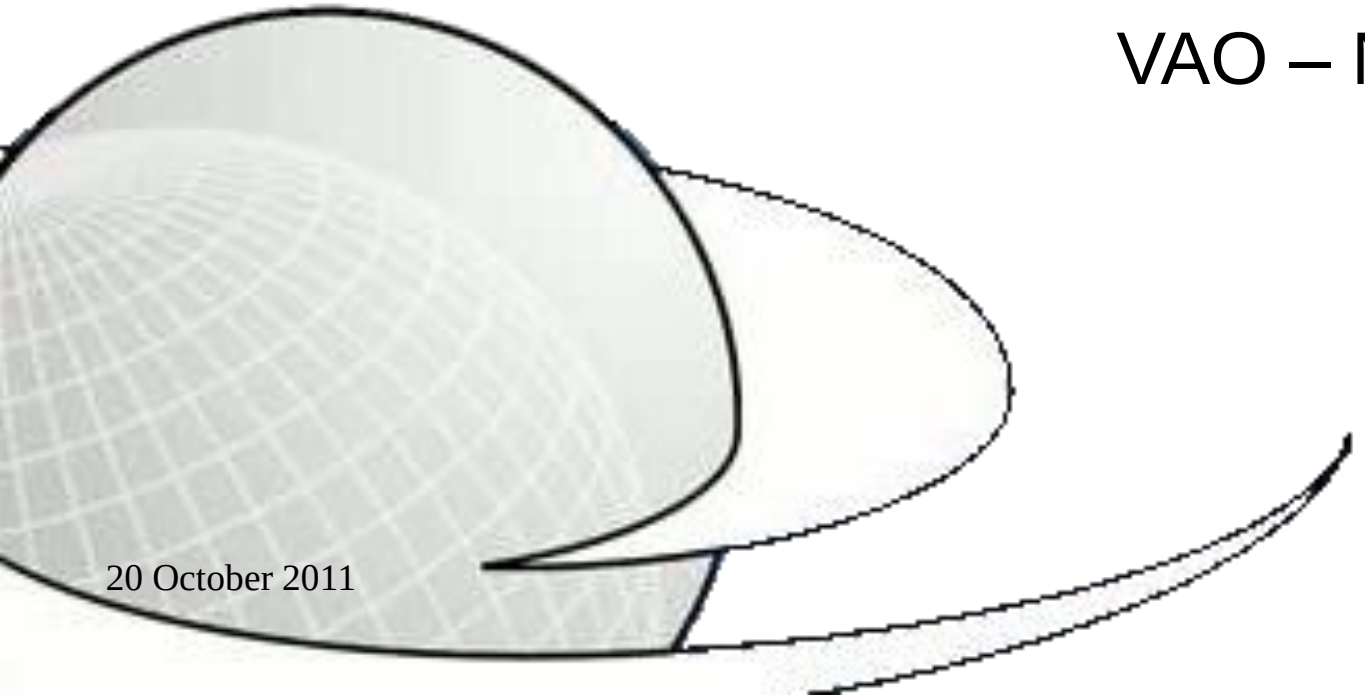
# VAO Single Sign-on with OpenID

Ray Plante

VAO – NCSA





20 October 2011

IVOA Interoperability Meeting -- Pune

# Common Identities across the VO

- VAO Single Sign-on follows on work in NVO
  - Manage users logins so they can access proprietary data across multiple archives
  - Work with both public and private data together with the same VO tools.
  - Portals use a plug-in to login NVO users
    - Currently support the NOAO Data portal, the DES portal, and our own Identity portal
  - NVO service based on pubcookie
    - While pubcookie was open-source, it was not based on an open standard
    - VAO:  migrate to OpenID

