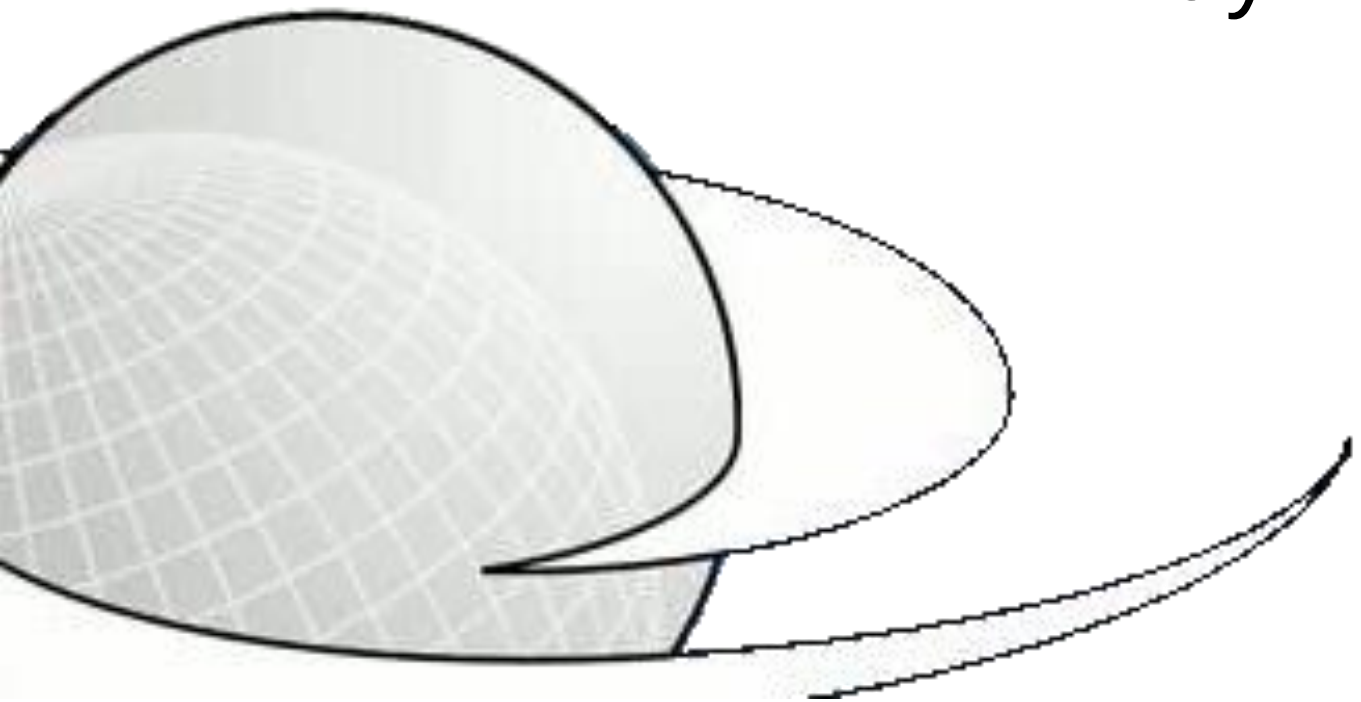
Emerging Authentication and Authorization Technologies

Ray Plante



23 October 2012
IVOA Interoperability Meeting – São Paulo

A&A currently in the IVOA

- Recommendation: SSO Profile: Authentication Mechanisms
  - 3 mechanisms: Digital signatures, TLS with username/password, **TLS with X.509 certs**
  - Focused on programmatic access to secured services.
  - Does not address any authorization issues

- Recommendation: Credential Delegation
  - Reflects the importance of X.509 certs

OpenID & Authenticating to Portals

- The challenge of certificates
  - Not user friendly
  - Not what web users are used to (username/password)
- VAO: OpenID-Certificate hybrid framework
  - User logs into portal w/federated un/pw via OpenID
  - OpenID: community standard for federated authentication
  - Includes standard mechanism to share user attributes
    - Real name, email, institution, home country
    - Requires approval from user before sharing
  - Leverage attribute exchange to deliver X.509 cert to portal
    - Portal can connect to secure services anywhere on user's behalf

OpenID & Authenticating to Portals

- Opportunity for standard?
  - VAO motivation: interoperable access to *proprietary* data *across archives*
  - Await existence of distributed assets (e.g. VOSpaces) to demonstrate usefulness
- VAOSSO: "productized" login services package
  - Allows for multiple independent deployments
  - VAO runs multiple mirrors for high availability

Restricted Authorization with OAuth

- Problem with delegated certificate
  - Portal can do anything user can do (for limited time)
    - Rogue or sloppy portal, anyone?
  - Trust established solely on who person is
    - No way for user to control what identity is used for
  - Desirable: let user control what can be done on a per-action basis
    - i.e. grant fine-grained authorization

Restricted Authorization with OAuth

- Enter Oauth
  - Community standard for granting and using authorization
  - Protocol for creating tokens that represent permission to do some specific things.
  - Does not ultimately address authentication
    - Implementations must insert means for user to prove themselves
    - VAO: OpenID authentication
    - Delegates authentication to third party services via OAuth token
  - VAO is using this to enable one-time sharing of data amongst an ad-hoc group
    - Distribute token via an access URL
- Concern regarding OAuth 2.0
  - Destabilized community
  - IETF RFC released this month

Authentication with Mozilla Persona

- SSO based around email addresses
  - Email address is your username, your (web) email provider provides login mechanism
  - Has OpenID-like mechanism that allows a portal to leverage the email provider's login mechanism to authenticate user
    - Mozilla calls on email providers (Google, Yahoo, anyone else) to support Persona protocol
    - Calls on browser vendors to support client side
    - Have clever work-arounds in advance of wide adoption
  - Low overhead for portals to use it
- Advantage over OpenID: Privacy concerns
  - If you use Google's or Facebook's OpenID provider to authentication, they can see which portals you are connecting to.
  - Persona does not expose this information to email providers

Persona for VAO?

- We could simultaneously support OpenID and Persona
  - Simple if logging in is all that is needed
  - Not sure how we would deliver X.509 cert
- Biggest issue: establishing long-term identity for interoperability
  - Maintain ownership of proprietary assets across sites: is email address a good basis?
    - Institutional email addresses change over time
    - Do we all need to get Google email addresses?
  - Can probably make this work