Ephemeral Diffie-Hellman Over COSE

EDHOC

draft-selander-ace-cose-ecdhe-09

Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson

IETF 102, ACE WG, Montréal, Jul 16, 2018

Status

- Formal verification of v-08
  - IT University of Copenhagen
  - Expected security properties verified
  - Concern about APP_2, addressed in v-09

- Substantial reduction of message sizes in v-09

CoAP Payload (Bytes)	TLS – PSK+DH	EDHOC – PSK+DH	TLS – DH	EDHOC – DH
Message #1	142	50	107	49
Message #2	135	49	264	125
Message #3	51	12	167	86
Total	**328**	**111**	**538**	**260**

Details changed in v-09

- Renamed APP2 to UAD2 to illustrate that Party U is not authenticated.
- Made S_U optional, e.g when CoAP is used.
- Changed RPK from X.509 to COSE_Key to allow usage of kid
- Always integrity protect the whole credential (certificate, COSE_Key)
- Reduction of overhead (next slide) following requests from applications for a more lightweight handshake (6TiSCH, NB-IoT)

Reduced overhead

- Remove nonces, implying no reuse of ephemeral keys.
- Send x-coordinate, curve alg, ciphertext, and encrypted signature instead of the full COSE structures (COSE_Key, COSE_Encrypt0, COSE_Sign1)
- Use array indexes to specify chosen algorithms
- EDHOC messages and plaintexts are sequence of CBOR elements instead of arrays

Next steps

- Continue formal verification and update security considerations
- More reviews