# Connecting the Browser world with the certificate world

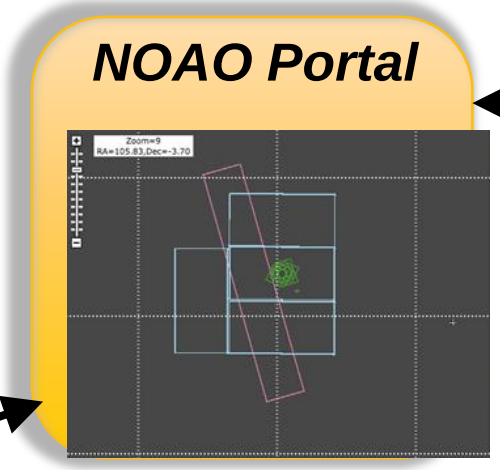
***NOAO Portal***

***Public SIA***

***Secured SIA***


***Login Service***

# Connecting the Browser world with the certificate world

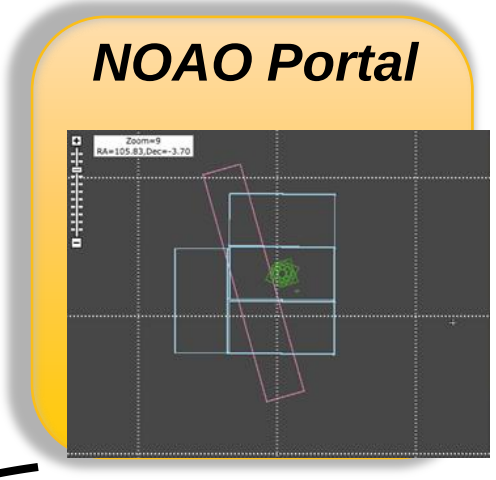



Public SIA

Secured SIA


Login Service

# Connecting the Browser world with the certificate world

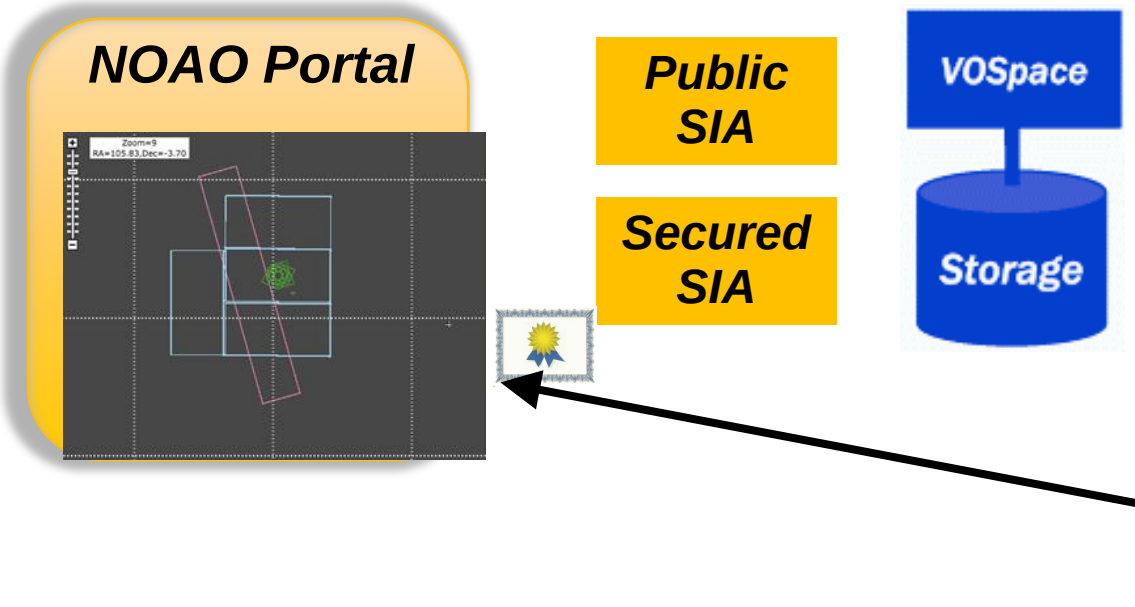



Public SIA

