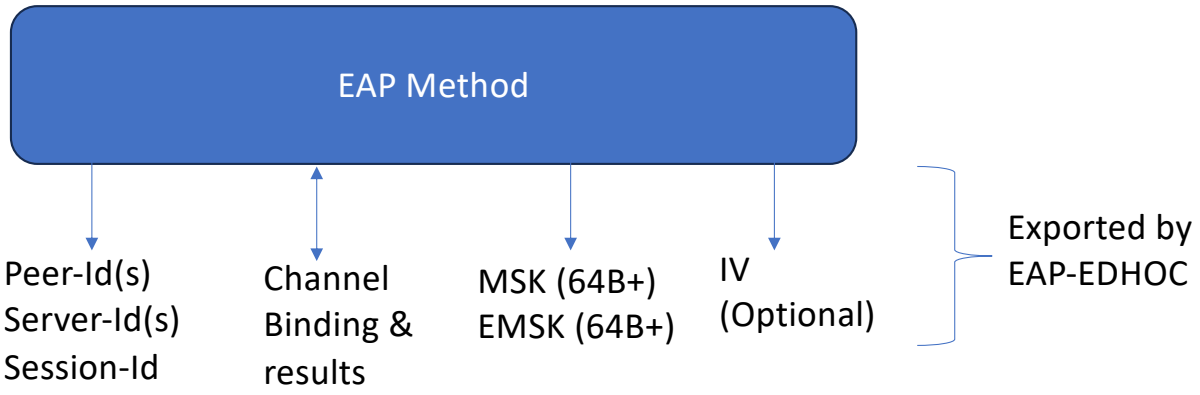
Reviews

Addressed comments from

- **Gabriel Lopez Millan**
- **Francisco Lopez Gomez (from now on co-author)**
- **Josh Howlett**

- **Thank you!**

Key Hierarchy




```
MSK          =  EDHOC_Exporter(TBD2, << Type >>, 64)
EMSK         =  EDHOC_Exporter(TBD3, << Type >>, 64)
Method-Id    =  EDHOC_Exporter(TBD4, << Type >>, 64)
Session-Id   =  Type || Method-Id
Peer-Id      =  ID_CRED_I
Server-Id    =  ID_CRED_R
```

ID_CRED_I and ID_CRED_R are used to identify the credentials of I and R

Security Considerations

Most security principles are inherited using EDHOC and its features

- Auth Principle
- Cipher suite Negotiation
- Mutual Authentication
- Integrity Protection
- Replay Protection
- Confidentiality
- Dictionary attack protection
- Session Independence

Other security claims

- Cryptographic strength and Forward secrecy
- Identity protection

Claim	
Auth. principle:	Certificates, CWTs and all credential types for which COSE header parameters are defined (1)
Ciphersuite negotiation:	Yes (2)
Mutual authentication:	Yes (3)
Integrity protection:	Yes (4)
Replay protection:	Yes (5)
Confidentiality:	Yes (6)
Key derivation:	Yes (7)
Key strength:	The specified cryptosuites provide key strength of at least 128 bits.
Dictionary attack prot.:	Yes (8)
Fast reconnect:	No
Crypt. binding:	N/A
Session independence:	Yes (9)
Fragmentation:	Yes (Section 3.1.6)
Channel binding:	Yes (Section 6.1.1: EAD_3 and EAD_4 can be used to convey integrity-protected channel properties, such as network SSID or peer MAC address.)

Security Considerations

Channel Binding

The channel binding protocol defined in [RFC6677] must be transported after keying material has been derived between the endpoints in the EAP communication and before the peer is exposed to potential adverse effects from joining an adversarial network.

Proposal: Use **External Authorization Data (EAD)**
EDHOC allows processing of external authorization data

EAD field: CBOR sequence of one or more EAD items
EAD item: A CBOR sequence of ead_label and optional ead_value

EAD_3 and EAD_4 fields, in EDHOC message_3 and message_4, respectively, are perfect candidates for this purpose.

New EAD ítems

ead_label = TBD5
ead_value is a CBOR byte string.

Claim	
Auth. principle:	Certificates, CWTs and all credential types for which COSE header parameters are defined (1)
Ciphersuite negotiation:	Yes (2)
Mutual authentication:	Yes (3)
Integrity protection:	Yes (4)
Replay protection:	Yes (5)
Confidentiality:	Yes (6)
Key derivation:	Yes (7)
Key strength:	The specified cryptosuites provide key strength of at least 128 bits.
Dictionary attack prot.:	Yes (8)
Fast reconnect:	No
Crypt. binding:	N/A
Session independence:	Yes (9)
Fragmentation:	Yes (Section 3.1.6)
Channel binding:	Yes (Section 6.1.1: EAD_3 and EAD_4 can be used to convey integrity-protected channel properties, such as network SSID or peer MAC address.)

Security Considerations

Fast reconnect

- Currently set to NO
- There is a possibility of supporting this with
  EDHOC PSK authentication -- draft-ietf-lake-edhoc-psk

Issue

- Dependency that will take time to be standardized

Proposal

- Not include it now, keep processing it and propose update to the specification

Opinions?

Claim	
Auth. principle:	Certificates, CWTs and all credential types for which COSE header parameters are defined (1)
Ciphersuite negotiation:	Yes (2)
Mutual authentication:	Yes (3)
Integrity protection:	Yes (4)
Replay protection:	Yes (5)
Confidentiality:	Yes (6)
Key derivation:	Yes (7)
Key strength:	The specified cryptosuites provide key strength of at least 128 bits.
Dictionary attack prot.:	Yes (8)
Fast reconnect:	No
Crypt. binding:	N/A
Session independence:	Yes (9)
Fragmentation:	Yes (Section 3.1.6)
Channel binding:	Yes (Section 6.1.1: EAD_3 and EAD_4 can be used to convey integrity-protected channel properties, such as network SSID or peer MAC address.)

Questions

THANK YOU