Authentication and Authorization for Constrained Environments (ACE)

draft-ietf-ace-oauth-authz-06

Ludwig Seitz (ludwig.seitz@ri.se)

IETF 98 ACE WG meeting
May 27, 2017

Major changes from -04 to -06

- RFC 2119 language for profile requirements
- Relation to OAuth2 grants & /authorize
- More security considerations for pop-keys
- Added Privacy Considerations
- Even more IANA mappings
- Reorg of the sections structure
  - Sorry profile authors, I broke your references

Grant flows & authorize endpoint

- Main grant used is *client credentials*
  - AS decides what access token to grant based on client credentials
  - Should we develop a dedicated ACE grant?
- Other ACE-relevant grants:
  - *authorization code*
  - *device code (draft-ietf-oauth-device-flow)*
- OAuth /authorize endpoint
  - Request grants (not used for *client credentials*)
  - Needs client UI → Out of scope for ACE

Security & Privacy Considerations

- Security
  - Tokens valid for multiple RS
    - Using the audience claim
  - Symmetric keys as pop-key

  → Any RS can impersonate the client to the other RS in the audience
- Privacy
  - With client credentials grant AS can track C
  - Non-encrypted CWT can leak information

Client and RS registration

- See Appendix D, what does the AS know?

Client:

- Identifier
- Supported profiles
- Supported key types
- Shared key or public key

RS:

- Same as for C, plus:
- Supported access tokens (e.g. CWT)
  - Supported COSE wrappers
- Expiration for tokens
- Scopes & Audiences?

Implementation status

- ACE Framework implemented in Java
  - https://bitbucket.org/lseitz/ace-java
- Parts missing
  - A profile (to run C – RS interactions)
  - Only Client Credentials grant
  - Constrained code forthcoming (IETF 99 ?)
- Who else wants to give it a go?

ACE profiles

- Currently 4
  1) CoAP over DTLS
  2) CoAP+OSCOAP
  3) MQTT over TLS
  4) Pub-Sub over CoAP
- Blutetooth Low Energy someone?
- I’m implementing 1 & 2
- Time to adopt some profiles?
  - *Note: Cannot fully demonstrate ACE framework without implementing a profile*

Thank you!

Questions/comments?