Authentication and Authorization for Constrained Environments (ACE)

draft-ietf-ace-oauth-authz-10 (= framework)
draft-ietf-ace-dtls-authorize-03 (=dtls profile)
draft-ietf-ace-oscore-profile-01 (=oscore profile)

Ludwig Seitz (ludwig.seitz@ri.se)

IETF 101 ACE WG meeting
March 19, 2018

Framework updates from 08 to 10

- Improved IANA section
- Allowed scope claim to be byte array
- Default names for introspect and token endpoints
- Removed client token design
- Clarifications on possible use of HTTP instead of CoAP

DTLS-profile updates from -02 to -03

- Clarified how client detects RPK/PSK mode
- PSK identity cleanup
  - Try psk identity as kid first, then check for access token
- Mandate Ed25519 for RPK mode
- Several clarifications to satisfy framework draft, Appendix C
- Placeholder: Plugtest results
- Next steps:
  - Gather more implementation experience
  - Insert examples
  - Collect reviews

OSCORE-profile updates from -00 to -01

- Added clarification that CWTs need to be encrypted
  - OSCORE master key is in the cnf claim
- Clarified how the proof-of-possession is done
  - Implicit by generating a valid OSCORE context
- Added security considerations
- Added IANA considerations

Discussion points

- Relationship to Token Binding work at OAuth
  - Question by Mike Jones
  - Volunteers from OAuth to work it out with us?
- Relationship to OCF work

Next steps

- WGLC?
- Implementations
  - Some interop testing this week
  - Bigger event at IETF 102
  - Known implementers:
    - RISE SICS
    - TZI Univ. Bremen
    - Jim Schaad
    - SEI lab at CMU