Ephemeral Diffie-Hellman Over COSE (EDHOC)

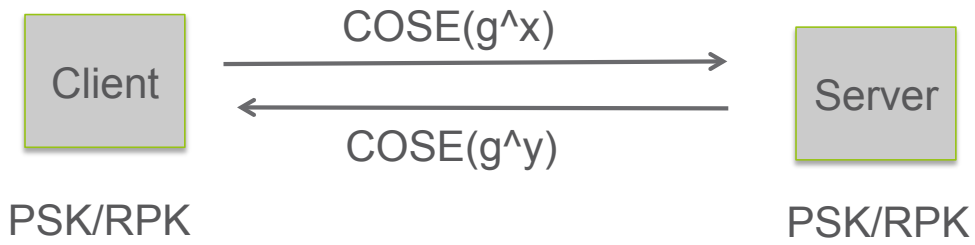
draft-selander-ace-cose-ecdhe-01

G. Selander, J. Mattsson, F. Palombini, Ericsson AB
IETF COSE WG meeting, April 4, 2016

ECDH-EE

› COSE provides a very compact representation of ECDH-SS, and -ES

› For better forward secrecy we want to use ECDH-EE, this is a first attempt



› Using COSE_Mac0_Tagged for pre-shared key (PSK), and COSE_Sign_Tagged for pre-established raw public keys (RPK).

› More protocol details in https://tools.ietf.org/html/draft-selander-ace-cose-ecdhe

ECDH-EE

- We assume this is out of scope for COSE (right?)
- Is there any other activity on/need for embedding security protocols in COSE?
- Are the COSE objects we use with this protocol well formed?
  - For example, in the signed DH, we put the identifier of the receiver in the external_aad.

  Do you have another proposal?
- Other comments?

Key Derivation

- COSE does not reference a specification for deriving the DH-shared secret (such as IEEE 1363-2000)
- E.g. ECDH-ES HKDF-256 is not explicitly defined

- Can we add this to the COSE draft?
- Providing a reference is enough, or more details as in TLS 1.3

https://tools.ietf.org/html/draft-ietf-tls-tls13-12#section-7.3.3

Thank you!

Questions/comments?