The US National Virtual Observatory

Matthew J. Graham (Caltech, NVO)

Introduction

- Controlling who has access to resources and what operations are permitted is a common activity across the VO:
  - editing resource records in the registry
  - deleting data objects in VOSpace
  - accessing proprietary data through DAL services
- Administrators do not like entrusting management operations to third parties
- Access rights and management systems will vary but it should be possible to define a common interface to manage access control *locally*

Concepts

- An *entity* can be a user, resource or operation
- A *token* is a tag to identify an entity – can be URI
- A *resource* is identified by a GUID
- A *user* is identified by a resolvable token – X.509 DN or URI
- An *operation* is identified by a resolvable token
- An *association* can exist between a resource, an operation and a resource
- A *set* or *collection* of resources, users or operations is identified by a token
- A human-readable *policy* can be associated with an operation

Methods

- defineCollection (collection, entities)
- deleteCollection (collection)
- getCollection (collection)
- getOperations (token, resource)
- getOperationDescription (operation)
- associate (user, resource, operation)
- dissociate (user, resource, operation)
- setPolicy (policy, operation)
- getPolicy (operation)

Use cases

- What operations are supported?
  Request: getOperations()
  Response: create, retrieve, update, delete
- What does an operation mean?
  Request: getOperationDescription(create)
  Response: This operation will create a new resource
- Let's set the policy for an operation:
  Request: setPolicy(createPolicy, create)
  Response: success
- Let's define some collections:
  Request: defineCollection(cruPerm, [create, retrieve, update])
  Response: cruPerm
  Request: defineCollection(crudPerm, [cruPerm, delete])
  Response: crudPerm
  Request: defineCollection(myGroup, [user1, user2, user3])
  Response: myGroup
  Request: defineCollection(someResources, [myResource1, myResource2])
  Response: someResources
- Let's give some permissions to some users:
  Request: associate(myGroup, someResources, cruPerm)
  Response: success
  Request: associate(user1, someResources, crudPerm)
  Response: success