SSO review

Introduction to GWS-1 session,
IVOA Interop.,
Moscow, September 2006

What are we making?

- Authentication not authorization
  - Standard enables authorization but does not define it
  - IVOA will not make authorization standards
- Profile on existing standards
  - Select/combine best bits of standards from outside IVOA
  - Not primary comp-sci research
- Set of standards, not a monolith
  - Aiming for 4 IVOA recommendations
  - Standardize the easy/urgent bits first

The four standards

- Authentication methods (v1.0 WD)
- Identity delegation (not written)
- Community services (not written; prototypes exist)
- Registration of secure services (initial draft)

Goals for this meeting

- Reinforce consensus about community services
- Exchange prototyping results
- Choose a method for expressing identity attributes

Agenda

- Update on NVO UAS (Ray Plante)
- ESO arrangements for web portals (Paul Harrison)
- Caltech's SSO implementation in VOSpace (Rixon pp Matthew Graham)
- AstroGrid prototyping progress since Victoria Interop (Guy Rixon)
- Authorization using ontologies (Norman Grey)
- Possible use of RDF and/or SAML inside attribute certificates (Norman Gray)

The attribute thing

- Need to express affiliation & group membership
- Communities may define groups
- How to express affiliations/groups to services?
- Need services to be able to trust attributes
- Possibilities:
  - Put RDF/SAML attributes in proxy certificates
  - Add attribute certificates to proxy chain
  - Refer enquiring service to SAML attribute service
  - Design SOAP header to express attributes