Observations from the OAuth Feature Survey

Mike Jones
March 14, 2013
IETF 86
Data Gathered to Date

- Data characterizing 9 implementations
  - With more to follow
- 191 characteristics of implementations collected
- Covering:
  - RFC 6749 (OAuth Authorization Framework)
  - RFC 6750 (OAuth Bearer Token Usage)
  - draft-ietf-oauth-saml2-bearer
  - draft-ietf-oauth-jwt-bearer
  - oauth-v2-multiple-response-types-1_0
  - Scopes defined by openid-connect-messages-1_0
All the specs are being used

• But they are being used differently
• Differences include:
  – Client types supported
  – Grant types used
  – Whether scopes are static values or structured
  – Whether access tokens are opaque or structured
  – Whether refresh tokens are supported
• Which extension points are used and how
Use of Extension Points is the Norm

• Extension points used include:
  – Scope values
  – Grant types
  – Response types
  – Request parameters (authorization & token)
  – Response parameters (authorization & token)
  – Protocol endpoints
  – HTTP authentication schemes
Interoperability is Being Achieved

• To achieve interop, implementations use common profiles
• Two profiles evident:
  – OpenID Connect profile of OAuth 2.0
  – OpenESPI - Smart Grid profile
• There may have been others
• Others were just building framework code
  – With interop achievable by applications using it