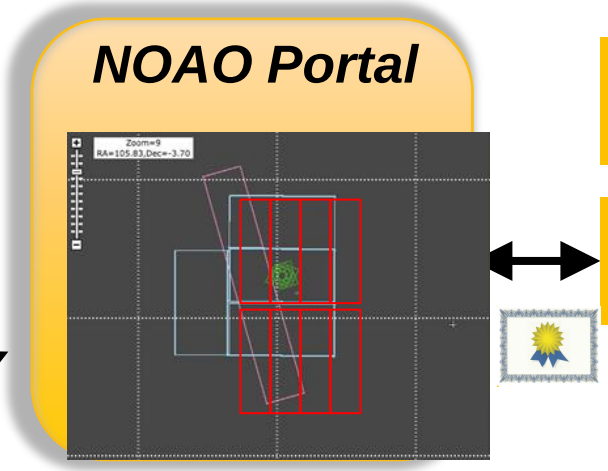
Secured SIA


Login with OpenID

# Connecting the Browser world with the certificate world



# Connecting the Browser world with the certificate world

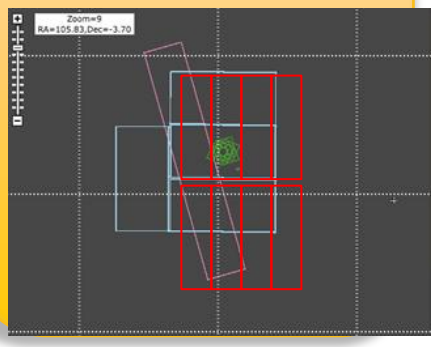





Public SIA

Secured SIA


# Connecting the Browser world with the certificate world




Public SIA

Secured SIA



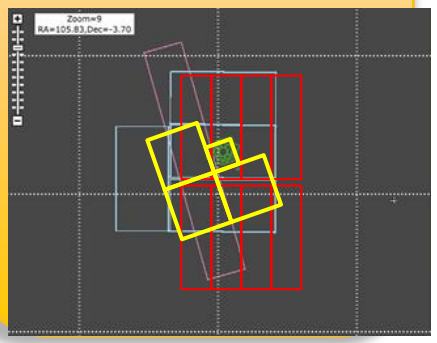
No Login Necessary

HST Archive

Secured SIA

