OAuth Token Introspection

IETF 90 Toronto

What is it?

- HTTP API for fetching information about a token
  - Is it valid?
  - Who authorized it?
  - Who was it issued to?
  - When does it expire?
  - When was it issued?
  - What scopes is the token authorized for?
  - Extensible with other information (like user-defined policies)

What is it for?

- Opaque artifact-style tokens
- Split deployments between RS and AS
  - RS gets token, says “I need an adult!”
- Looser coupling between RS and AS
  - Cross-domain token federation

Basic Process

- Client presents token to RS
- RS calls token introspection endpoint of AS
  - RS authenticates during this call (with another token or with credentials of some kind)
- AS validates the token & looks up metadata
  - AS-specific process: DB lookup, process token contents, magic
- AS returns JSON object with information about the token

Usage patterns

- Bearer tokens
  - RS sends the token value directly to the AS
- JWT bearer tokens in cross-domain deployments
  - RS parses JWT, looks up issuer, introspects at the issuer
- PoP/HoK tokens
  - RS sends the token ID (“access_token” value) to the AS

Document status

- Individual draft submission -00 in November 2012
- Current draft: -06
- Several implementations in the wild