*

OAuth 2.0 Authorization Server Discovery Metadata

draft-ietf-oauth-discovery

Mike Jones
IETF 96, Berlin
July 2016

Document Status

- Current draft is draft-ietf-oauth-discovery-03
- Functionality scoped back to only authorization server metadata document definition
  - Format based on significant existing practice

- Some consider the spec complete for their use cases
- Phil Hunt has been asking us to also work on use cases that start at the resource server
  - The OAuth metadata set is not complete for those use cases
  - Currently, metadata documents defined for clients and authorization servers but not for resource servers

Proposed Resolution

- Fill gap by defining resource server metadata document
- Mike and Phil have agree to work on this together
- draft-jones-oauth-resource-metadata coming soon

Feature Outline

- JSON document, parallel to the other metadata formats
- Contains URI identifying resource, for integrity purposes
- Can list authorization servers to use
- Can list RFC 6750 bearer token methods supported
- Can list scopes used with this resource
- Can provide documentation about resource
- Can provide privacy policy for resource
- Can provide terms of service for resource
- Located at .well-known/oauth-resource-server

Signed Metadata

- Some use cases require signed metadata
  - For instance, federation establishment and maintenance
  - Roland Hedberg’s OpenID Connect federation spec needs it
- We have signed client metadata
  - Software Statement
- We don’t have signed authorization server metadata

- **Proposal:** Also define signed metadata formats for authorization server and resource server metadata
  - Parallel to software statements for clients

Referencing RS Metadata from AS Metadata

- **Proposal:** Define optional “resources” AS metadata value to list resources that can be used with the AS
  - Just like “authorization_servers” RS metadata can list ASs that can be used with the resource

- For use cases with enumerable sets, will enable AS and RS metadata documents to cross-reference one another

Naming Question

- Because it used to also define discovery mechanisms, current AS metadata document title is:
  - OAuth 2.0 Authorization Server Discovery Metadata
- Some have asked us to remove “Discovery” from name
- Others point out that metadata is the *discovery result*
- Discussion: Should we remove “Discovery”?

- Note: Current working RS Metadata document title is:
  - OAuth 2.0 Resource Server Metadata
- Removing “Discovery” would make the names more parallel

Discussion

- Shall we proceed in the ways described?