Authentication and Authorization for Constrained Environments (ACE)

draft-ietf-ace-oauth-authz-04

Ludwig Seitz (ludwig@sics.se)

IETF ACE WG meeting, IETF 97
17. November, 2016

Major changes from -02 to -04

- Removed references to OAuth PoP drafts
- Clarified requirements on profiles
- Simplified token request C → AS
- Updated security considerations

Relation to OAuth PoP drafts

- Status of PoP drafts at OAuth WG unclear

  → removed references to:
    - draft-ietf-oauth-pop-architecture
    - draft-ietf-oauth-pop-key-distribution
- Current solution: Specify “ACE-PoP” here
  - ACE profiles need to specify PoP protocols
  - See examples in OSCOAP and DTLS profiles
- Copied relevant security considerations
  - (With acknowledgments)
- Feedback (especially from OAuth) needed!

Memory refresher: Profiles

- This document: framework
- Profiles: interoperable implementations
  - Define discovery
  - Define comm protocol
  - Define commSEC (e.g. DTLS over CoAP)
  - Authentication and Proof-of-Posession
  - Content formats
- Current:
  - CoAP-OSCOAP (draft-seitz-ace-oscoap-profile)
  - CoAP-DTLS (draft-gerdes-ace-dtls-authorize)
- Upcoming (IETF 98?): MQTT

Requirements on profiles

- -02: Requirements on profiles scattered
- -04: Collected in Appendix C
- Should they be in the normative part?

Simplified Token Request Protocol

- -02: Negotiation of profile parameters
  - Seemed over-engineered
  - AS would know client and RS capabilities
- -04: Removed negotiation
  - AS determines profile & parameters based on registration info
  - AS informs client of chosen profile & parameters
- Feedback from the WG welcome!

Security Considerations

- Copied and adapted large parts from draft-ietf-oauth-pop-key-distribution
- Mentioned in the Acknowledgments
  - Is that appropriate?

Implementations

- SICS implementation ongoing
  - Java library for AS/Client/RS
  - BSD 3.0 license
  - C implementation for Client/RS will come later
  - Will announce on ACE ML when published
- SEI, Carnegie Mellon University
  - Use case: Tactical Environments
  - Implementation target: Q3 2017
- We think it is time for implementations
  - Interop possible at IETF 98?

Thank you!

Questions/comments?