Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: EDHOC as KMP for 802.15.9
Date Submitted: 14 May, 2024
Source: Göran Selander, Ericsson, goran.selander@ericsson.com

Abstract: EDHOC is a new lightweight security handshake protocol standardized by the IETF (RFC 9528). EDHOC enables a low complex implementation with few and short messages using generic encoding (CBOR) and security processing (COSE) which makes it suitable for low-cost / low-power deployments, in particular for establishing shared secret keys for 802.15.4 links. This presentation gives a background of lightweight security work in the IETF with focus on EDHOC.

Purpose: Specify EDHOC as a new KMP for 802.15.9

Notice: This document has been prepared to assist the IEEE Std 802.15.9. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

EDHOC as KMP for 802.15.9

IEEE 802 Wireless

IG Crypto

14 May, 2024

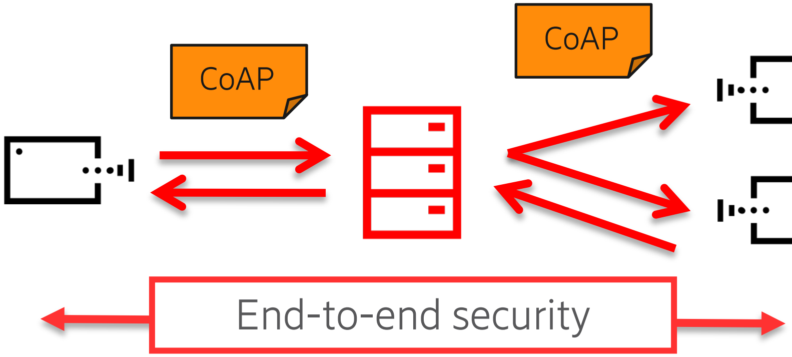
IETF Lightweight Security Background

- The IETF has developed lightweight protocols and enablers suitable for constrained environments, e.g. 6LoWPAN, 6TiSCH, CBOR, CoAP
- This effort also extends to security, for example COSE (RFC 9052), OSCORE (RFC 8613), ACE-OAuth (RFC 9200), EDHOC (RFC 9528)
- Building on lightweight primitives
  - CBOR (Concise Binary Object Representation, RFC 8949) for encoding
  - COSE (CBOR Object Signature and Encryption) for secure encapsulation and extensible identification of algorithms and credentials
  - May use CoAP, but not required in general
- Used for keying link layer
  - CoJP for 6TiSCH (RFC 9031) uses CoAP / OSCORE
    - Extended to EDHOC in draft-ietf-lake-authz
  - Keying of MACsec with EAP-EDHOC (draft-ietf-emu-eap-edhoc)

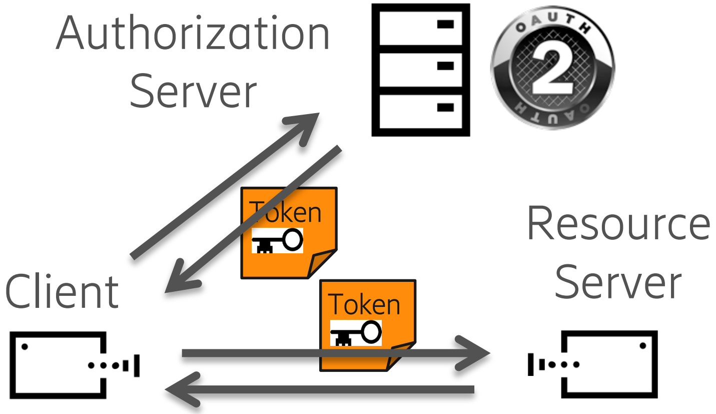
IETF Lightweight Security Examples

OSCORE

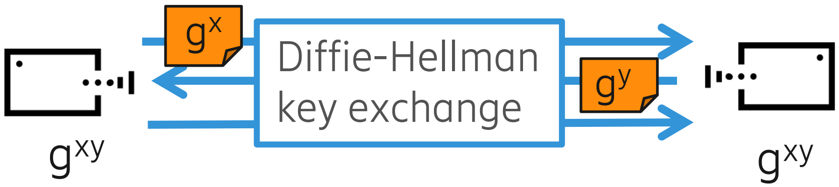
Group OSCORE



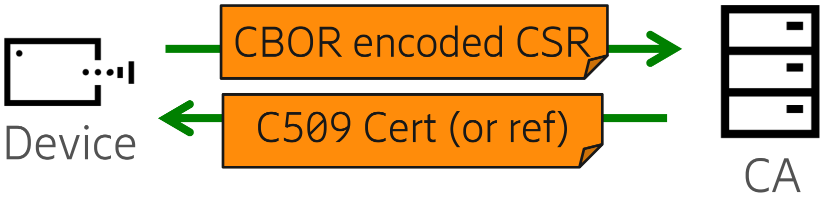
ACE-OAuth



EDHOC



CBOR encoded certificate management



EDHOC authenticates and establishes keys

- **Ephemeral Diffie-Hellman Over COSE – RFC 9528**
  - Lightweight security handshake
  - Authentication and derivation of shared secret keys
- **Lightweight protocol**
  - Lightweight primitives
  - Low message overhead
- **Secure design**
  - Extensive security analysis
- **Benchmark use cases**
  - Parallel handshakes, e.g. network formation
  - Frequent handshakes, e.g. intermittent actuations

EDHOC	Bytes
Message 1	37
Message 2	45
Message 3	19
Total	101

Example
Message sizes of an EDHOC protocol session

Keying 802.15.4 with EDHOC

- EDHOC is a lightweight authentication and key establishment protocol matching 802.15.4 objectives
- EDHOC builds on lightweight standardized enablers CBOR and COSE enabling code reuse
- Other current work on specifying the use of EDHOC to establish link layer keys
- EDHOC has analogous properties as other KMPs in 802.15.9 allowing a straightforward addition