THE INTERNATIONAL VIRTUAL OBSERVATORY ALLIANCE

Identity Management in the NVO

Single Sign-on Support

Ray Plante

18 May 2007
IVOA Interoperability Meeting – Beijing

User Authentication Server: 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

    See the NOAO Portal Demonstration Quicktime Movie:

    http://www.ctio.noao.edu/~chrism/NOAO_NVO_Portal.mov
- Can also download certificates direct to the local platform:
  - End-entity Certs in PKCS12 format
  - Proxy Certs via MyProxy protocol
- 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

- Continue to support portal-managed certs
  - Currently supported Portals:
    - NOAO NVO Portal: www.nvo.noao.edu
    - Caltech NESSSI Portal: nesssi.caltech.edu
    - Dark Energy Survey Project Data Portal
  - Portal toolkit (slowly) improving
    - With help of portal partners (Matthew Graham, Chris Miller)
    - Installation of Globus no longer required (only need the Globus JavaCOG jar files)
- NVO User Identity Portal under development
  - Now support download of End-Entity Certs in PKCS12 format.
    - For loading into client-side applications; namely, a browser
    - Driver: NESSSI portal
  - Will add other account profile management services
    - Forgot password, username
    - Host, service certificate request services (will require strong cert)

Modes of Secure Portal Interaction

- The NESSSI Portal supports 2 modes:
  - Portal-managed certificates
  - Client-side certificates
    - User loads certificate into browser
    - Based on user interaction model supported by the US Dept. of Energy grid community
      - Browser connects directly with secure services
    - NVO Identity Portal will create EECs with a lifetime of up to 1 year
      - Portals are restricted to 36 hours

- Both modes have advantages/disadvantages
  - Client-side certs:
    - + Good support now from browsers, not difficult
    - + Simplifies portal implementation
    - + (Gets around a bug we're currently having with AJAX - UAS interactions.)
    - − Introduces notion of certificates to user
    - − Cannot support delegation
      - One secure service accesses another secure service on user's behalf
      - Expected to be important for interaction with VOSpace's outside of portal

On-going & Future Developments

- Identity Verification
  - Techniques for setting up webs of trust
  - Techniques for encoding the verification processes that were successful

- Migrate away from Pubcookie?
  - Problems:
    - Not standardized on the protocol level
    - Implementation is opaque and rigid
      - Though has lots of customization hooks
  - Alternatives?
    - Central Authentication Service (CAS): http://www.ja-sig.org/products/cas
    - Other open-source projects are emerging (SUN, josso.org, …)