DTLS and OSCOAP

Transport layer security

and

Application layer security

Current state of the draft

- Transport layer security
  - Based on DTLS
- Application layer security
  - Based on OSCOAP and COSE

- Connection to OSCOAP has been loosened slightly saying ObjectSecurity

How to use PoP token key in DTLS

- Use the symmetric PoP key as DTLS PSK
- Use the asymmetric PoP key as RPK for authentication of the client and “client information” RPK attribute for authentication of the RS.
- How to use a client certificates is not defined yet?

- One to one mapping do not mix usage of symmetric and asymmetric keys to keep it simple.

How to use PoP token key in OSCOAP

- OSCOAP is object security for CoAP
  Builds on COSE. Works with symmetric keys and uses a handshake to establish symmetric session keys

- Symmetric PoP keys could be used directly or to establish session keys.
- Asymmetric PoP keys should be used to establish symmetric session key.

Alternatives

- Alternative 1
  Define extension points and specify details for DTLS and OSCOAP in other documents.
- Alternative 2
  Define extension points and specify exact usage for DTLS and specify details OSCOAP in other documents.
- Alternative 3
  Define extension points and specify exact usage for DTLS and OSCOAP in this document.

Questions for the WG

- Which alternative should we proceed with?
  - 1, 2, 3 or Other
- In what WG should object security be in?
  - ACE, CORE or Other
- Should we define how to use client certificates?