SCIM & OAuth

IETF91

Novermber 14, 2014

Introduction

- A collection of extensions and schema enhancements related to OAuth

Authentication / Binding

- Over the past year, we've had some questions about whether SCIM should do authentication.

  – We've indicated that SCIM is a protocol on top of HTTP and thus should use mechanisms already defined for HTTP such as OAuth

- App access (introspection?) to end-user session information as part of SCIM

SCIM as an OAuth Resource

- Directory
  - User information for OAuth Subjects
- Access Control Model
  - What are the "scopes"
  - E.g. we could follow LDAP's model
    - A general model
    - No specific inter-op, just requirements
    - Supports notion of operations against self, etc.

OAuth Extensions for SCIM

- Following slides are about using SCIM to support management of OAuth information
- This work is a collection of items
- They may not be appropriate for this WG

OAuth Resource Registration

- OAuth resource information
  - Discovery of end-points
  - OAuth discovery items
  - Registered Scopes

Client Software

- Definition of client apps that may register with an OAuth server
  - May include approved software statements
  - Defines classes of "client" instances

Client Registration Information

- Information on instances of client apps registered
- Used in User profile/mdm/mam systems to allow users to see authorized clients etc.

OAuth Grants

- Endpoints or extensions to track extensions approved by SCIM Users

- Enables user self-service and revocation

- List outstanding tokens and expiries?