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

draft-ingles-eap-edhoc-04

Eduardo Inglés Sanchez, University of Murcia
Dan Garcia-Carrillo, University of Oviedo
Rafael Marín-López, University of Murcia
Göran Selander, Ericsson
John Preuß Mattsson, Ericsson (presenter)

IETF 116, EMU WG, March 27th, 2023

Summary -04

- Background
- Recap EDHOC Exchange
- Benefits of EDHOC as EAP method
- Added Security Considerations
- Status of the draft

Background

- EAP suitable for wide range of deployments
- Fundamental part of 5G authentication
    - EAP can be used in both primary and secondary authentication
- Primary authentication = access authentication
    - any EAP method can be used in private networks, e.g. factory
- Secondary authentication = user connection
    - any EAP method can be used
- A lightweight EAP method is missing for constrained IoT

Benefits of EDHOC as EAP method

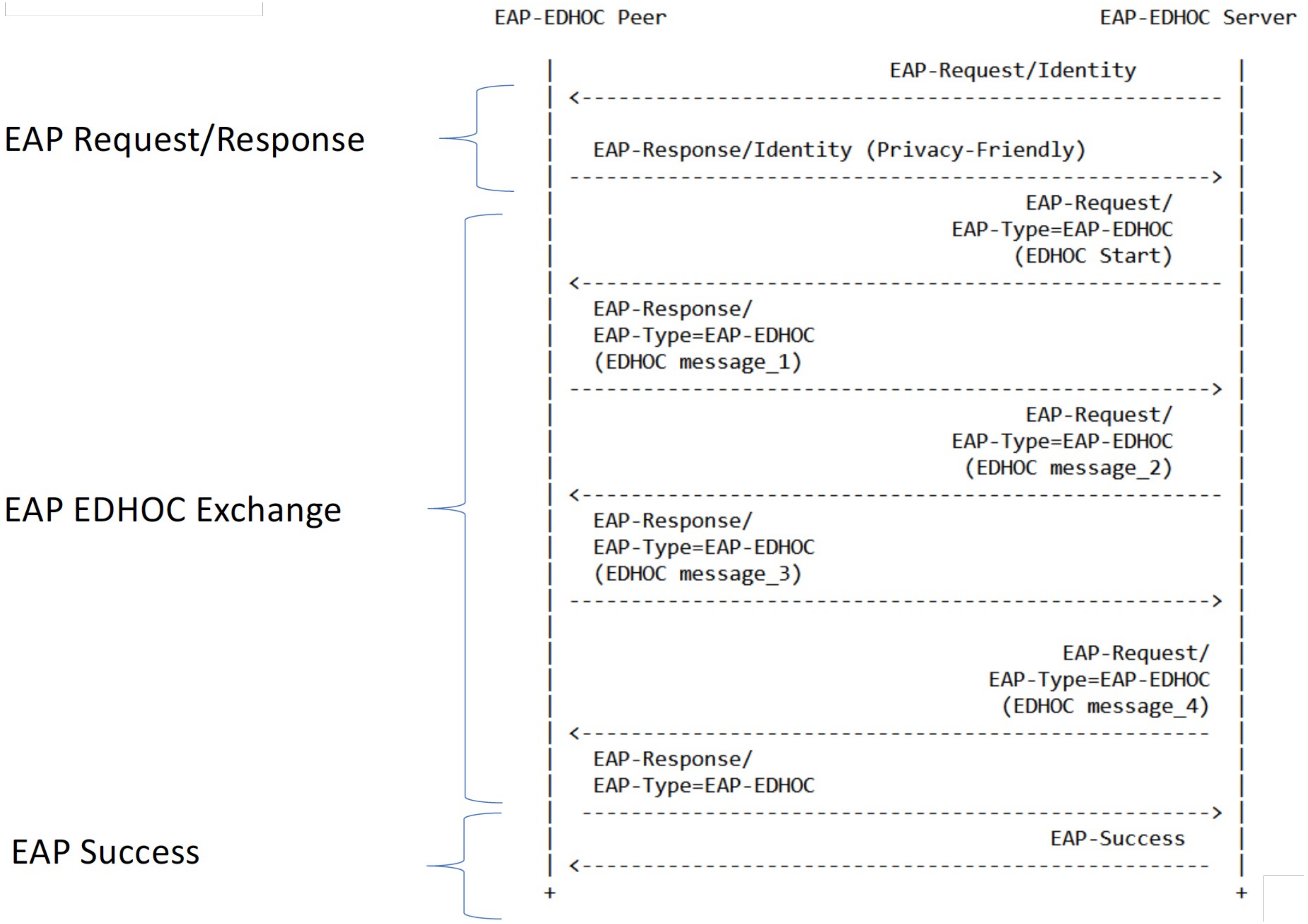
- Lightweight Authenticated Key Exchange
  - Compact message encoding