# Connecting the Browser world with the certificate world

NOAO Portal



Public SIA

Secured SIA

VOSpace

Storage

Login Service

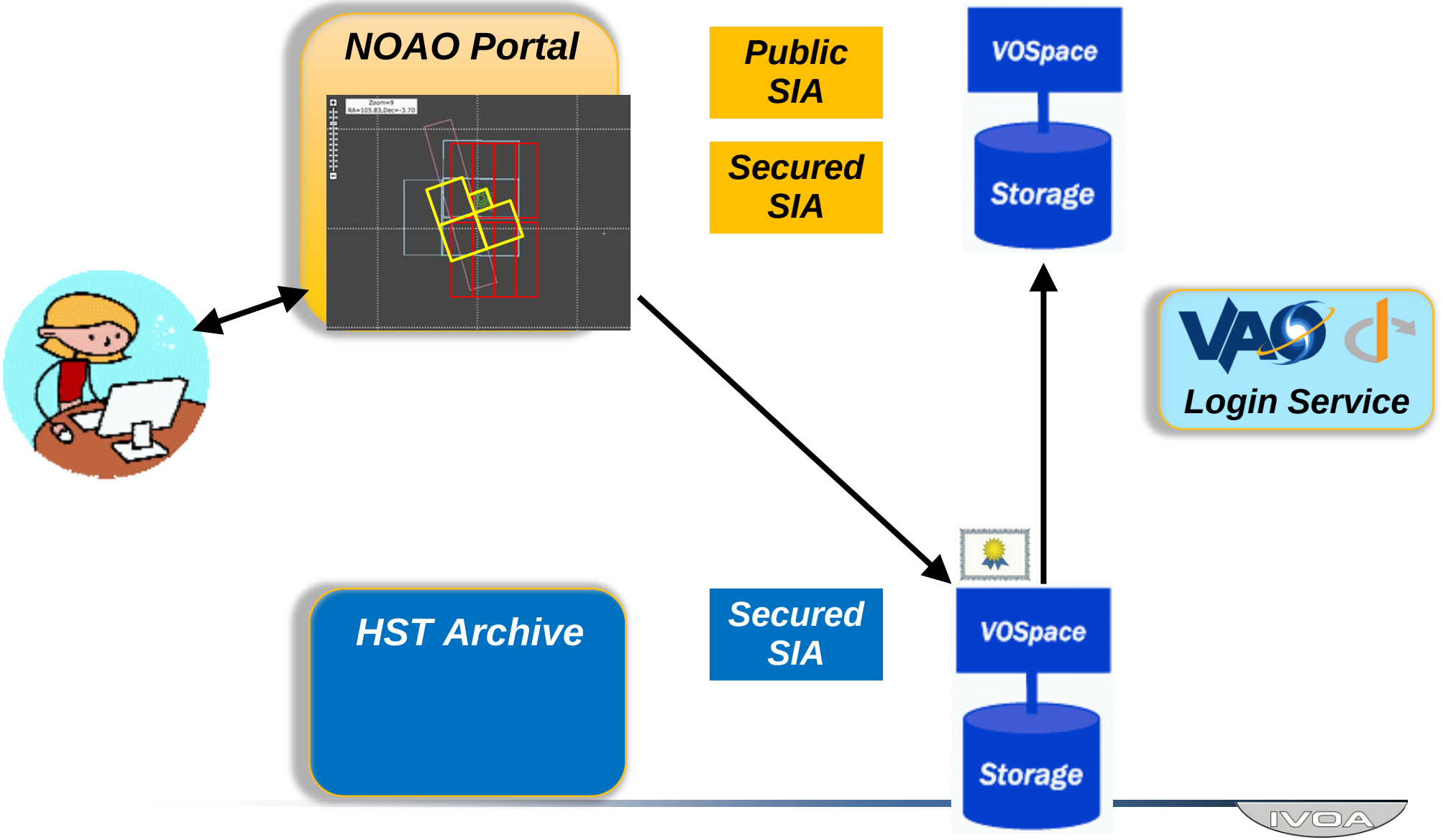
HST Archive

Secured SIA

VOSpace

Storage

# Connecting the Browser world with the certificate world



# Common Identities with OpenID

- OpenID provides interoperability with the IT world
  - A portal can choose to accept Google logins or VAO logins
  - A user can log into non-VO sites with their VAO login.

