Reciprocal OAuth

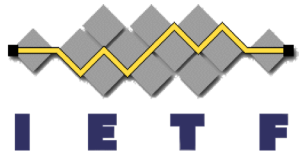
ietf-oauth-reciprocal

Dick Hardt
IETF 102, Montreal
July 2018

Since Singapore

- Changed name to “reciprocal” from “mutual”
- Added reciprocal parameter
- Adopted as WG document

Problem



- User would like authorize party A and party B to access protected resources at each other
- Eg. Alexa and Sonos integration
  - Alexa calls Sonos to play a station
  - Sonos calls Alexa to update current song
- Setup is complicated and confusing as 2 OAuth flows are required

Current User Flow 1/2

- 1) User clicks to add Sonos in Alexa App
- 2) User authenticates to Sonos
- 3) User authorizes Alexa at Sonos
- 4) User redirected to Alexa with Sonos authorization code
- 5) Alexa exchanges Sonos authorization code for access token
- 6) Alexa redirects to Sonos to start 2nd flow

Current User Flow 2/2

- 7) Sonos redirects to Login With Amazon
- 8) User authenticates at Amazon
- 9) User authorizes Sonos at Amazon
- 10) User redirected to Sonos with Alexa authorization code
- 11) Sonos exchanges Alexa authorization code for access token
- 12) User is redirected to Alexa at completion

Reciprocal OAuth User Flow

- 1) User clicks to add Sonos in Alexa App
- 2) User authenticates to Sonos
- 3) User authorizes Alexa at Sonos
- 4) User redirected to Alexa with Sonos authorization code
- 5) Alexa exchanges Sonos authorization code for access token
- 6,7,8 removed
- 9) User authorizes Sonos at Alexa
- 10B) **Alexa calls Sonos token endpoint with Alexa authorization code**
- 11) Sonos exchanges Alexa authorization code for access token

Reciprocal Scope

- Sonos (party B) can include scope in Authorization Response

```
HTTP/1.1 302 Found Location:
 https://client.example.com/cb
    ?code=SplxlOBeZQQYbYS6WxSbIA
    &state=xyz
    &reciprocal=example_scope
```

Reciprocal Authorization Code

- Alexa (party A) calls token endpoint with
  - grant_type “urn:ietf:params:oauth:grant-type:reciprocal”
  - Party B access token
  - authorization code

Example

```
POST /token HTTP/1.1 Host: server.example.com
Authorization: Basic ej4hsyfishwssjdusisdhkjsdksus
Content-Type: application/x-www-form-urlencode
 grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-
type%3reciprocal
 &code=hasdyubasdjahsbdkjbasd
 &client_id=example.com
 &access_token=sadadojsadlkjasdkljxxlkjdas
```

Updating Authorization

- Change in authorization granted in voice interface
- Allows incremental scopes
- New authorization code to Sonos to acquire new refresh and access tokens

Symmetrical Relationship

- User can start at either Alexa or Sonos
- Either party update other's authorization

Implementations

- Alexa and Sonos
- Others in development

Next Steps

- Fix typos ☺

- Include updating authorization?
- Other suggestions?