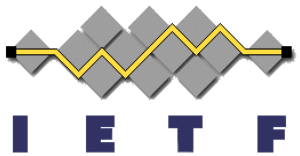
*

OAuth 2.0 Authorization Server Discovery Metadata



draft-ietf-oauth-discovery

Mike Jones

IETF 101, London

March 2017

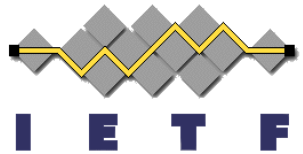
Document Status

- Current draft is draft-ietf-oauth-discovery-10
  - Since Singapore, -08, -09, -10 published to address Designated Expert and IESG feedback
- Was on January 25, 2018 IESG Telechat
- All IESG positions are now Yes or No Objection
  - https://datatracker.ietf.org/doc/draft-ietf-oauth-discovery/ballot/
- Now in “AD Followup” state
- One normative change was made as a result of IESG feedback

Change to .well-known string processing rules

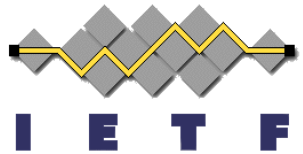
- Well-known string previously appended to issuer value
  - E.g., https://example.com/issuer1/.well-known/oauth-authorization-server
- Well-known string now inserted between host name and path in issuer value
  - E.g., https://example.com/.well-known/oauth-authorization-server/issuer1
- No change if issuer doesn’t have

Reason for Change



- BCP 190 (URI Design and Ownership) prohibits spec use of URI path namespace except for registered usages starting with “/.well-known”
- Old rules violated this by using “/.well-known” in locations other the beginning of the path

Impact of the Change



- Means OpenID Connect Metadata documents will be at a different location than OAuth AS Metadata documents
  - (when the issuer contains a path component)
- Services that are both an OpenID Connect OPs and general-purpose OAuth ASs may have to publish metadata in both locations
  - (at least for a transition period)
- Clients that are both OpenID Connect RPs and general-purpose OAuth clients may have to look for metadata in both locations
  - (at least for a transition period)
- New OAuth services should use the new location

Next Steps

- Needs AD action to send to the RFC Editor