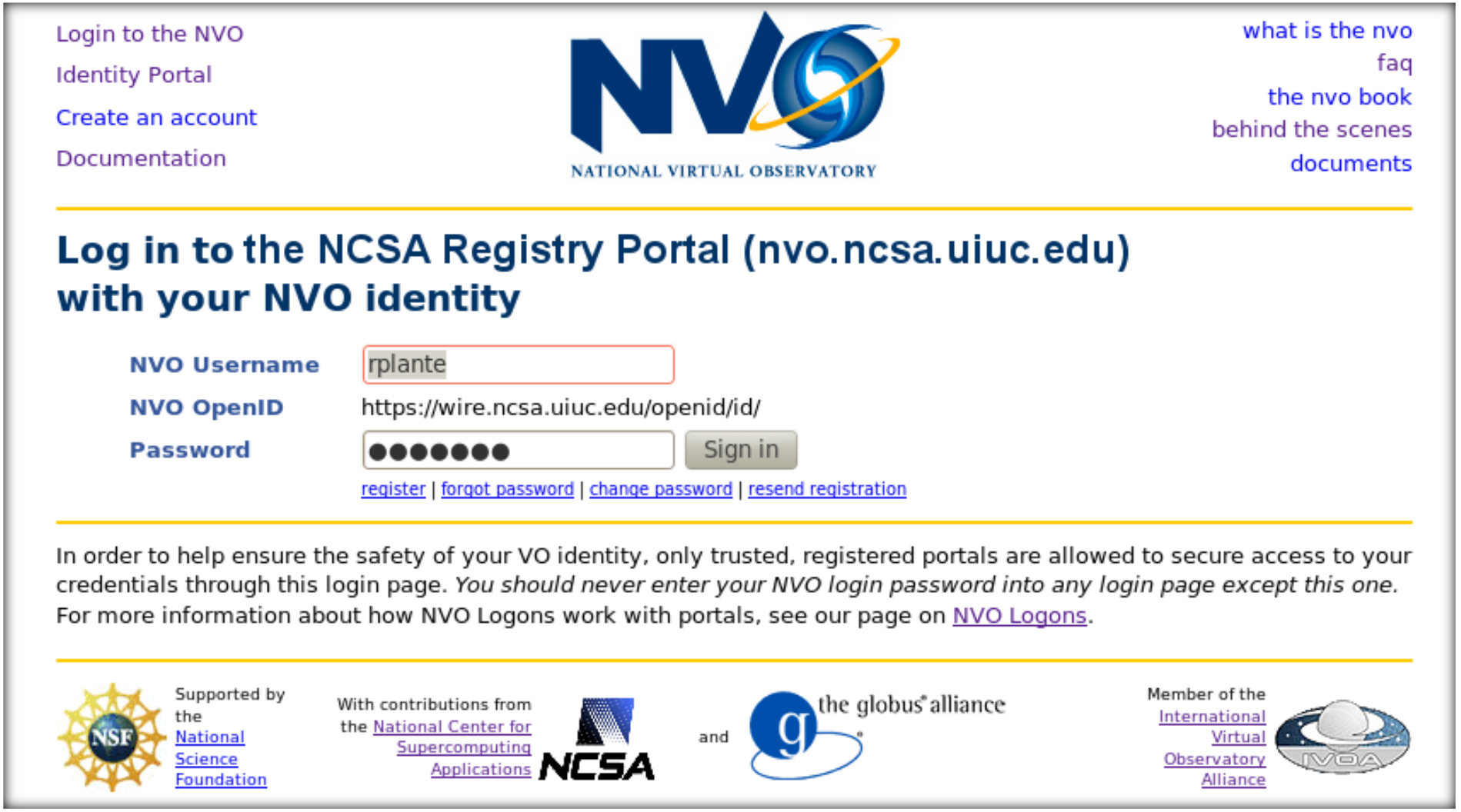
- VAO OpenIDs provides added features for Portal:
  - can retrieve X509 certificate on user's behalf
  - can retrieve metadata about user (with permission)
    - Real name, institution, country of residence, phone number
  - can get added assurances about user's identity


NVO Registration Portal
NVO @ NCSA
Publishing
Search @ STScI
Search @ Carnivore
RofR
Contact Us
National Virtual Observatory
Hosted By
NCSA
National Center for Supercomputing Applications
Welcome to the NVO Registration Portal at NCSA
New! Now you can log in with your VAO Login.
Don't have a VAO Login? Get one here!
Login with your VAO Login Now
Is this your first time registering?
If so, the first thing you must do is register your organization, providing us with some general information in our registration form. You will then be prompted to make up a login name and password that will allow you to return to this site to register other related resources.
And don't worry about long the registration form looks like. You will discover that registering additional resources is easier since you can inherit values from previously registered resources.
Click this checkbox to try out the form without publishing the data.
To get started by registering your organization, click:
Create new site
Do you already have a login?
Please provide username and password to access your registered resources.
Username:
Password:
Click this checkbox to log in to your non-publishing scratch area.
Login
Reset Form
If you would like to look at a sample repository, log in as "sample", password "sample".

# Logging In


NVO Registration Portal
NVO @ NCSA
Publishing
Search @ STScI
Search @ Carnivore
RofR
Contact Us
National Virtual Observatory
Hosted By
NCSA
National Center for Supercomputing Applications
New! Now you can log in with your VAO Login.
Don't have a VAO Login? Get one here!
Login with your VAO Login Now
If so, the first thing you must do is register your organization, providing us with some general information in our registration form. You will then be prompted to make up a login name and password that will allow you to return to this site to register other related resources.
And don't worry about long the registration form looks like. You will discover that registering additional resources is easier since you can inherit values from previously registered resources.
Click this checkbox to try out the form without publishing the data.
To get started by registering your organization, click:
Create new site
Please provide username and password to access your registered resources.
Username:
Password:
Click this checkbox to log in to your non-publishing scratch area.
Login
Reset Form
If you would like to look at a sample repository, log in as "sample", password "sample".

