Token Introspection

IETF92

Justin Richer

Changes From WGLC

- Removed “resource_id” (nobody was using it)
- Added privacy considerations
- Clarified “active” and added security notes for auth servers
- Changed “user_id” to “username”
  - This will break some existing implementations but the ones I’ve talked to are OK with this change
- Updated references

Open Issue: Registries

- Two ways to communicate token information
  - Inside the token (JWT)
  - From a service (introspection)
- Originally defined completely separately
  - "Why not use the same fields?"
- First, introspection "imported" the JWT fields
- Then, introspection extended the JWT registry
  - But that's really confusing it turns out

WAYS FORWARD FOR REGISTRIES

Option 1:

Extend the JWT registry

- Pros:
  - Automatic deconfliction
  - One list to check for all possible values
- Cons:
  - Some fields don't make sense inside a JWT or inside an introspection response
- Options:
  - Add a field to the JWT registry for a "target" application of any given field

Option 2:

New, complete introspection registry

- Pros:
  - Each registry is canonical for its usage
- Cons:
  - Fields need to be registered twice if usable in both locations, information skew
  - Two lists to check
- Options:
  - Seed the introspection registry with all current fields from JWT registry

Option 3:

New introspection-only registry

- Pros:
  - Clear demarcation for usage
  - Maximize re-use of JWT
- Cons:
  - No clear process for cross-registry deconfliction (that I can see)
- Options:
  - Ensure that the reviewers for introspection registry are the same as those for JWT