OAuth 2.0 Authorization Server Discovery Metadata

draft-ietf-oauth-discovery

Mike Jones
IETF 95, Buenos Aires
April 2016
Current draft addresses WGLC feedback

- See https://tools.ietf.org/html/draft-ietf-oauth-discovery-02#appendix-B for specific changes made
- (obviously other than the “don’t do this work” feedback)
Use Cases Covered (1)

- OAuth 2.0 client configuration
  - Provides data needed to configure a client to use an authorization server in a standard format
  - Superior to publishing the same data on developer Web pages in an ad-hoc manner

- AS configuration validation
  - Clients can validate issuer returned per draft-ietf-oauth-mix-up-mitigation with metadata issuer
  - Clients can validate AS metadata obtained at configuration time against AS metadata obtained at runtime
Use Cases Covered (2)

- Authorization Server Discovery Result
  - The AS Discovery Metadata document is the result of AS discovery processes, such as WebFinger lookup of the AS

- AS Metadata Registry enables extensibility
  - Enables publication of application-specific metadata about the authorization server
  - For example, publication of resource server info when RS controlled by the authorization server
Implementation Status

- Several OAuth clients using for configuration
  - E.g., Microsoft ADAL OAuth client, RoHe client
- All OpenID Connect Discovery implementations use this AS metadata format
  - E.g. 23 implementations using this metadata format listed at [http://openid.net/certification/](http://openid.net/certification/)
Next Step for Spec: Request Publication

● Why?
  ● Standardize existing practice for AS metadata
  ● Enables AS configuration to be validated at runtime for mix-up mitigation

● But what if we haven’t thought of everything?
  ● The registry enables extensibility

● But what about solving discovery all-up?
  ● The AS metadata format is stable and any AS discovery solutions developed will use it
OAuth Discovery

Landscape and Use Cases

- Discussing, agreeing on Discovery use cases is likely the most productive WG next step
- In one common use case, AS controls single RS – as in OpenID Connect use case
- Phil, Tony leading discussion on use case in which client knows both intended RS & AS
- Many other use cases already implemented
- Hopefully understanding diverse OAuth Discovery use cases will result in new widely applicable consensus Discovery solutions
Next steps towards deeper OAuth Discovery

- Determine use cases we want to enable
- Evaluate possible solutions
- Create additional discovery specifications standardizing those solutions