Mutual OAuth
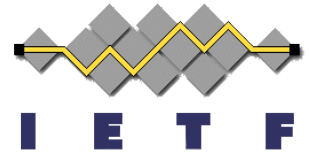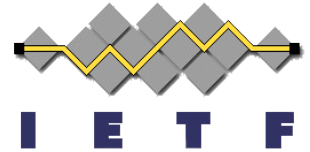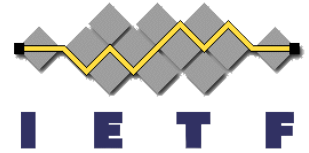
draft-hardt-mutual-oauth

Dick Hardt
IETF 100, Singapore
November 2017

Problem

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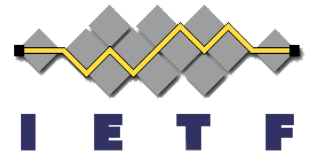- Setup is complicated and confusing as 2 OAuth flows are required

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
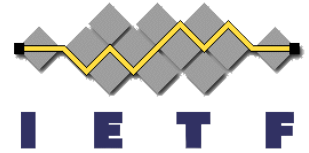
Current User Flow 2/2

- 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
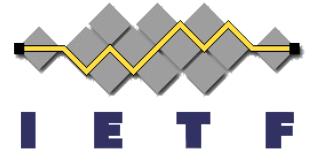
Mutual Oauth User Flow

- 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) **Alexa calls Sonos token endpoint with Alexa authorization code**
- 7) Sonos exchanges Alexa authorization code for access token *(was step 11)*
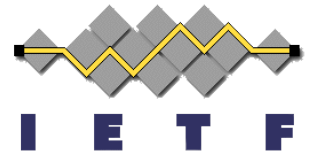
AuthN Code Context

- Alexa uses Sonos access token to pass Alexa authorization code

- Scope represented by Alexa authorization code is configured out of band

- Sonos makes standard access token request with Alexa authorization code

Next Steps

- OAuth WG Interest?