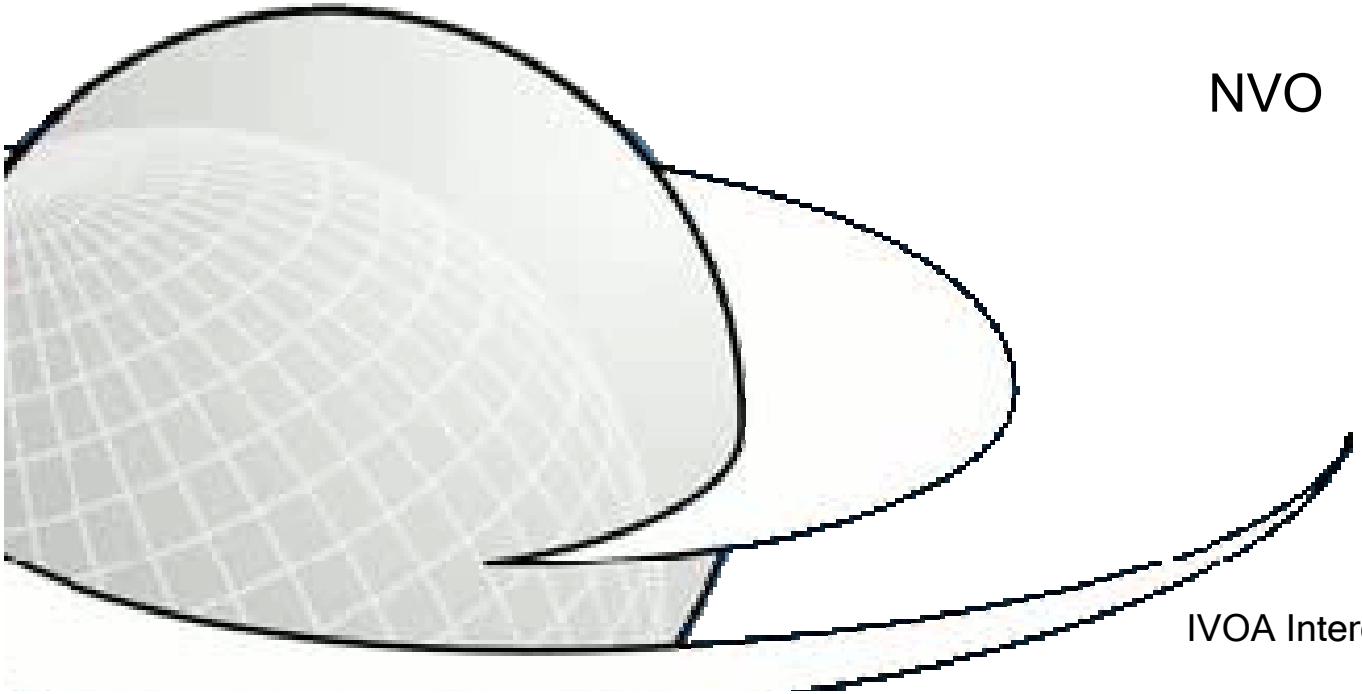
THE INTERNATIONAL VIRTUAL OBSERVATORY ALLIANCE

OpenID, Portal Security, and Access Rights

Ray Plante

NVO



29 October 2008

IVOA Interoperability Meeting -- Baltimore

Portal-based Single Sign-on

- Goals:
  - Users have a single login name/password for use with any NVO-compliant portal
  - A compliant portal provider can
    - Interoperate with users' remote data and other secured assets
    - Intermix public and proprietary data in the same interface
  - Users can establish secure sessions that span across multiple portals and services

User Experience

- Portal Registration
  - User registers with portal: fills in form
  - Portal forwards user and minimal registration info NVO registration form
    - User creates VO identity with NVO
    - User returned to portal
- Logging In
  - User visiting portal clicks on “login” link
  - Link forwards user to NVO login service
  - On successful authentication, user is returned to portal
  - In the background, portal retrieves a user certificate from NVO login server

Deployment Details

- We provide a portal toolkit for plugging NVO logins into a portal
- Technologies Used:
  - Pubcookie – delegated authentication
  - MyProxy – EEC & proxy certificate creation
  - Apache
    - mod_perl, mod_pubcookie, mod_myproxy
  - Purse – user management at login server
- Services
  - Authentication services replicated at NCSA and NOAO for high-availability
  - MyProxy service
  - Identity Portal
    - User can maintain metadata, passwords, preferences
    - Can download certs for loading into client applications (browser)
- Compliant Portals
  - NOAO NVO Portal – used to access proprietary data in VO environment
  - NESSSI Portal – access to grid processing
  - DES Project Portal

Motivating OpenID

- Opportunity for standardization
  - Pubcookie is not a good basis: does not define its protocol
- Portal providers want a way to access user metadata/attributes
  - e.g. latest email address
  - We must address the privacy issues
- We want to provide strong identities
  - Authenticated attributes indicate
    - the identity is recognized by an authority as bona fide
    - the identity owner is a member of some group
  - Provide this information
    - Embedded in the credentials
    - Delivered on demand via service

OpenID is attractive

- Serves same role as pubcookie: web-based delegated authentication
  - Open, documented protocol
  - Broad support in many languages
  - Simpler integration with portal software
- Provides mechanism for sharing user attributes with portal
  - Privacy Issues addressed:
    - User can preset preferences for sharing information
    - In the absence of preferences, user is asked interactively
  - Smooth integration with portal interaction