Resource Indicators for OAuth 2.0

Brian Campbell et al.

IETF 95
Buenos Aires
April 2016

What is it?

- A new “resource” parameter
  - URI where the client intends to use the access token
  - Applicable on the:
    - Authorization request for access tokens that will be returned from the authorization endpoint
    - Token request for access tokens that will be returned from the token endpoint
  - Usage implies the resource is not persisted with the grant
Why Bother?

- Enables access token to be minted appropriate to the target resource
  - Encryption, content/claims, reference vs. JWT, keys/algs, etc.
- Facilitates audience restricting access tokens
  - AS may use the exact "resource" value for audience or it may map to a more general URI or abstract identifier for the RS
- General concept has been discussed for some time
  - ‘audience’ in tschofenig-oauth-audience, ‘aud’ in oauth-pop-key-distribution, ‘resource’ & ‘audience’ in oauth-token-exchange
- Proprietary variations already exist and deployed
- Arguably an omission of the original OAuth 2.0 spec
Relation to Scope?

- Scope is ‘what’
  - Sometimes overloaded to convey the location of the resource server (or it’s implied)
    - But not always feasible or desirable

- Resource is ‘where’
  - & allows for distinct treatment of ‘where’ from ‘what’
Next Steps?

- Please read (it’s relatively short)
- Feedback, changes, additions, vague & incomprehensible criticisms…
- Better title?
- Consideration as a WG document?
- Kill it?
- Let it linger for a few years until the idea is resurrected in some other form?
- Other?