NEW VERSION -04

- Built on the SIGMA family of key exchange protocols
  - Aligning with state-of-the-art security protocols
  - Has better security properties.
  - IKEv2 and TLS 1.3 are also based on SIGMA.
- 3 messages instead of 2
  - But no extra round-trips. Application data can be sent together with message 3 (similar to TLS 1.3)
- Still implemented using CBOR and COSE
- Still Diffie-Hellman (DH) key exchange protocol with ephemeral keys
THE BASIC SIGMA PROTOCOL

- The parties exchanging messages are called "U" and "V". U and V exchange identities and ephemeral public keys. They compute the shared secret and derive the keying material.

**Figure 1: The basic SIGMA protocol**
THE BASIC SIGMA PROTOCOL

• The parties exchanging messages are called "U" and "V". U and V exchange identities and ephemeral public keys. They compute the shared secret and derive the keying material.
The Basic Sigma Protocol

- The parties exchanging messages are called "U" and "V". U and V exchange identities and ephemeral public keys. They compute the shared secret and derive the keying material.

Figure 1: The basic SIGMA protocol
THE BASIC SIGMA PROTOCOL

- The parties exchanging messages are called "U" and "V". U and V exchange identities and ephemeral public keys. They compute the shared secret and derive the keying material.
THE BASIC SIGMA PROTOCOL

• The parties exchanging messages are called "U" and "V". U and V exchange identities and ephemeral public keys. They compute the shared secret and derive the keying material.

Figure 1: The basic SIGMA protocol
EDHOC

- Based on the SIGMA-I protocol that includes encryption. Adds nonces, explicit key derivation, and algorithm negotiation. Realized using CBOR and COSE.

- The DH key exchange messages may be authenticated using either pre-shared keys (PSK), raw public keys (RPK) or X.509 certificates (Cert).

EDHOC with asymmetric keys.
EDHOC

- Based on the SIGMA-I protocol that includes encryption. Adds nonces, explicit key derivation, and algorithm negotiation. Realized using CBOR and COSE.

- The DH key exchange messages may be authenticated using either pre-shared keys (PSK), raw public keys (RPK) or X.509 certificates (Cert).

EDHOC with asymmetric keys.
EDHOC

- Based on the SIGMA-I protocol that includes encryption. Adds nonces, explicit key derivation, and algorithm negotiation. Realized using CBOR and COSE.

- The DH key exchange messages may be authenticated using either pre-shared keys (PSK), raw public keys (RPK) or X.509 certificates (Cert).
EDHOC

- Based on the SIGMA-I protocol that includes encryption. Adds nonces, explicit key derivation, and algorithm negotiation. Realized using CBOR and COSE.

- The DH key exchange messages may be authenticated using either pre-shared keys (PSK), raw public keys (RPK) or X.509 certificates (Cert).
EDHOC

- Based on the SIGMA-I protocol that includes encryption. Adds nonces, explicit key derivation, and algorithm negotiation. Realized using CBOR and COSE.
- The DH key exchange messages may be authenticated using either pre-shared keys (PSK), raw public keys (RPK) or X.509 certificates (Cert).
EDHOC

- Based on the SIGMA-I protocol that includes encryption. Adds nonces, explicit key derivation, and algorithm negotiation. Realized using CBOR and COSE.

- The DH key exchange messages may be authenticated using either pre-shared keys (PSK), raw public keys (RPK) or X.509 certificates (Cert).

EDHOC with asymmetric keys.
EDHOC MESSAGE FLOW

- All EDHOC messages are encoded with CBOR
- EDHOC message_2 and message_3 uses COSE
- Protected application data can be sent together with message 3
EXAMPLE

• Can e.g. be implemented as CoAP message exchanges with the CoAP client as party U and the CoAP server as party V.

• EDHOC and OSCOAP can be run in sequence embedded in a 2-round trip message exchange, where the base_key used in OSCOAP is obtained from EDHOC.

This is how EDHOC is used in the OSCOAP profile of ACE draft-seitz-ace-oscoap-profile
NEXT STEPS

• Two implementations underway
  • SICS
  • Jim Schaad

• Minor updates based on review comments

• Ask for CFRG review