# Logging in


Login to the NVO
Identity Portal
Create an account
Documentation
NATIONAL VIRTUAL OBSERVATORY
what is the nvo
faq
the nvo book
behind the scenes
documents
Log in to the NCSA Registry Portal (nvo.ncsa.uiuc.edu) with your NVO identity
NVO Username
rplante
NVO OpenID
https://wire.ncsa.uiuc.edu/openid/id/
Password
Sign in
register | forgot password | change password | resend registration
In order to help ensure the safety of your VO identity, only trusted, registered portals are allowed to secure access to your credentials through this login page. You should never enter your NVO login password into any login page except this one.
For more information about how NVO Logons work with portals, see our page on NVO Logons.
Supported by the National Science Foundation
With contributions from the National Center for Supercomputing Applications
NCSA
and
the globus alliance
Member of the International Virtual Observatory Alliance
IVOA

# Logging In


Login to the NVO
Identity Portal
Create an account
Documentation
NATIONAL VIRTUAL OBSERVATORY
what is the nvo
faq
the nvo book
behind the scenes
documents
Do you trust nvo.ncsa.uiuc.edu/cgi-bin/sso/vaologin.cgi /index.html
The website nvo.ncsa.uiuc.edu/cgi-bin/sso/vaologin.cgi/index.html has asked you to confirm your NVO identity as unittest.
It also requires your NVO login ID (username).
Yes, share my NVO login ID (username), unittest.
Remember these settings for nvo.ncsa.uiuc.edu/cgi-bin/sso/vaologin.cgi/index.html and don't ask me again next time.
Sign in
Yes, I trust nvo.ncsa.uiuc.edu/cgi-bin/sso/vaologin.cgi/index.html. Sign in with my NVO login, unittest.
Cancel
No, I decline. Return to nvo.ncsa.uiuc.edu/cgi-bin/sso/vaologin.cgi/index.html without signing in.
Use a different ID
Sign out and use a different NVO identity to access nvo.ncsa.uiuc.edu/cgi-bin/sso/vaologin.cgi /index.html.

# Status

- OpenID-based services undergoing testing
  - For fall release
  - Includes tools for managing identity (user metadata, permissions)
  - Registration, Forgot password?, Forgot login?...
  - Download certs
- Developed toolkit for Portals
  - For plugging in support for VAO OpenID logins
  - Multi-language/framework
    - Java/servlet
    - Python module
    - Command line tool
      - For plugging into arbitrary CGI script
    - Possible others: php, .NET
- Usage
  - VAO: New Registry Publishing Interface
  - Will migrate NOAO, DES
  - Other archives/portals encouraged to participate

# Opportunities for Interoperability

- Trusted VO OpenID providers
  - Other VO projects that maintain user identities could offer OpenID authentication
  - We could trust each others providers
  - Provide common user metadata
  - Share trusted identity assertions
    - Verification of user's identity
    - "This user has a Grid Canada Identity"
    - "This user has observed on NOAO facilities"
  - Authorization groups

# Authorization Groups

- Collaborative Access
  - CADC transfer stats illustrate that authorization groups are important to astronomers.
  - Can we share group information (with permission)?
  - Is there a role we can play to help users maintain group memberships?
  - How should that connect with resource-specific permssions?

# OAuth: restricted access

- VAO VOSpace (Dmitry Mishin)
  - Supports OAuth as an authorization mechanism
  - Integrates easily with OpenID
  - Also widely supported
- Some advantages
  - With our model use of X.509 certs, portal can do *anything* the user can do for the life of the cert.
    - We will have a mechanism for discouraging passing a cert to an "untrusted" portal.
  - OAuth allows to delegate authorization for a very specific action at a specific site
    - "Access these files from this site"
- Are there use cases where this would be a preferred mode?