Authentication and Authorization for Constrained Environments (ACE)

draft-ietf-ace-oauth-authz-22 (= framework)
draft-ietf-ace-oauth-params-04 (=params)

Ludwig Seitz (ludwig.seitz@ri.se)

IETF 104 ACE WG meeting
March 29, 2019

Framework updates from 16 to 17

- Added section on how RS verifies incoming tokens
- Added section on protection of authz-info
  - No actions on children of authz-info
  - Only POST allowed
  - Rate limitations
- Removed expiration based on sequence numbers
- Added minimal security requirements for communication
  - Encryption, integrity protection, replay-protection, freshness, binding response to request

Framework updates from 17 to 19

- Added definition of “Authorization Information”

  = whatever the RS uses to determine access rights

  - Not to be confused with “Access Information”
    - AS → client in access token response
- “AS information” → “AS Request Creation Hints”
  - RS can now also specify require scope and audience
- Added “kid” to AS Request Creation Hints
  - Request new token for some security association
- Security consideration for multi-RS audiences
  - Symmetric key protection not enough
- Expert review instructions for mapping registries

Framework updates from 19 to 22

- Added text about expiration of RS keys
  - Avoid sending sensitive requests to RS using expired key
- Updated IANA mapping sections to only be “Expert review” or “private use”
  - No need for a spec to register: “assertion = 47”
- Made error responses optional for RS
  - May not be able/want to respond

Params updates from 00 to 04

- Added examples
- Replaced “req_aud” with “audience” from OAuth token exchange

Next Steps

- Fix issues with mapping
  - (Yes there still are some)
- Add processing instructions for cnonce
  - Got lost when copied from DTLS profile
- Add clarifications