OAuth WRAP
Overview

Dick Hardt
IETF 77, March 22, 2010
Name History

- Simple OAuth
- Simple Auth
- WRAP
  (Web Resource Authorization Protocol)
- OAuth WRAP
Authors

• Allen Tom, Yahoo!
• Brian Eaton, Google
• Yaron Goland, Microsoft

• Editor: Dick Hardt
OAuth 1.0A Issues

- Client implementation pain (crypto)
- Single profile (web app and rich app)
- Tight coupling between AS & PR
  - Enterprise use cases
  - Scale in large deployments
Use Cases

• User Delegation
  - Web App
  - Rich App (PC, phone, device)

• Authorization Delegation
  - Cloud Computing
Cloud Use Case

Client

PR
(Protected Resource)

AS
(Authorization Server)
Accessing a PR

Client → AS
  (A) Credentials

AS → PR
  (B) Access Token

PR → Client
  (C) Access Token
Obtaining Refresh Token

Client → (B) Access Token, Refresh Token → AS

PR
Refreshing Access Token

Client → (A) Credentials
Client ← (B) Access Token
Client → (C) Access Token

PR

AS
Refreshing Access Token

Client → (B) Access Token → AS

Client ← (A) Refresh Token ← AS

(C) Access Token → PR
Terminology

- Client (Web App, Rich App, Mobile App, Device...)
- Protected Resource
- Authorization Server
- User
- Access Token (short lived bearer token)
- Refresh Token (long lived bearer token)
Access Token

- Out of scope for OAuth WRAP
- Likely contains:
  - Authorization / scope(s) / permission(s) / role(s) / identifier(s)
  - Expiration
  - AS Signature
Refresh Token

- Out of scope for OAuth WRAP
- Issued and consumed by AS
- Contains information needed to issue a new Access Token
WRAP Capabilities

- Claims oriented model
- Separation of AS and PR
- Delegated Access for users
- Delegated Authorization for PR
- Single PR entry point
Potential Future

• JSON results from AS
• method parameter in AS calls
• additional profiles
• optional, standard JSON Access Token
• client signing / creation of Access Token (OAuth 1.0 like functionality)