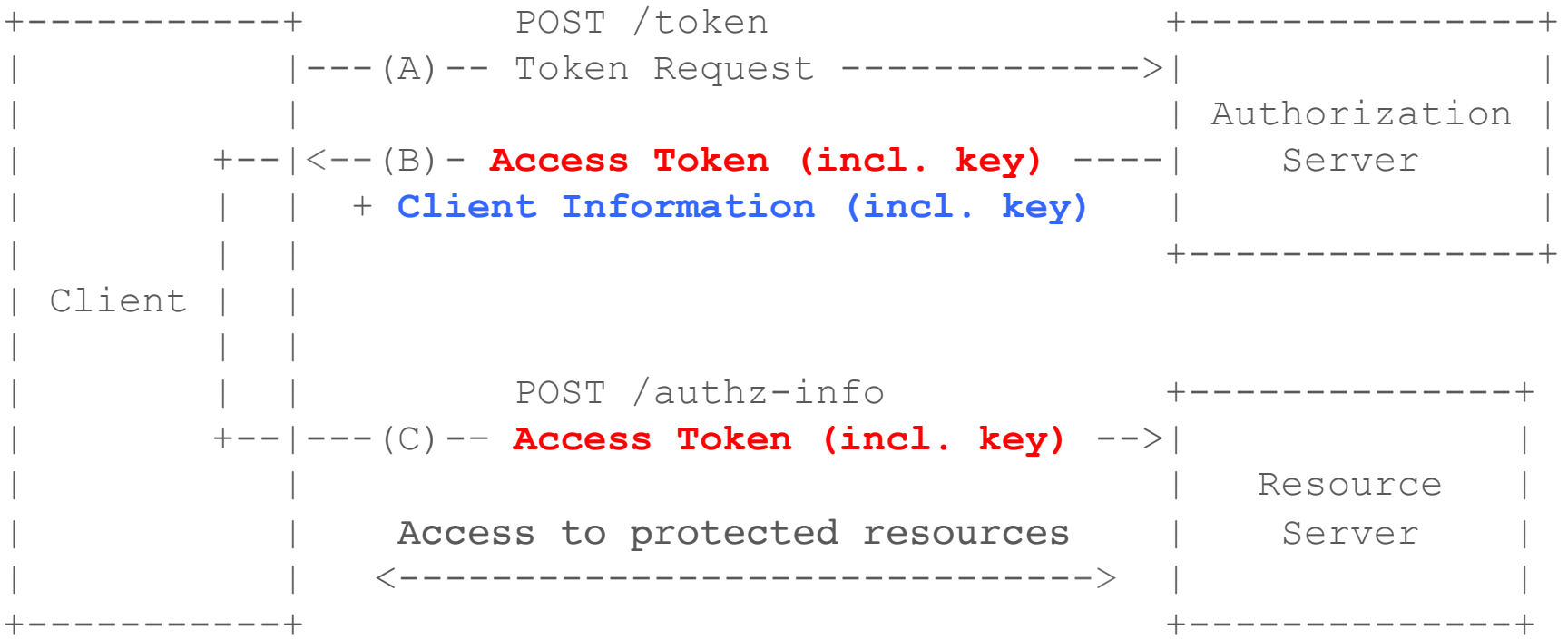
EDHOC

draft-selander-ace-cose-ecdhe

Göran Selander, John Mattsson, Francesca Palombini
IETF 96, ACE WG, Berlin, Jul 20, 2016

Background: ACE Framework



- The AS distributes keys for authentication between C and RS
- Symmetric key could be used “directly”
- Public keys can authenticate key establishment
- **EDHOC does key establishment based on COSE**

Why COSE (CBOR Object Signing and Encryption)?

COSE is a generic object security format for the IoT

1. Many potential applications
   - Used in ACE framework: Access Token (CWT), Client Token
   - Used in OSCOAP and the ACE OSCOAP profile
   - Will be used to protect multicast CoAP messages
   - Other applications: secure firmware update, etc.

→ there is a good chance your device will have COSE code

2. COSE is not bound to a particular protocol layer

COSE specification: draft-ietf-cose-msg

How is EDHOC using COSE?

- COSE specifies key establishment protocols
  - ECDH-SS and ECDH-ES
  - **EDHOC implements ECDH-EE** (6.2.2.2 in NIST SP-800-56a)
    - 2-pass instead of 1-pass
    - provides forward secrecy

- COSE specifies
  - data structures and types
  - encoding of messages
  - context for KDF
  - key derivation process, including security considerations
- **EDHOC references and uses this**

What else is EDHOC doing?

- Negotiation of hash algorithm used with KDF to derive keys
  - Requesting party proposes array of at least one algorithm
  - Responding party selects one
- Negotiation of AEAD to use with derived keys
  - Requesting party proposes array of at least one algorithm
  - Responding party selects one
- Replay protection of request based on sequence numbers
  - Reject messages with lower number than previously received
- Parties may send nonces contributing to the salt of the KDF
  - Not necessary but recommended in RFC5869
- Parties may authenticate using PSK, RPK or X.509 certificates
  - In the latter case, parties may send certificates

How is EDHOC using CoAP?

- COSE messages are payload in CoAP POST request & response
- No security needed for transporting the messages
- EDHOC is small code addition given COSE and CoAP

- EHDOC can be used to authenticate, establish keys, negotiate algorithms etc. over foo
  - E.g. for COAP over foo (UDP, TCP, Bluetooth, 802.15.4 IE, . . .)

- EDHOC does not require CoAP, can be used directly over foo
- Examples of message sizes
  - PSK: ~ 80 bytes
  - RPK: ~ 140 bytes

What does EDHOC mean?

› Ephemeral Diffie-Hellman over COSE

Next steps

- Update based on review comments
- Find a home for this work
- Ask CFRG for review
- Implementation

Thank you!

Comments/questions?