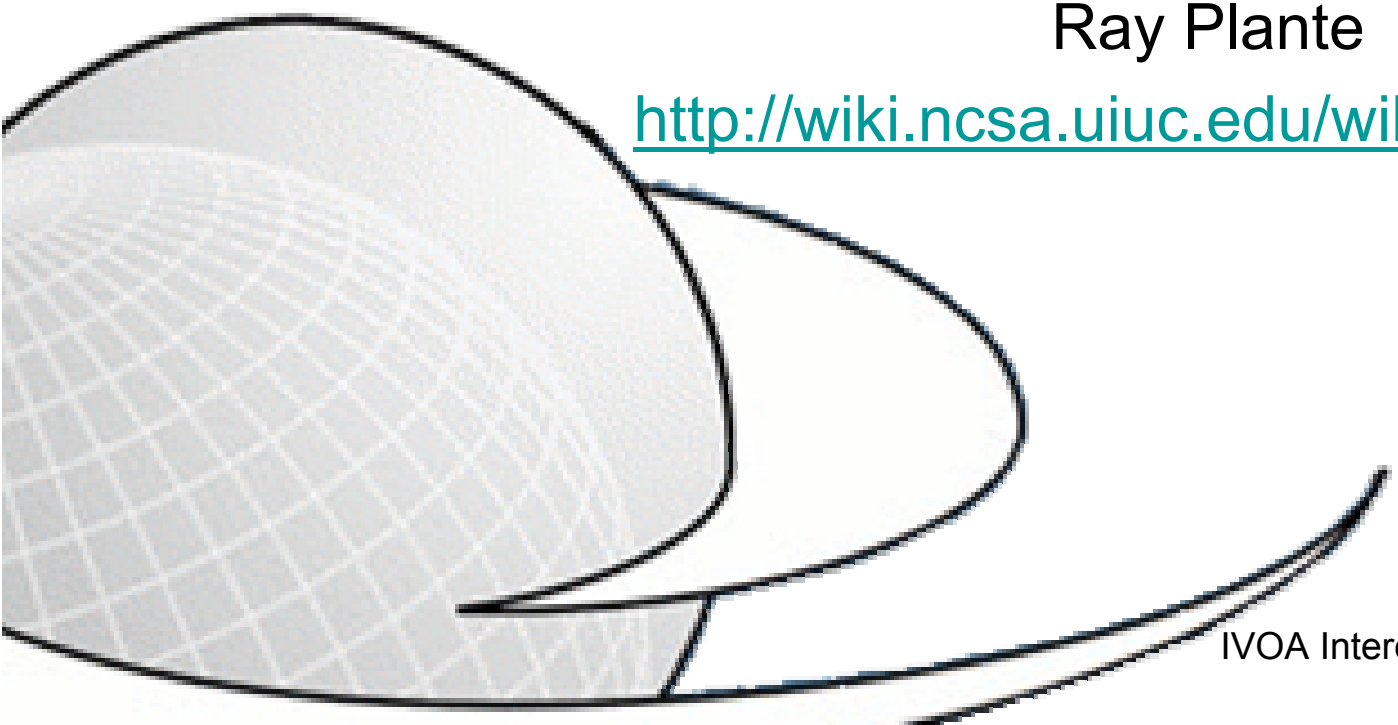
User Authentication Services in the NVO

Status and Plans

Ray Plante

http://wiki.ncsa.uiuc.edu/wiki/NVO_SSO/



19 September 2006
IVOA Interoperability Meeting – Moscow

UAS: What is it?

- A suite of services for…
  - Creating (and verifying) VO identities
  - Making them available to portals and client applications in the form of X.509 credentials
- Special focus on portal-managed credentials
  - When logging into a portal, users are sent to an NVO login screen (managed by NVO)
  - Credentials are delivered to portal for use on user's behalf
  - pubcookie used to delegate login to central service
  - NVO registration integrated with local portal integration
- Direct MyProxy-based access supported as well
- Two parts
  - UA services: hosted by VO project
  - Portal toolkit: for retrieving user credentials
    - In the form of Apache modules for transparent support

Both parts are available for download and use

Status of deployment

- UAS currently hosted at NCSA:
  http://nvoapp1.ncsa.uiuc.edu/
- Near-successful deployment into NVO Nesssi portal
  - Provides access to applications running on TeraGrid
  - Nesssi portal software has some problems handling proxy chains longer than 2
  - Demonstrated at NVO Summer School
- Next portal: NOAO Science Archive
  - This fall
- Other interested portals:
  - NRAO
  - Dark Energy Survey
- Software available at http://wiki.ncsa.uiuc.edu/wiki/NVO_SSO/
  - UAS
    - As tarballs (with 3rd-part installation requirements)
    - As VMWare virtual machines: already installed, just configure.

Current Work

- Switching to “on-line” CA for MyProxy
  - Will deliver “end-entity certificates” created on-the-fly based on latest information about user
  - More/less transparent change for portals/users
- Addition of Identity Verification Services
  - Via collaboration with Globus team
  - At registration, asynchronously contact multiple identity verification services (IVS)
  - When an IVS responds positively, “yes” is stored in user database
  - A record of verifications is written into certificate as SAML-encoded attributes
  - Turns *weak* certificates into *strong* ones

More on Identity Verification

- Who might host them?
  - NVO
  - Observatories
  - Academic departments
- What does verification mean?
  - Each IVS will provide a statement, *e.g.*
    - "this person with email address was awarded time on our telescope"
    - "this person is known as a member of our department"
- How will this information be used?
  - We plan to release reference software (Java, C) for extracting verification information for use by services
  - Service can choose which IVSes it trusts and can use the presence of IVS identifiers to allow access to service.
  - Note: verification attributes are not authorization attributes
    - Services may use verification attributes to assign authorization attributes to the user.
- Timescale:
  - Winter/Spring of this year
  - Reconsidering Shibboleth-based approach

Future Work

- Trans-IVOA federation of Identities
  - Login interoperability across VO projects
  - pubcookie has some limititations for federating
    - Looking at Shibboleth-based approach.