- Short exchange
  - 4th message including success indication

- Low overhead use of certificates and raw public keys
  - Support for CBOR encoded credentials (CWT, C509, …)
  - Support for credentials by reference (kid, x5t, …)

EAP-EDHOC exchange

- Message flow and properties similar to EAP-TLS.
- Much smaller messages sizes for RPK (100 bytes instead of 800 bytes).
- Mandatory ECDHE and identity protection



EAP Request/Response

EAP EDHOC Exchange

EAP Success

```
EAP-EDHOC Peer                                          EAP-EDHOC Server

  |                           EAP-Request/Identity                     |
  | <------------------------------------------------------------------ |
  |                                                                    |
  |   EAP-Response/Identity (Privacy-Friendly)                         |
  | ------------------------------------------------------------------> |
  |                                           EAP-Request/             |
  |                                      EAP-Type=EAP-EDHOC            |
  |                                            (EDHOC Start)           |
  | <------------------------------------------------------------------ |
  |   EAP-Response/                                                    |
  |   EAP-Type=EAP-EDHOC                                               |
  |   (EDHOC message_1)                                                |
  | ------------------------------------------------------------------> |
  |                                           EAP-Request/             |
  |                                      EAP-Type=EAP-EDHOC            |
  |                                       (EDHOC message_2)            |
  | <------------------------------------------------------------------ |
  |   EAP-Response/                                                    |
  |   EAP-Type=EAP-EDHOC                                               |
  |   (EDHOC message_3)                                                |
  | ------------------------------------------------------------------> |
  |                                                                    |
  |                                              EAP-Request/          |
  |                                         EAP-Type=EAP-EDHOC         |
  |                                          (EDHOC message_4)         |
  | <----------------------------------------------------------------- |
  |   EAP-Response/                                                    |
  |   EAP-Type=EAP-EDHOC                                               |
  |  ----------------------------------------------------------------> |
  |                                               EAP-Success          |
  | <----------------------------------------------------------------- |
  +                                                                    +
```

Added Security Considerations

- EAP-EDHOC inherits the security properties of EDHOC

1. **Mutual authentication**: The initiator and responder authenticate each other through the EDHOC exchange.

2. **Forward secrecy**: Only ephemeral Diffie-Hellman methods are supported by EDHOC, which ensures that the compromise of one session key does not also compromise earlier sessions' keys.

3. **Identity protection**: EDHOC secures the Responder's credential identifier against passive attacks and the Initiator's credential identifier against active attacks. An active attacker can get the credential identifier of the Responder by eavesdropping on the destination address used for transporting message_1 and then sending its own message_1 to the same address.

4. **Cipher suite negotiation**: The Initiator's list of supported cipher suites and order of preference is fixed and the selected cipher suite is the first cipher suite that the Responder supports.

5. **Integrity protection**: EDHOC integrity protects all message content using transcript hashes for key derivation and as additional authenticated data, including, e.g., method type, ciphersuites, and external authorization data.

Possible additions

- Resumption of EAP-EDHOC
  - Explore EDHOC rekey design and use cases
  - Started thread in mailing list
    - https://mailarchive.ietf.org/arch/msg/emu/ymSr0nFt183n7HbBfjHJl6sGJZw

Status of the draft

- EDHOC is mature
    - Any changes expected to be minor, not affecting the purpose of EAP-EDHOC
- This draft ready for implementation & interop testing
    - Implementation wise we are working on different fronts
        - Exploring hostapd
        - EAP implementation in freeradius
        - uedhoc-uoscore implementation for the actual EDHOC implementation inside EDHOC
- Ready for adoption?

Thank you!